STANDARD RELATED DOCUMENT

ADatP-4774.4

GENERATING ALTERNATIVE CONFIDENTIALITY METADATA LABELS

Edition A, Version 1

AUGUST 2024

NORTH ATLANTIC TREATY ORGANIZATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

6 August 2024

1. The enclosed Standard-related Document ADatP-4774.4, Edition A, Version 1 GENERATING ALTERNATIVE CONFIDENTIALITY METADATA LABELS, which has been approved in conjunction with ADatP-4774 by the nations in the Digital Policy Committee (DPC), is promulgated herewith.

2. ADatP-4774.4 Edition A, Version 1 is effective upon receipt.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database ((https://nso.nato.int/nso/) or through your national standardization authorities.

4. This publication shall be handled in accordance with C-M(2002)60.

FOR

Rob TRABUCCHI
Deputy Director
NATO Standardization Office

Thierry POULETTE
Major General, FRA (A)
Director, NATO Standardization Office

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.1. BACKGROUND

The Confidentiality Metadata Label Syntax (Reference [1]) defines a syntax for the representation of a confidentiality metadata label.

When a data object is created within a domain, the originator/creator of the data object assigns a confidentiality metadata label to the data object that is used to support access and release decisions for the data object.

The originator confidentiality metadata label is specified using values from confidentiality metadata labelling policy that is in force within the originating domain, and the systems and services within the originating domain are configured with access control policies that are written using the same confidentiality metadata labelling policy.

When the data object is exchanged with a coalition partner, it enters the coalition partner's domain where the systems and services are configured with access control policies that are written using the coalition partner's confidentiality metadata labelling policy (and not necessarily the originator confidentiality metadata labelling policy).

In order to ensure that the data object is handled correctly within the coalition partner's domain either:

1) The access control policies within the coalition partner's domain must be updated to process confidentiality metadata labels that use the originator's confidentiality metadata labelling policy; or
2) The data object must be assigned an additional confidentiality metadata label, using values from the coalition partner's confidentiality metadata labelling policy, which result in coequal security measures as required by the originator's confidentiality metadata label

1.2. OBJECTIVE

The objective of this document is to provide guidance on the mapping of an originator's confidentiality metadata label to an corresponding alternative confidentiality metadata label.

1.3. REQUIREMENT LEVELS

This document uses the keywords defined in RFC 2119 (Reference [12]) (e.g., SHALL, SHOULD, MAY) to define the requirement levels for specific parts of alternative confidentiality metadata label processing.

As this document is not a normative part of STANAG 4774, these keywords are only applicable to those nations that choose to adhere to this document.

1.4. METADATA

Table 1 provides a human readable summary of the NATO Core Metadata Specification (NCMS) metadata elements that are bound, in a machine readable form, to this document (mandatory metadata elements are highlighted in red).

Table 1: NCMS Metadata Elements

Metadata Element	Value
Originator Confidentiality Label/Marking	NATO UNCLASSIFIED *(PUBLIC UNMARKED upon promulgation)*
Metadata Confidentiality Label/Marking	NATO UNCLASSIFIED *(PUBLIC UNMARKED upon promulgation)*
Title	Generating Alternative Confidentiality Metadata Labels
Subject	Guidance on the mapping of an originator confidentiality metadata label to a corresponding alternative confidentiality metadata label.
Abstract	N/A
Identifier	urn:nato:stanag:4774:4:A:1
Version	EdA V1
Creator	NATO Communication and Information Agency (NCIA)
Date Created	June 16, 2023
Publisher	NATO Standardization Office (NSO)
Date Issued	*(Promulgation Date)*
Date Valid	*(NATO Effective Date)*
Language	ENG *(FRE for French/dual language version)*
References	urn:nato:stanag:4774:A:1 urn:nato:stanag:4774:1:A:1 urn:nato:stanag:4774:2:A:1
Replaces	N/A
Copyright	True
Rights Holder	North Atlantic Treaty Organization (NATO)
Rights	This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (https://nso.nato.int/nso/) or through your national standardization authorities.

Additional NCMS metadata elements, and COI metadata elements, may also be bound to this document.

CHAPTER 2 ALTERNATIVE CONFIDENTIALITY METADATA LABEL GENERATION

2.1. INTRODUCTION

An alternative confidentiality metadata label can be generated from an originator confidentiality metadata label (or possibly an alternative confidentiality metadata label) if there is a set of agreed coequal security measures between the confidentiality metadata labelling policy of the source confidentiality metadata label (originator or alternative) and the confidentiality metadata labelling policy of the new alternative confidentiality metadata label.

If there are no agreed policy elements defined between the two confidentiality metadata labelling policies that are semantically comparable and require coequal security measures, then an alternative confidentiality metadata label cannot be generated.

