Data Centric Security and Federated Mission Networking

Isode

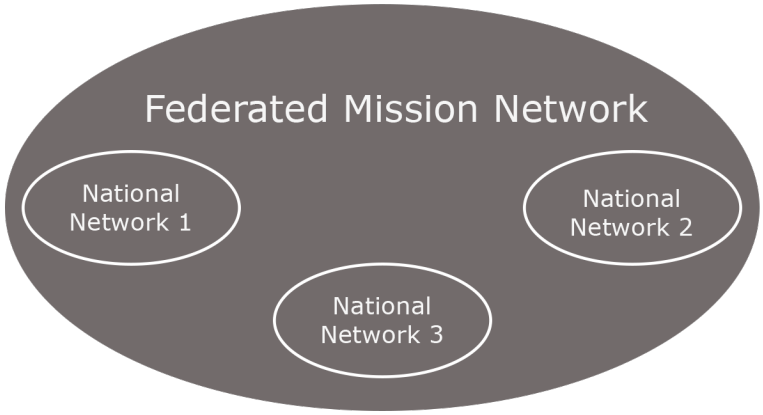
Federated Mission Networking (FMN) is a key NATO initiative for deploying multi-nation operations with maximum interoperability. Data-centric security (DCS) is a security approach that controls access to information based on the information, in contrast to the older Network-centric security model. This paper looks at how DCS can be used with FMN, with particular focus on XMPP and Messaging applications provided by Isode.

Data Centric Security

Data Centric Security has two key concepts for protecting data:

1. Associating Confidentiality Labels with information. Confidentiality Labels are standardised in STANAG 4774, and STANAG 4778 specifies how these labels are bound to various protocols and data formats
2. Access control follows the Confidentiality Metadata Based Access Control (CMBAC) standardised in STANAG 5678 to check Confidentiality labels against Confidentiality Clearances in the context of a security policy.

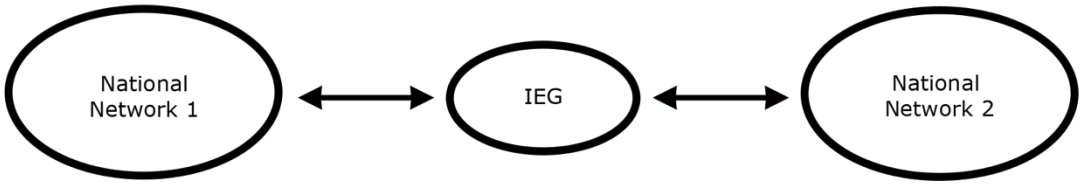
Data Centric Security and Isode's DCS products are described in more detail in the Isode white paper, Isode Approach to Data Centric Security using NATO Confidentiality Labels.



In a Federated Mission Network, a number of national networks will be openly interconnected. There will be a core shared network infrastructure with elements such as IP Routers and Domain Name Service working for the whole mission network. This is intended to provide a coherent and efficient overall system with communication between partners.

It is also important that each National Network can operate independently without any critical dependencies on the federation. Identities of users and other entities, along with associated authentication and authorisation, are managed independently in each national network. This means that each national network has its own Identity Provider (IDP).

Cross-Domain Comparison



Another contrasting approach for connecting national networks is the cross-domain approach illustrated above. Here, national networks are separated by an Information Exchange Gateway (IEG). The IEG protects against information leakage out of a network and against malware entering. In this model, national networks generally have independent security policies and PKI, with conversion happening at the boundary.

Isode provides two cross-domain capabilities:

- For XMPP, the solution is described in the Isode white paper, Isode's XMPP Cross Domain Solution.
- For Email and Military Messaging, the solution is described in the Isode white paper Cross Domain Military Messaging.

Note that there is no IEG or equivalent in a Federated Mission Network.

Confidentiality Labels for a Federated Mission Network

The FMN model is that a Federated Mission Network will have a single security policy that will be adopted by all participating nations. This means that access control can be applied consistently across the whole network. A security policy, which will generally be specified with a Security Policy Information File (SPIF), defines the structure of the labels used and how access control (CMBAC) is applied.

The rest of this section gives an example of a NATO FMN approach. The principles could be applied to a non-NATO FMN with an independent security policy.

A NATO Mission Network will use a NATO policy. A NATO Mission will be approved by the North Atlantic Council (NAC) and be assigned a name such as ISAF or KFOR. Missions can include both NATO nations and non-NATO partner nations. The name will be used as a Security Context Category Value in the policy.

