Isode Approach to Data Centric Security using NATO Confidentiality Labels

Isode

Data Centric Security (DCS) is a key trend in secure networking. This white paper starts with an overview of DCS and shows the central role that NATO Labelling, specified in STANAGs 4774 and 4778, are expected to play.

The white paper then looks at Isode product support for STANAG 4774/4778, noting results from the multi-nation interoperability trials at CWIX 2025 in June 2025. This paper sets out Isode vision for DCS showing a mix of current and planned capabilities.

Data Centric Security

Data Centric Security (DCS) essentially means that access to data is controlled by the data. It contrasts with Network Centric Security, where access to a network gives access to data. DCS is seen as vital protection for a modern secure network. The broad DCS concept is that access to every piece of data is controlled. More details on DCS are provided in NATO "Data-Centric Security Implementation Plan."

Security Labels and DCS

DCS needs a flexible mechanism to control access to data which works in a large scale federated environment. Security Labelling provides this mechanism and is central to DCS. The model of security labelling has been well established for physical documents. Electronic security labels clearly identify the rights needed to access associated data.

Details on electronic security labels and their use is provided in the Isode white paper "Access Control using Security Labels & Security Clearance".

NATO Labelling

For DCS to work effectively, it is necessary to have a widely adopted security label standard. NATO is moving to mandate use of NATO Confidentiality Labels specified in STANAG 4774 "CONFIDENTIALITY METADATA LABEL SYNTAX", published as ADatP-4774. Isode anticipates that STANAG 4774 will be widely adopted, and this paper is primarily focused on STANAG 4774.

STANAG 4774 is based on the SDN.801c model developed by NSA. This leads to a flexible security label structure with classification (Secret, Top Secret etc) plus an extensible category mechanism that allows a security policy to associate information with a label. For example, the "Additional Sensitivity" category in the NATO policy allows indications such as ATOMAL, which restricts access to those cleared for atomic information access.

This is an example security label following the policy of CWIX 2025:

```
<ConfidentialityLabel xmlns= urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
ReviewDateTime="2034-04-18T09:26:56Z">
   <ConfidentialityInformation>
      <PolicyIdentifier
URI="urn:oid:1.3.6.1.4.1.31778.102.25">CWIX25</PolicyIdentifier>
      <Classification>SECRET</Classification>
      <Category URI="urn:oid:1.3.6.1.4.1.31778.103.15" Type= PERMISSIVE"
TagName= Releasable To">
         <GenericValue>AUS</GenericValue>
      </Category>
   </ConfidentialityInformation>
   <CreationDateTime>2025-04-18T09:27:52Z</CreationDateTime>
</ConfidentialityLabel>
```

Some points to note:

1. This label is XML-encoded, noting that STANAG 4774 supports other encodings, including JSON and CBOR.
2. The label contains label lifecycle information (creation data and review date), which is a key feature of STANAG 4774.
3. The security policy, which defines label structure, is identified by an object identifier (globally unique reference) and a string ("CWIX25").
4. The security classification is SECRET.
5. The CWIX 2025 policy has one security category (releasable to). This label shows releasable to Australia (AUS).

Access Control

Access Control using security labels is provided by checking a security label against a security clearance in context of a security policy. This check is commonly referred to as an Access Control Decision Function (ACDF). Details are provided in the white paper referenced above.

Use of ACDF to check labels is often referred to as Rule Based Access Control (RBAC), confusingly sharing an acronym with Role Based Access Control. It is a simple and clean approach. Note that security labels are always checked against security clearances. It is generally not possible to compare labels against labels. ACDF is central to DCS, as the primary goal of labelling data is to facilitate enhanced protection, sharing, and access control.

Label Binding

It is important to explicitly associate security labels and other meta-data with data being handed. STANAG 4778 "METADATA BINDING MECHANISM" formalizes this binding for STANAG 4774 labels and other data such as meta data specified in STANAG 5636. STANAG 4778 specifies generic mechanisms, with specific bindings for a number of data formats and protocols. The bindings of most interest to Isode are for XMPP and SMTP, which are discussed later.