If semantically comparable policy elements are defined for both confidentiality metadata labelling policies, an alternative confidentiality may still not be able to be generated if the source confidentiality contains components that have not been identified in the mapping, or are specifically prohibited.

2.2. MAPPING

The generation of an alternative confidentiality metadata label from an originator confidentiality metadata label requires the mapping of all the elements of the originator confidentiality label (as shown in Figure 1).

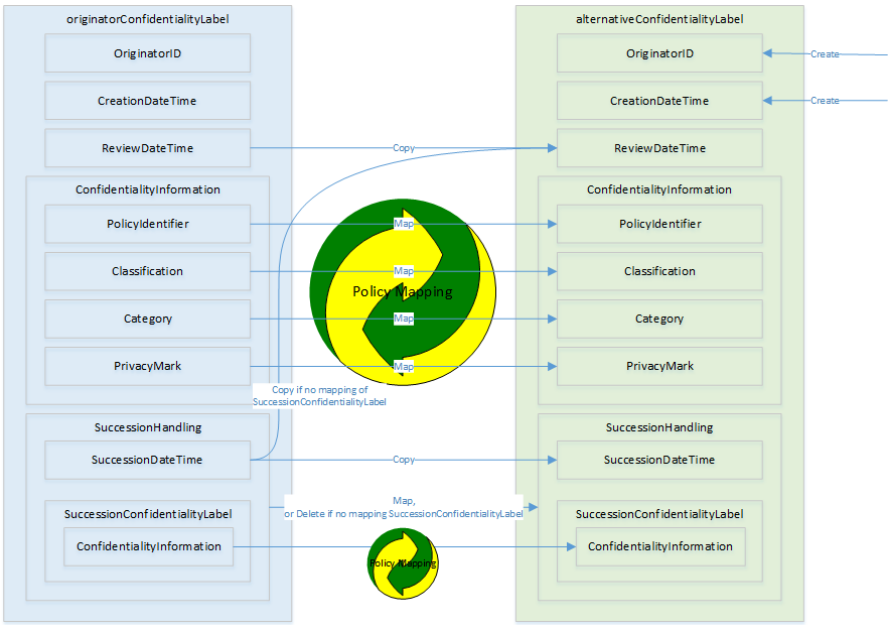

Figure 1: Mapping Between originatorConfidentialityLabel and alternativeConfidentialityLabel

This includes the following confidentiality metadata label elements:

- Confidentiality Information
- OriginatorID
- CreationDateTime
- ReviewDateTime
- SuccessionHandling

The mapping of each of these components is described in the following sections.

2.2.1. Confidentiality Information

The mapping of the confidentiality information element of a confidentiality metadata label is specific to the source and target metadata confidentiality labelling policies.

This mapping is discussed in more detail in section Chapter 3.

2.2.2. OriginatorID

The OriginatorID element of the originator confidentiality metadata label contains information about the originator of the confidentiality metadata label.

The OriginatorID element of the alternative confidentiality metadata label SHOULD reflect the system or individual that has performed the mapping from the originator confidentiality metadata label.

Originator Confidentiality metadata label

```
<ConfidentialityInformation>
  <PolicyIdentifier>
    NATO
  </PolicyIdentifier>
  <Classification>
    UNCLASSIFIED
  </Classification>
  <Category TagName=”Context”>
    <GenericValue>
      NATO
    </GenericValue>
  </Category>
  <OriginatorID
IDType=”uniformResoourceIdentifier”>
    https://www.ncia.nato.int/
  </OriginatorID>
</ConfidentialityInformation>
```

Alternative Confidentiality metadata label

```
<ConfidentialityInformation>
  <PolicyIdentifier>
    XXX
  </PolicyIdentifier>
  <Classification>
    OFFICIAL
  </Classification>
  <Category TagName=”Releasable to”>
    <GenericValue>
      NATO
    </GenericValue>
  </Category>
  <OriginatorID
    IDType=”directoryName”>
    cn=gateway1,ou=IEGB,o=NATO
  </OriginatorID>
</ConfidentialityInformation>
```

Figure 2: Mapping of OriginatorID from originatorConfidentialityLabel to an alternativeConfidentialityLabel

2.2.3. CreationDateTime

The CreationDateElement of the originator confidentiality metadata label expresses the date and time of the original classification by the originator.

The CreationDateElement of the alternative confidentiality metadata label SHOULD reflect the date and time of the generation of the alternative confidentiality metadata label.