The following examples use a hypothetical mission name of MROD. Basic labels for the MROD mission would be:

- NATO/MROD SECRET
- NATO/MROD RESTRICTED

Labels could be further constrained by the use of categories within the policy. These examples use values from the Special Designator category:

- NATO/MROD SECRET ATOMAL
- NATO/MROD SECRET BOHEMIA
- NATO/MROD SECRET ATOMAL/BOHEMIA

The EYES ONLY category can be used to constrain labels to specific nations on the mission network. For example:

- NATO/MROD SECRET UK ONLY
- NATO/MROD CONFIDENTIAL UKRAINE, AUSTRALIA ONLY

Users will be assigned STANAG 4774 Confidentiality Clearances following the security policy that will constrain which information a user has access to.

Federating Messaging and XMPP

XMPP, Email and Military Message are built on protocols designed for federation. This means that in a mission network with open network connectivity between national networks that federation of these applications will "just work".

The rest of this paper looks at considerations of additional functionality needed.

DCS & Message Delivery

This section and the following ones reference DCS functionality provided by Isode products. In particular:

- Messaging checks provided by Isode's M-Switch product set out in the Isode white paper Security Label Capabilities in M-Switch Products.
- XMPP checks provided by Isode's M-Link product set out in the Isode white paper XMPP and Security Labels.

In order to support DCS, a baseline for XMPP, Email, and Formal Military messaging will be used by the clients to add security labels to messages, which is done by Isode's Swift and Harrier clients.

For the DCS to be useful, access control (CMBAC) needs to be applied. For push technologies like XMPP and messaging, a natural place to perform this is in the server performing message delivery. This will ensure that a user will only receive messages that the user is cleared to see. Isode supports this by providing in Isode's Cobalt product the ability to configure a STANAG 4774 Confidentiality Clearance for the user. This is then used for CMBAC prior to delivery; Isode XMPP and Messaging servers support these checks.

This is a fundamental mechanism to support DCS in the federated environment where there is no IEG capability. Nations can trust each other to ensure that messages are delivered only to appropriate users.

Peer Controls

A complementary control provided by Isode's XMPP and Messaging servers is to provide CMBAC with a Confidentiality Clearance associated with a peer link between two nations. This could be used to check the EYES ONLY security category to require that, if present, the destination country is set.

This will allow messages to be blocked at a stage earlier than delivery, which improves responsiveness to the sender and avoids transferring a message further than is needed.

Federating XMPP MUC Rooms

In a military environment, communication is invariably by use of MUC (Multi User Chat) rooms, rather than 1:1 chats.

In a federated environment, one approach to support communication is to have users join MUC rooms hosted by partner nations. However, a better approach is to use Federated MUC (FMUC) described in the Isode white paper, Federated Multi-User Chat.

In an FMUC deployment, users will always join a local MUC room, which is a natural approach. As part of the mission federation, these rooms will be connected together. This provides a scenario where communication can be shared between nations, but in the event of network partition, each nation can continue internal communication.

Address Books for Messaging

When sending messages, it is highly desirable to have an address book. A common approach is to use LDAP (Lightweight Directory Access Protocol) to access address information in a directory server. This is the approach taken for both Email and Military Messaging by Isode's Harrier client.

An important benefit of this approach is that Harrier can determine recipient capabilities and, in particular, the STANAG 4774 Confidentiality Clearance of each user in the address book. This enables Harrier to perform a CMBAC check on each recipient (using the proposed Confidentiality Label of the message) and either advise when this check fails or prevent sending. The choice will depend on whether the check can be relied on in all scenarios.

In a cross-domain scenario, the only way to provide an address book for remote recipients is to perform some sort of directory synchronisation across the domain boundary, perhaps using a tool such as Isode's Sodium Sync.

In a mission federation, a simpler approach is possible, as it will typically be possible to access the directory of a peer nation. This will enable a client such as Harrier to be configured to access the address book of each federated nation. This will enable the lookup of all users and also CMBAC checks as to whether a message will be delivered.

File Access and "Pull" Applications

Messaging and XMPP are "push" applications which can be deployed quite simply in a federated environment. "Pull" applications, such as file access, have additional requirements that are worth noting.

To access a file on a system in a partner nation will require authorisation. The difficulty is that the accessing user will be using the local IDP, whereas the application will require the use of its own IDP.

The solution to this is provided by STANAG 5663, "Federated Identity, Credential and Access Management (ICAM)". This specifies how to provide the necessary authorisation using OAuth technologies.

This approach might also have uses for XMPP to authorise access to remote MUCs.

Conclusions

For XMPP and SMTP messaging, federated operation is natural, and basic operation in a Federated Mission Network works without any special changes. When DCS is introduced, additional requirements arise, in particular the need to apply CMBAC access control to the message delivery to ensure that messages are only delivered to users with appropriate clearance.

Isode

www.isode.com

14 Castle Mews, Hampton
Middlesex, TW12 2NP

Secure, Seamless Communication Solutions