STANAG 4778 allows association of multiple labels with data and can associate labels with different parts of the information—an approach historically termed "portion marking." This is important in more complex scenarios when associating a single label with the entire object does not suffice.

As well as defining the basic binding, STANAG 4778 provides an option for cryptographic binding using digital signature mechanisms. This binding provides digital signature verification, which is important to validate:

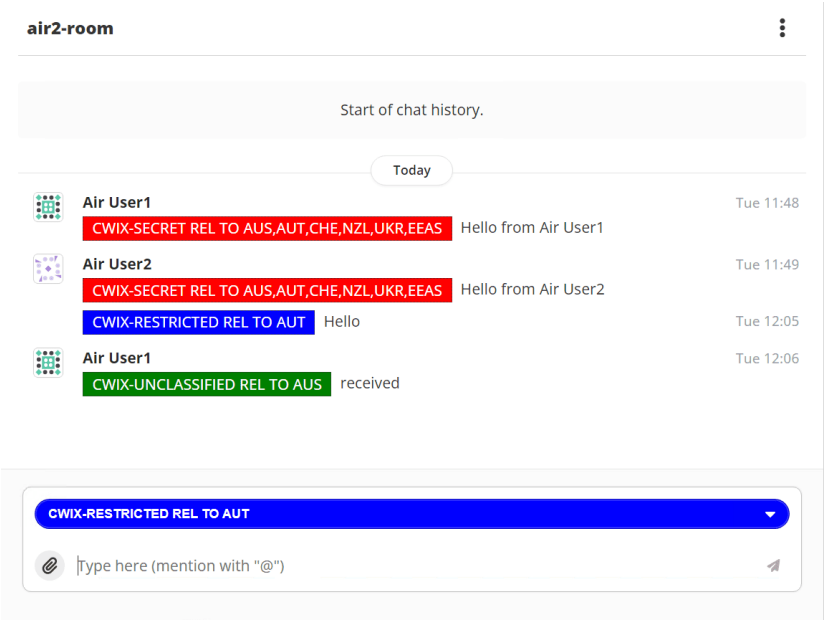
- That a valid label is provided.
- That the label is correctly associated with the data
- That the data has not been modified since the label binding (content integrity).

The digital signature can usually also be used to validate the originator.

Isode STANAG 4774 Infrastructure

Isode provides a number of applications with STANAG 4774 support. These all rely on common infrastructure. For a given deployment of STANAG 4774, label structure is specified by a security policy. More information is provided in the Isode white paper "Creating and Managing a Security Label Policy." A security policy is represented as Security Policy Information File (SPIF). Isode uses the Open XML SPIF format, which is also used by NATO.

SPIFs are too complex to manipulate manually, and so an editor is important. Isode provides a SPIF editor as part of its product set. This is shown below, editing the CWIX 2025 SPIF. It can handle more complex SPIFs.



SPIFs managed by SPIF Editor are used by Isode applications to create and validate STANAG 4774 labels. The SPIF editor can also create STANAG 4774 label catalogs from a SPIF, including setting review date and setting the default label. The catalog is useful for

product configuration tools to conveniently set labels. It is also important for end user UIs to allow convenient drop-down selection of commonly used labels.

A sample catalog with two STANAG 4774 labels following CWIX 2025 SPIF is shown below:

Things to note:

1. The catalog follows the format specified in XEP-0258. There was no requirement to design a new format, as this one can be used with STANAG 4774 labels.
2. Each label has a selector, which is a short string suitable for use in drop down menu selection. This value can be edited when creating the catalog.
3. Each label has a display marking, derived from the SPIF, comprising a string and a colour. This enables UIs to correctly display the labels.