Originator Confidentiality metadata label

```
<originatorConfidentialityLabel>
  <ConfidentialityInformation>
    <PolicyIdentifier>
      NATO
    </PolicyIdentifier>
    <Classification>
      UNCLASSIFIED
    </Classification>
    <Category
      TagName=”Context”>
      <GenericValue>
        NATO
      </GenericValue>
    </Category>
  </ConfidentialityInformation>
  <CreationDateTime>
    2022-05-26T16:22:46+01:00
  </CreationDateTime>
</originatorConfidentialityLabel>
```

Alternative Confidentiality metadata label

```
<alternativeConfidentialityLabel>
  <ConfidentialityInformation>
    <PolicyIdentifier>
      XXX
    </PolicyIdentifier>
    <Classification>
      OFFICIAL
    </Classification>
    <Category
      TagName=”Releasable to”>
      <GenericValue>
        NATO
      </GenericValue>
    </Category>
  </ConfidentialityInformation>
  <CreationDateTime>
    2022-10-19T13:46:05+01:00
  </CreationDateTime>
</alternativeConfidentialityLabel>
```

Figure 3: Mapping of CreationDateTime from originatorConfidentialityLabel to an alternativeConfidentialityLabel

2.2.4. ReviewDateTime

The ReviewDateTime element refers to the date the confidentiality metadata label should be reviewed.

Thus the ReviewDateTime element of the alternative confidentiality metadata label SHALL be the same as the ReviewDateTime element of the originator confidentiality metadata label.

See Figure 4 for an example mapping.

Originator Confidentiality metadata label

```
<originatorConfidentialityLabel>
  <ConfidentialityInformation
    ReviewDateTime=
    ”2027-05-26T16:22:46+01:00”>
    <PolicyIdentifier>
      NATO
    </PolicyIdentifier>
    <Classification>
      UNCLASSIFIED
    </Classification>
  </ConfidentialityInformation>
</originatorConfidentialityLabel>
```

Alternative Confidentiality metadata label

```
<alternativeConfidentialityLabel>
  <ConfidentialityInformation
    ReviewDateTime=
    ”2027-05-26T16:22:46+01:00”>
    <PolicyIdentifier>
      XXX
    </PolicyIdentifier>
    <Classification>
      OFFICIAL
    </Classification>
  </ConfidentialityInformation>
</alternativeConfidentialityLabel>
```

Figure 4: Mapping of ReviewDateTime from originatorConfidentialityLabel to an alternativeConfidentialityLabel

The ReviewDateTime element may not present in the originator confidentiality metadata label if a SuccessionHandling element is present.

In the event that an alternative SuccessorHandling element cannot be derived from the originator SuccessorHandling element (see section 2.6), then the ReviewDateTime element of the alternative confidentiality metadata label SHALL be set to the SuccessionDateTime element of the originator confidentiality metadata label. This will

indicate that the alternative confidentiality metadata label should be reviewed at the time when the successor confidentiality metadata label would have come in to force.

Figure 5 show the resulting alternative confidentiality metadata label when there is no valid mapping (from the “NATO” policy to the “XXX” policy) of the SuccessorConfidentialityLabel element in the originator confidentiality metadata label. In this case, the alternative confidentiality metadata label has no SuccessionHandling element, and a ReviewDateTime element with the time that the succession would have occurred.

Originator Confidentiality metadata label

```
<originatorConfidentialityLabel>
  <ConfidentialityInformation
    <PolicyIdentifier>
      NATO
    </PolicyIdentifier>
    <Classification>
      UNCLASSIFIED
    </Classification>
  </ConfidentialityInformation>
  <SuccessionHandling>
    <SuccessionDateTime>
      2027-10-19T14:05:32+01:00
    </SuccessionDateTime>
    <SuccessorConfidentialityLabel>
      <ConfidentialityInformation
        <PolicyIdentifier>
          PUBLIC
        </PolicyIdentifier>
        <Classification>
          UNMARKED
        </Classification>
      </ConfidentialityInformation>
    </SuccessorConfidentialityLabel>
  </SuccessionHandling>
</originatorConfidentialityLabel>
```

Alternative Confidentiality metadata label

```
<alternativeConfidentialityLabel>
  <ConfidentialityInformation
    ReviewDateTime=
    ”2027-10-19T14:05:32+01:00”>
    <PolicyIdentifier>
      XXX
    </PolicyIdentifier>
    <Classification>
      OFFICIAL
    </Classification>
  </ConfidentialityInformation>
</alternativeConfidentialityLabel>
```

Figure 5: Mapping of ReviewDateTime from SuccessionDateTime

2.2.5. SuccessionHandling

Originator Confidentiality metadata label

```
<originatorConfidentialityLabel>
  <ConfidentialityInformation
    <PolicyIdentifier>
      NATO
    </PolicyIdentifier>
    <Classification>
      UNCLASSIFIED
    </Classification>
  </ConfidentialityInformation>
  <SuccessionHandling>
    <SuccessionDateTime>
      2027-10-19T14:05:32+01:00
    </SuccessionDateTime>
    <SuccessorConfidentialityLabel>
      <ConfidentialityInformation
        <PolicyIdentifier>
          PUBLIC
        </PolicyIdentifier>
        <Classification>
          UNMARKED
        </Classification>
      </ConfidentialityInformation>
    </SuccessorConfidentialityLabel>
  </SuccessionHandling>
</originatorConfidentialityLabel>
```

Alternative Confidentiality metadata label

```
<alternativeConfidentialityLabel>
  <ConfidentialityInformation
    <PolicyIdentifier>
      XXX
    </PolicyIdentifier>
    <Classification>
      OFFICIAL
    </Classification>
  </ConfidentialityInformation>
  <SuccessionHandling>
    <SuccessionDateTime>
      2027-10-19T14:05:32+01:00
    </SuccessionDateTime>
    <SuccessorConfientialityLabel>
      <ConfidentialityInformation
        <PolicyIdentifier>
          XXX
        </PolicyIdentifier>
        <Classification>
          UNMARKED
        </Classification>
      </ConfidentialityInformation>
    </SuccessorConfidentialityLabel>
  </SuccessionHandling>
</alternativeConfidentialityLabel>
```

Figure 6: Mapping of SuccessionHandling

If an alternative SuccessorConfidentialityLabel cannot be derived from the originator SuccessorConfidentialityLabel (as a value is present that causes the mapping to be rejected), then no SuccessionHandling element SHALL be included in the alternative metadata confidentiality metadata label and the ReviewDateTime set as described in paragraph 2.5.

See Figure 5 above for an example.

2.3. GENERATION

An alternativeConfidentialityLabel SHOULD be generated from the originatorConfidentialityLabel.

In the event there is no valid mapping from the confidentiality metadata labelling policy of the originatorConfidentialityLabel, an alternativeConfidentialityLabel, that has a confidentiality metadata labelling policy that can be mapped to the required alternative confidentiality metadata labelling policy, MAY be used.

An alternativeConfidentialityLabel may be generated from an originatorConfidentialityLabel by:

- the originator who expects the data object to be transferred to another domain that is governed by a different confidentiality metadata labelling policy. The resulting alternativeConfidentialityLabel (or lack thereof) may influence the originatorConfidentialityLabel that the originator specifies.
- The originating domain, prior to transferring the data object to an external domain that is governed by a different confidentiality metadata labelling policy.
- The recipient domain, after receiving the data object from the originator's domains that is governed by a different confidentiality metadata labelling policy.

If an alternativeConfidentialityLabel with the required confidentiality metadata labelling policy is already bound to the data object, it is subject to local policy as to whether that alternativeConfidentialityLabel shall be used or replaced. For example, the local policy may take into account who generated the alternativeConfidentialityLabel (OriginatorID) or when the when alternativeConfidentialityLabel was generated (CreationDateTime).

2.4. BINDING

The alternativeConfidentialityLabel SHALL be bound to the same data object as the originatorConfidentialityLabel from which is derived using an ADatP-4778 (Reference 4-1[4]) compliant metadata binding.

The originatorConfidentialityLabel (OCL) will be bound to the data object by the originator. If the originator also generates an alternativeConfidentialityLabel (ACL), then it SHOULD be held within the same binding.

If an alternativeConfidentialityLabel (ACL) is generated by an entity other than the originator, it SHOULD be bound to the same data object by the entity performing the generation of the ACL.

The alternative confidentiality metadata label SHALL be placed into a separate metadata binding container and bound to the same data objects as the corresponding originator confidentiality metadata label. This approach ensures integrity and authenticity of the originator's metadata binding.

Figure 7 shows how this approach is applied to encapsulating, embedded and detached bindings.