Application Integration Points

There are three points in the application architecture where STANAG 4774 support is relevant. These are common to both messaging and XMPP:

1. Client support is central and critical. There are two basic functions needed:

    - Assigning labels to messages, either by selection from catalog or by label creation.
    - Display of received labels. The labels are transferred in protocol as XML. The client must use a SPIF to validate and correctly display a label.

The client may also check recipient clearance to prevent the sender from sending a message to a recipient not allowed to receive it.

2. Server support is also important, and three functions may be provided:
    - Authorisation of local delivery. The server is expected to perform ACDF on arriving messages and only deliver messages to users with rights to see them. This is a key enforcement point for DCS.
    - Authorisation of onward transfer, to prevent transfer to recipients not allowed to receive the message or over channels without suitable clearance.
    - Label transformation. This might include mapping to legacy label formats or mapping to a different security policy. The latter is often important in conjunction with cross domain.

3. Cross domain. When transferring messages cross domain, secure validation of security labels is a vital check.

Isode Messaging Support

Isode provides STANAG 4774 support for both email and formal military messaging. This follows the SMTP Binding specified in ADatP-4778.2 "PROFILES FOR BINDING METADATA TO A DATA OBJECT."

Harrier

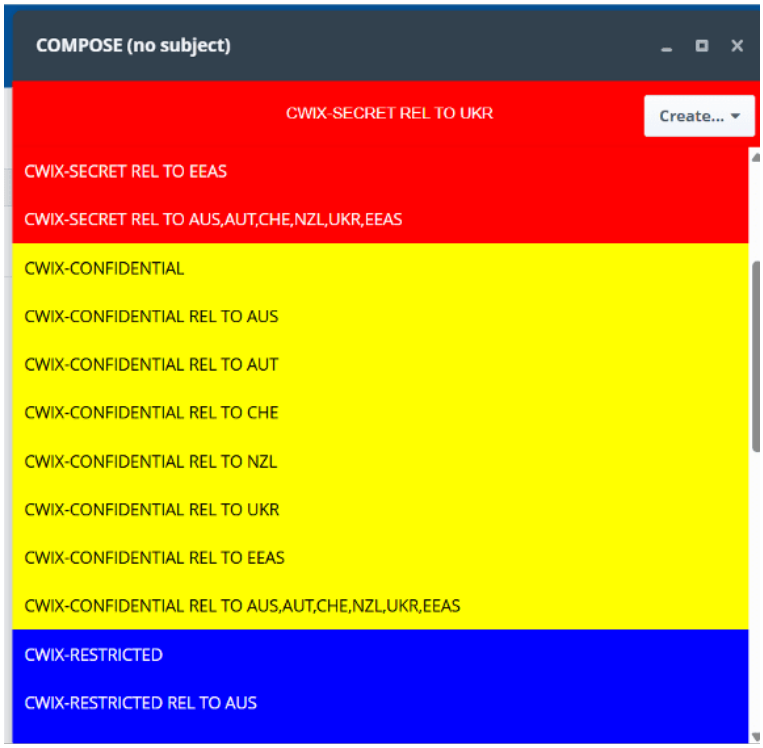
Harrier is Isode's messaging client, which provides full military messaging support but may also be used for email. Primary selection of label is from a drop-down selection based on two catalogs:

- A system catalog of labels available to all users and roles; and
- A personal catalog of additional labels that can be managed from Harrier.