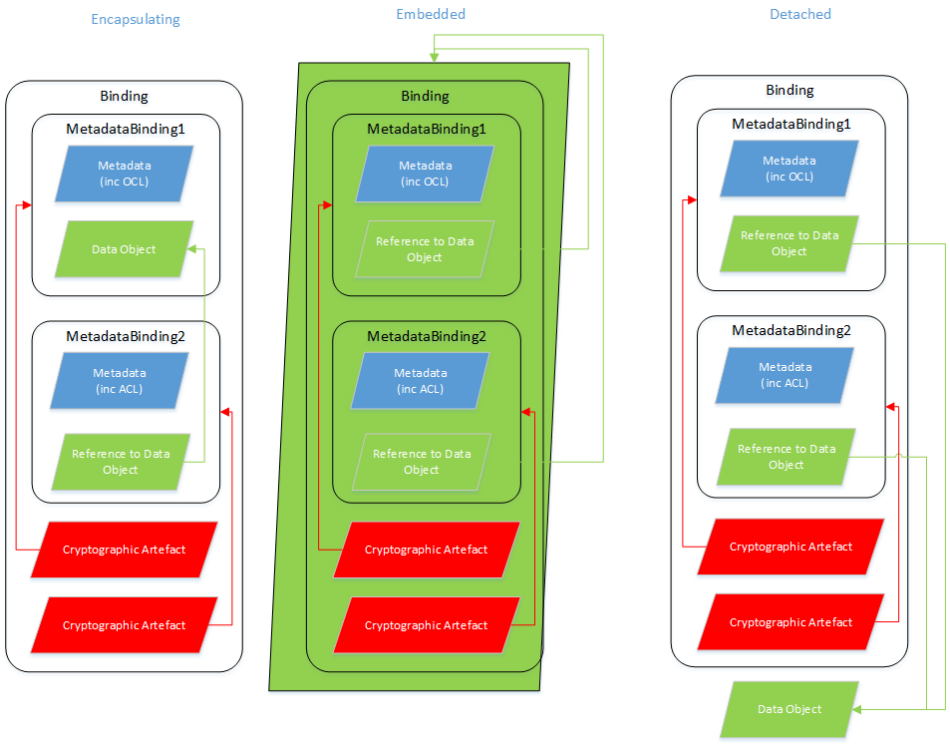

Figure 7: Binding of an alternativeConfidentialityLabel (ACL), generated by an entity other than the originator, to a Data Object

A separate Signature within the BindingInformation provides integrity and authentication for the binding containing the alternativeConfidentialityLabel.

CHAPTER 3 GENERATING ALTERNATIVE CONFIDENTIALITY METADATA LABELS

3.1. INTRODUCTION

In order to generate an alternative confidentiality metadata label from a source confidentiality metadata label, equivalencies must exists between the two confidentiality metadata labelling policies. Specifically semantically comparable mappings must be specified for the components of the ConfidentialityInformation element of the confidentiality metadata label:

- PolicyIdentifier
- Classification
- PrivacyMark
- Category

These mappings can then be used to generate an alternative confidentiality with the corresponding values.

The semantically comparable mappings are captured using a template which simplifies the process of capturing the equivalencies between the NATO confidentiality metadata labelling policy and a National confidentiality metadata labelling policy.

The intent is not to capture the complete National confidentiality metadata labelling policy, but rather only those elements that have an equivalence with the NATO confidentiality metadata labelling policy.

This requires at least semantically comparable mappings between the mandatory PolicyIdentifier and Classification elements which will be exchanged between NATO and the Nation.

In this case, any categories present in a confidentiality metadata label would cause the generation of an alternative confidentiality metadata label to fail (as the confidentiality metadata label contains values which cannot be mapped to equivalent values).

At a more detailed level, the mappings can be considered between Categories.

A common Category is a “Releasable to” (or similar) category that allows the dissemination of information to entities beyond the set of entities implied by the PolicyIdentifier. For example “NU” information can be disseminated to all NATO Nations, whilst “NU Releasable to Ukraine” information can be disseminated to all NATO Nations and Ukraine. Where a National policy contains a “Releasable to” (or similar) Category, the mappings with the NATO policy could be defined.

When capturing semantically comparable mappings between Categories, there may be no fitting values in the destination (alternative) confidentiality metadata labelling policy for a given category value. In this case, the presence of the category value would cause the generation of an alternative confidentiality metadata label to fail. However, when defining the semantically comparable mappings, it may be agreed that the value does not need to be mapped to a corresponding value, and it is acceptable for the value to be discarded.

This is most likely for informative Categories (which are not considered in the access control decision function) and permissive Categories that are used to extend the dissemination of information. It is highly unlikely that restrictive Category values will be discarded.

3.2. TEMPLATE

In order to consistently capture the semantically comparable mappings between the NATO confidentiality metadata labelling policy and a National confidentiality metadata labelling policy, a template is provided in the form of an Excel workbook (Reference IEPD:4774.4#template) (see Figure 8).

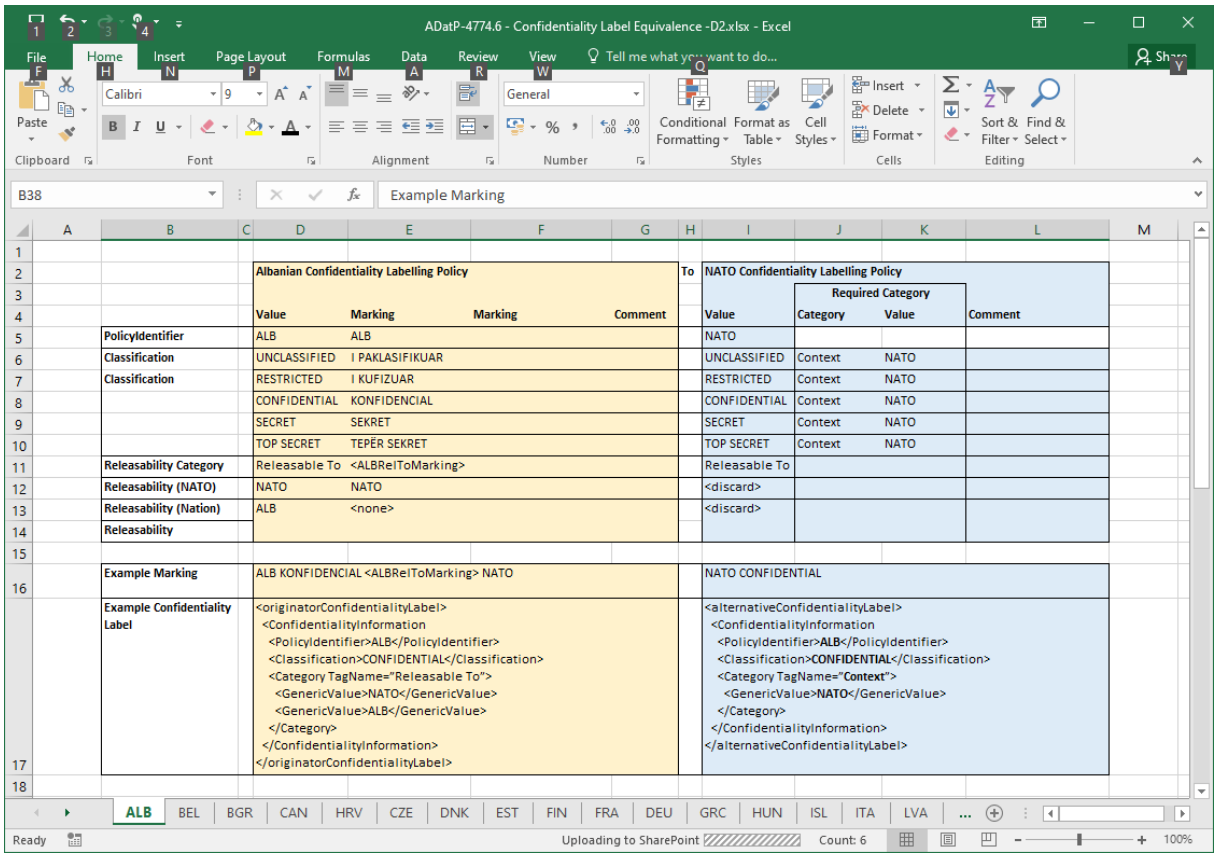

Figure 8: Example Equivalence Template

This template is further described in ANNEX A.

3.3. SAMPLE EQUIVALENCES

Using the workbook template a fictitious sample with equivalences have been developed between NATO and Framland[1] and included as Annex B within this document.

Actual semantically comparable mappings between NATO and other security policies are maintained in a separate document by the NATO Information Management Authority.

3.4. SECURITY POLICY INFORMATION FILE

A Security Policy Information File (SPIF) can be used to capture a machine readable representation of a confidentiality metadata labelling policy, including the value domains for use within a confidentiality metadata label (see Chapter 3 of Reference [2] for more details).

The SPIFs defined by this document do not contain a complete description of the National confidentiality metadata labelling policy, but only those values which has an corresponding value with the NATO confidentiality metadata labelling policy (and vice versa).

They are to be used solely to the generation of alternative confidentiality metadata labels and not to be used for generating national originator confidentiality metadata labels.

Where a nation already captures their national confidentiality metadata labelling policy as a SPIF, the national SPIF will be referenced where appropriate.

[1] Framland is a fictitious non-NATO Nation taken from NATO's Skolkan exercise setting developed by the Joint Warfare Centre (JWC).

INTENTIONALLY BLANK

CHAPTER 4 REFERENCE MATERIALS

4.1. REFERENCES

[1] ADatP-4774 “Confidentiality Metadata Label Syntax”, Edition A Version 1, 20th December 2017

[2] ADatP-4774.1 “Confidentiality Metadata Label Syntax (CMLS) – Implementation Guidance” Edition A Version 1 November 2021

[3] ADatP-4774.2 “Guidance on the Digital Labelling of NATO Information”, Edition A, Version 1, 1st June 2021

[4] ADatP-4778 “Metadata Binding Mechanism”, Edition A, Version 1, October 2018.

[5] AC/35-D/1002-REV10(INV) “NATO Security Classifications with their National Equivalents”, 3rd March 2023

[6] RFC 3114 “Implementing Company Classification Policy with the S/MIME Security Label”, W. Nicolls, May 2002

[7] ADatP-5653 “NCDF Part IV: Information Exchange Package Documentation Specification” Edition A, Verion1, Draft 0.2 February 2022

[8] X.411 “Information Technology – Message Handling Systems (MHS): Message Transfer System: Abstract Service Definition and Procedures” International Telecommunication Union (ITU) 18th June 1999

[9] RFC 2634 “Enhanced Security Service for S/MIME”, P Hoffman, Editor, Request for Comments 2634, Network Working Group, Internet Engineering Task Force June 1999

[10] BG-BOD-D-2014-0262-REV4-NR-REL “BICES Group BICES Standard Operating Procedure for Protective Security Markings Version 2.5”, July 2020, NATO RESTRICTED Releasable To Australia, Austria, Finland, Ireland, New Zealand, Switzerland, EU

[11] AC/322-N(2011)0130 “Guidance on the Marking of NATO Information”, Consultation, Command and Control Board (C3B), 16 June 20211.