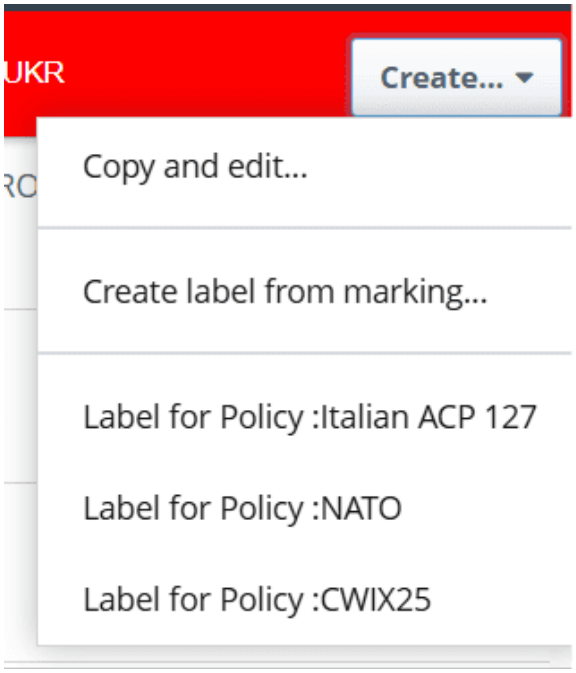
An example using a CWIX 2025 catalog is shown below:

```
<catalog xmlns="urn:xmpp:sec-label:catalog:2">
   <item selector="CWIX25|SECRET">
      <securitylabel xmlns="urn:xmpp:sec-label:0">
         <displaymarking bgcolor="red" fgcolor="white">CWIX-
SECRET</displaymarking>
         <label>
            <ConfidentialityLabel
xmlns= urn:nato:stanag:4774:confidentialitymetadatalabel
ReviewDateTime= 2034-04-18T09:26:56Z">
               <ConfidentialityInformation>
                  <PolicyIdentifier
URI="urn:oid:1.3.6.1.4.1.31778.102.25">CWIX25</PolicyIdentifier>
                  <Classification>SECRET</Classification>
               </ConfidentialityInformation>
               <CreationDateTime>2025-04-18T09:27:52Z</CreationDateTime>
            </ConfidentialityLabel>
         </label>
      </securitylabel>
   </item>
   <item selector="CWIX25|UNCLASSIFIED|REL TO
AUS/AUT/CHE/GEO/MOL/NZL/TUN/UKR/EEAS >
      <securitylabel xmlns= urn:xmpp:sec-label:0">
         <displaymarking bgcolor= fgcolor="white">CWIX-UNCLASSIFIED REL
TO AUS,AUT,CHE,GEO,MOL,NZL,TUN,UKR,EEAS</displaymarking
         <label>
            <ConfidentialityLabel
xmlns="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
ReviewDateTime="2034-04-18T09:26:56Z">
               <ConfidentialityInformation>
                  <PolicyIdentifier
URI="urn:oid:1.3.6.1.4.1.31778.102.25">CWIX25</PolicyIdentifier>
                  <Classification>UNCLASSIFIED</Classification>
                  <Category URI="urn:oid:1.3.6.1.4.1.31778.103 15"
Type="PERMISSIVE" TagName= Releasable To">
                     <GenericValue>AUS</GenericValue>
                     <GenericValue>AUT</GenericValue>
                     <GenericValue>GEO</GenericValue>
                     <GenericValue>MOL</GenericValue>
```