[12] IETF RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels”, at http://tools.ietf.org/html/rfc2119, March 1997.

4.2. INFORMATION EXCHANGE PACKAGE DOCUMENTATION

4.2.1. Introduction

This standardization document refers to machine-readable artefacts contained within one or more Information Exchange Package Documentation (IEPDs) (Reference [7]) that have been published as part of a standard or standard-related document, including this document.

A reference to an machine-readable artefact is of the following form:

IEPD:<iepdPrefix>'#'<artefactId>

where:

i. *iepdPrefix* is a prefix identified for an IEPD in Table 2
ii. *artefactID* identifies an artefact through its id attribute in the IEPD catalogue.

For example,

(Reference IEPD:4774.4#template)

identifies an artefact in the IEPD that has an identifier of template.

4.2.2. IEPDS

Table 2: IEPD Summary Table

Prefix	Title	Identifier	Version
4774.4	Generating Alternative Confidentiality Metadata Labels	urn:nato:stanag:4774:4:A:1:iepd:alternative.xfr	1.0

4.2.2.1. Checksums

A checksum has been generated over the IEPD zip package which may be used to verify the integrity of IEPD.
The checksum (SHA256) for the IEPDs are shown SRD in Table 3

Table 3: IEPD Checksums.

IEPD	Checksum
4774.4	141bc5b17c8ece11c2be1eaed5df4cc785d53f9e287365ab2846e3276a02bcd5

In order to verify the integrity of the IEPD, a new checksum should be generated for the IEPD zip package obtained, and compared to this value. If the values are the same, then the IEPD is the one to which this SRD relates.

A checksum can be generated using various tools and a range of platforms. For example, on the Windows platform the certutil utility could be used:

```
> certutil -hashfile '.\ADatP-4774.4 EDA V1 XFR.iepd' SHA256
SHA256 hash of .\ADatP-4774.4 EDA V1 XFR.iepd:
141bc5b17c8ece11c2be1eaed5df4cc785d53f9e287365ab2846e3276a02bcd5
CertUtil: -hashfile command completed successfully.
>
```

4.2.3 Artefacts

Identifier	Description
template	An Excel workbook containing a mapping template worksheet, and a worksheet for the sample mappings between the policies of NATO and Framland.
pol-xfr	An XML SPIF containing a subset of the Framland confidentiality metadata label policy with semantic mappings to the NATO confidentiality metadata labelling policy.
pol-nato	An XML SPIF containing the NATO confidentiality metadata label policy with semantic mappings to the Framland confidentiality metadata labelling policy.

INTENTIONALLY BLANK

ANNEX A LABELLING POLICY MAPPING TEMPLATE

A.1. INTRODUCTION

A template in the form of a Microsoft Excel workbook (Reference IEPD:4774.4#template) is provided with this document and can be used to capture the mapping of corresponding components and values between the NATO confidentiality metadata labelling policy and national confidentiality metadata labelling policy.

The template can be used to capture the necessary and sufficient details of the national confidentiality metadata labelling policy that have an equivalency with the NATO policy.

This template captures the details of:

- the identifier to be used to identify a national confidential label; to
- the classifications of the national confidentiality metadata labelling policy;
- the security category within the national confidentiality metadata labelling which allows the dissemination of national confidentiality metadata labelled information to other entities (e.g. NATO);
- details of the corresponding phrases that will be used to display a national confidentiality metadata label in a human readable form; and
- the mappings between the national confidentiality metadata labelling policy values and the NATO confidentiality metadata labelling policy values.

The template may also be used to capture details of additional the national confidentiality metadata labelling policy security categories whose values may be safely discarded or have a mapping to an equivalent NATO security category value.

This template does not capture details of any privacy marks used by a national confidentiality metadata labelling policy, as the privacy mark is an informative component of the confidentiality metadata label which is not used when making an access control decision. The default assumption is that all privacy marks can be discarded when generating an alternative confidentiality label.

The template is not intended to capture the complete details of a national confidentiality metadata labelling policy, but just the necessary and sufficient details to support mapping of corresponding components and values with NATO confidentiality metadata labelling policy.

The template is primarily aimed at capturing the equivalencies with confidentiality metadata labelling policy of a NATO Nation, but it can also be used to capture equivalencies with the confidentiality metadata labelling policy of a non-NATO nation, or any another entity, with which NATO has signed a security agreement.