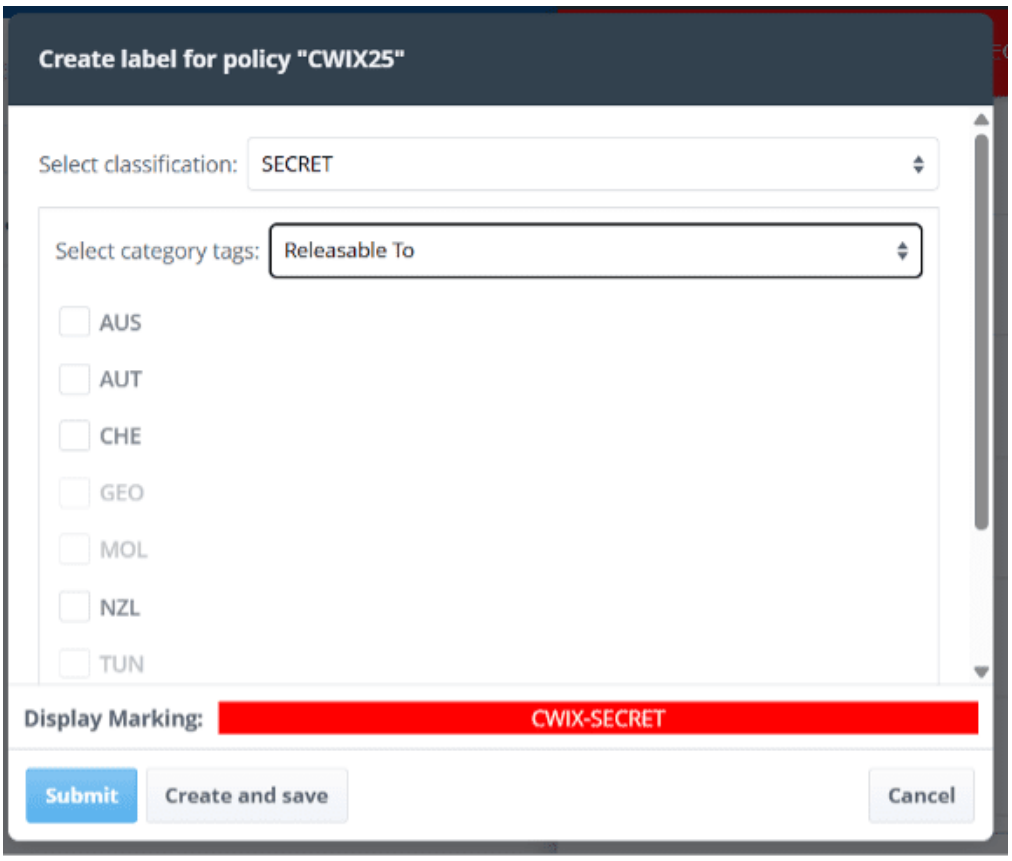
```
                        <GenericValue>NZL</GenericValue>
                        <GenericValue>CHE</GenericValue>
                        <GenericValue>TUN</GenericValue>
                        <GenericValue>UKR</GenericValue>
                        <GenericValue>EEAS</GenericValue>
                    </Category>
                </ConfidentialityInformation>
                <CreationDateTime>2025-04-18T09:27:52Z</CreationDateTime>
            </ConfidentialityLabel>
        </label>
    </securitylabel>
  </item>
</catalog>
```



If the desired label is not in the catalog drop down, any valid label can be created. The user is given a number of options to create the label, including selection of any security policy that Harrier is aware of:



When a policy is selected, a straightforward UI is presented to configure the label. The following screenshot is from CWIX 2025 SPIF.



Note:

1. Classification is chosen as SECRET from drop-down selection.
2. "Releasable To" values are chosen by check box.
3. Some values are greyed out, as these are valid tag values not permitted for use with SECRET.
4. Label can be used once for the current message or also saved in personal catalog for future use.

Harrier accesses an ACP 133 directory using M-Vault (Isode's Directory Server) to look up recipients and to check clearances. Harrier will only allow selection of labels which the originator is allowed to access. Harrier will only allow sending of messages to recipients cleared to receive the label.

Harrier digitally signs messages using S/MIME including signing the message header. This provides content integrity checking and securely binds the STANAG 4774 label to the message.

M-Switch

M-Switch security label capabilities are described in detail in the Isode white paper "Security Label Capabilities in M-Switch Products," which will be extended to support STANAG 4774. M-Switch supports a wide range of security label formats, all driven from a core Isode SPIF. It is anticipated that many security label deployment will migrate to STANAG 4774, but some legacy usage such as ACP 127 will be used for a long while. A key M-Switch capability is conversion between STANAG 4774 labels and other label formats.

M-Switch also uses ACDF checking against security clearances to provide Security Enforcing Functionality (SEF). Key elements of this:

Only delivering messages to mailboxes with clearance to receive the label on the message. This is DCS enforcement.

Checking messages against clearance of message routes, to prevent inappropriate transfer over a channel not cleared for all traffic.

Using security labels and clearances to determine the correct channel, for example, to send NATO-labelled messages over channel with NATO crypto and national messages over a channel with national crypto.

Cross Domain

Isode's messaging cross domain solution is described in the white paper "Cross Domain Military Messaging". The key components from a security label perspective:

1. M-Guard, Isode's XML Guard that provides secure unidirectional validation of XML messages, suitable for use across a domain boundary.

2. Military Messaging Application Profile, which specifies XML message formats and checking rules for use with an XML Guard. This includes STANAG 4774 label checking, using exact match of allowed labels.
3. M-Switch Edge, which converts standard messages to the XML messages needed by M-Guard and following the Military Messaging Application Profile.
4. M-Switch providing conversion of STANAG 4774 labels between different policies. This is important cross domain, as typically different security policies will be used in each domain.

This provides secure checking of STANAG 4774 labels in email and military messaging over a cross-domain boundary.

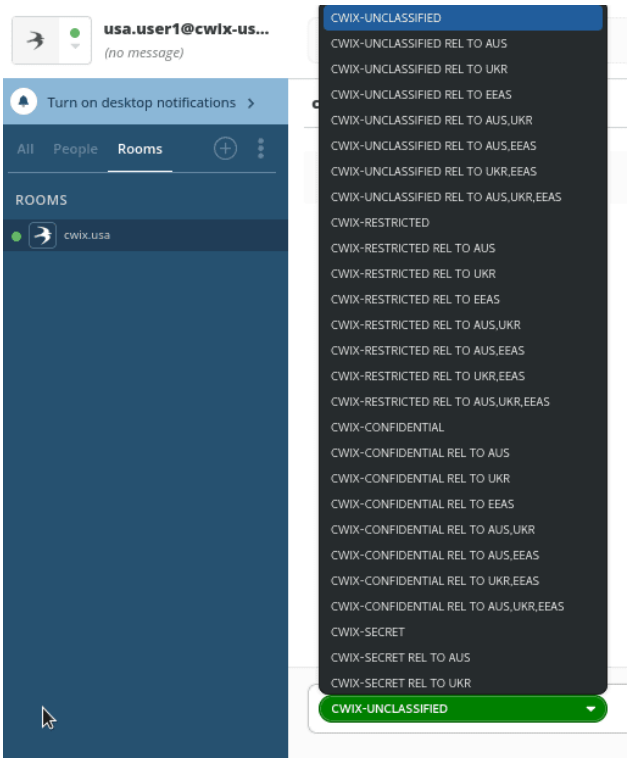
Isode XMPP Support

XMPP is the open standard for presence and chat used by NATO.

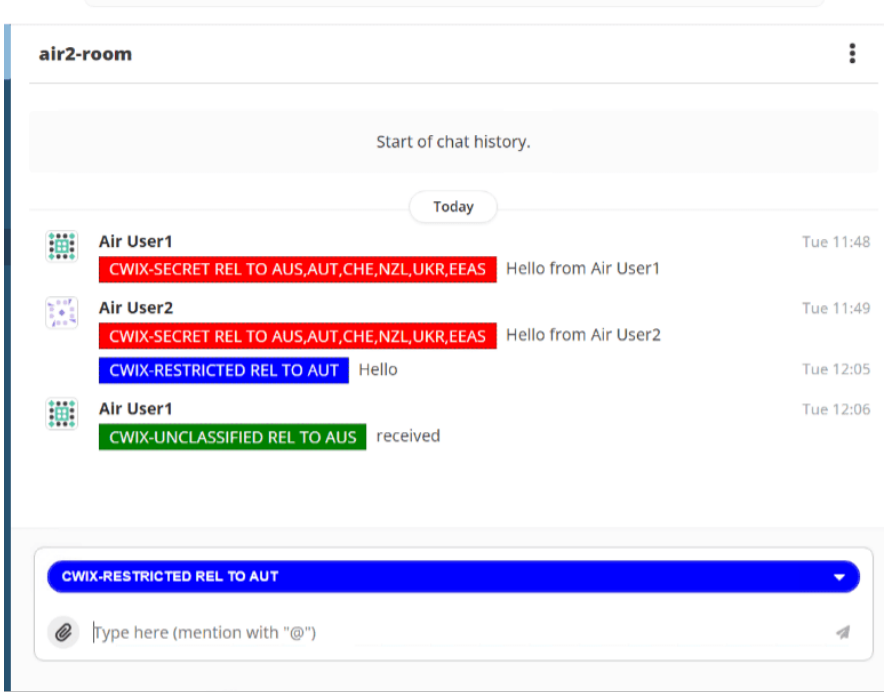
Swift

Historically, Swift has used XEP-0258, "Security Labels in XMPP," which provides a flexible security label mechanism that enables a simple, lightweight client implementation. This approach is not possible with STANAG 4774, which needs support in the client.

Swift uses an Isode STANAG 4774 label catalog to provide convenient drop-down selection of STANAG 4774 labels. Label selection from a CWIX 2025 catalogue is shown in the following screenshot.



On message reception, Swift uses a configured SPIF to validate incoming labels and generate a correct display marking to present to the user. An example is shown below, which shows different labels in a MUXC room and label selected for compose of a new message.



Swift will also display the Label Display Marking for a MUC room configured in M-Link, described below. It also enables a more compact display, as the per-stanza security labels are not shown when the display marking matches that for the MUC room. This is described in more detail with M-Link.

M-Link

M-Link security provides flexible security label / security clearance based ACDF described in the Isode white paper "Using Security Labels to Control Message Flow in XMPP Services." Security Labels and Security Clearances can be configured to provide controls at server, domain, MUC room and user level. Controls message delivery based in user clearance provide DCS enforcement. It is planned to extend this capability to support STANAG 4774.

M-Link controls which messages are allowed in a MUC room, by use of a security clearance, this is the DCS access control. M-Link can configure a Security Label Display Marking for each MUC room, which is used by Swift. This will generally be configured to match the Security Clearance and provides a helpful user experience.

M-Link can transform security labels, which is useful to map to systems running XEP-0258 and to provide STANAG 4774 policy transformation.

Cross Domain

Isode's XMPP cross domain solution is described in the white paper "Isode's XMPP Cross Domain Solution". The key components from a security label perspective:

1. M-Guard, Isode's XML Guard that provides secure unidirectional validation of XML messages, suitable for use across a domain boundary.
2. XMPP Application Profile, which specifies the XMPP standards allowed in stanzas sent over M-Guard and rules to constrain those standards. This includes the XMPP message formats specified in ADatP-4778.2 and rules for STANAG 4774 label checking, using exact match of labels allowed and other options.
3. M-Link Edge, which transfers XMPP stanzas to and from M-Guard. It can also perform STANAG 4774 label conversion between different policies.

This provides secure checking of STANAG 4774 labels in XMPP over a cross domain boundary.

Product Status / Plans

This section lists Isode products which have or have planned STANAG 4774 support.

Product	Version/Status
SPIF Editor	Shipped with M-Vault 19.1
Harrier	Planned for Harrier 4.2 (Q4 2025)
M-Switch	Planned for M-Switch 19.2 (Q1 2026)
M-Switch Edge (for mapping to M-Guard)	M-Switch Edge 19.1
MMHS Application Profile	Profile Available to run with M-Guard 1.5
Swift	Planned for Q4 2025
M-Link	Planned for future release
XMPP Application Profile	Profile Available to run with M-Guard 1.5

Conclusion

This white paper has shown how NATO labelling, including STANAG 4774 Confidentiality Labels are central to providing DCS and shows current and planned support in the Isode product set.

Isode

www.isode.com

14 Castle Mews, Hampton
Middlesex, TW12 2NP

Secure, Seamless Communication Solutions