The template is divided into two sections:

1. National Confidentiality metadata labelling Policy to NATO Confidentiality metadata labelling Policy
2. NATO Confidentiality metadata labelling Policy to National Confidentiality metadata labelling Policy

A.2. National Confidentiality metadata labelling Policy to NATO Confidentiality metadata labelling Policy

The first section of the template captures the values domains of the national confidentiality metadata labelling policy and specifies the corresponding components and values with the NATO confidentiality metadata labelling policy.

A.2.1. Value Domains

The value domains that are captured to support equivalency mapping with the NATO confidentiality metadata labelling policy are:

- the policy identifier [mandatory]
- the classification [mandatory]
- the releasability category [optional].

		Framland Confidentiality Labelling Policy			
		Value	**Marking**	**Marking**	**Comment**
PolicyIdentifier		XFR	XFR		
Classification		*RESTRICTED*	KÄYTTÖ RAJOITETTU Suojaustaso IV		
		CONFIDENTIAL	LUOTTAMUKSELLINEN Suojaustaso III		
		SECRET	SALAINEN Suojaustaso II		
		TOP SECRET	ERITTÄIN SALAINEN Suojaustaso I		
Releasability Category		*Releasable To*	*<XFRRelToMarking>*		
Releasability (NATO)		*NATO*	*NATO*		
Releasability (Nation)		*XFR*			
Releasability					

Figure 9: Example National Confidentiality metadata labelling Policy Value Domains

A.2.1.1 Policy Identifier

The PolicyIdentifier value (*Value* column) identifies the confidentiality metadata labelling policy to which a confidentiality metadata label relates, and consequently the valid value domains for the classifications and category values within the confidentiality metadata label.

It is recommended to use a value that is already assigned to the nation to avoid conflict with other policy identifiers.

The policy identifier value may be rendered in human readable markings in a variety of languages, and these are specified in the *Marking* columns.

A.2.1.2. Classifications

The national policy classification values are listed in the “Classification” section. These values should reflect the classifications that have been identified in the security agreement with NATO. In addition, an UNCLASSIFIED value may also be included.

It is recommended that the same value domain defined in both X.411 (Reference [8]) and RFC 2634 (Reference [9]) is used wherever possible for the Classification value domain. The national language(s) classification markings of the classification values should be specified in the Marking column.

Where a national classification does not align with the X.411/RFC 2634 value domain (e.g. OFFICIAL (UK)) then an appropriate value should be defined[2].

Note, the classification value domain to be used in the national confidentiality metadata label is entirely at the discretion of the nation.

A.2.1.3. Categories

It is assumed that the national confidentiality metadata labelling policy will include a category that allows the dissemination of nationally confidentiality metadata labelled information beyond the nation e.g. to allow the dissemination of national information to NATO. (The NATO confidentiality metadata labelling policy has a category called “Releasable To” to support such dissemination to, for example, non-NATO nation.)

This information is not mandatory, but providing details will improve the equivalency mapping between confidentiality metadata labels and support onward exchange of information with a third party.

The *Releasability Category* identifies the name of the category (the type is assumed to be “PERMISSIVE”).

The *Releasability (NATO)* identifies the *Releasability Category* value that allows information to be disseminated to NATO.

The *Releasability (Nation)* identifies the *Releasability Category* value that allows information to be disseminated with the nation. This is required when other releasability values are present to support the access control decision. In general,

[2] The classification hierarchy is not captured by the template as it is not used when defining equivalent confidentiality labels.

this value is not shown in a human readable marking and consequently have a blank marking phrase.

Additional releasability values may specified which may, in turn, be mapped to the equivalent NATO confidentiality metadata label (Releasable to category) values. For example, values that represent non-NATO nations.

Other categories of the national confidentiality metadata labelling policy are not captured by this template[3].

A.2.1.4. Summary

In summary, the section identifies the value domains of the national policy which will be used in a national confidentiality metadata label, as shown in Figure 10

Example Marking	XFR LUOTTAMUKSELLINEN Suojaustaso III <XFRRelToMarking> NATO
Example Confidentiality Label	<originatorConfidentialityLabel> <ConfidentialityInformation> <PolicyIdentifier>XFR</PolicyIdentifier> <Classification>CONFIDENTIAL</Classification> <Category TagName="Releasable To"> <GenericValue>NATO</GenericValue> <GenericValue>XFR</GenericValue> </Category> </ConfidentialityInformation> </originatorConfidentialityLabel>

Figure 10: Example Confidentiality metadata label using the National Value Domains

A.2.2. Equivalencies

The national value domains identified in section A.2.1. are then mapped to the corresponding values in the NATO confidentiality metadata labelling policy.

	Framland Confidentiality Labelling Policy				To	NATO Confidentiality Labelling Policy			
							Required Category		
	Value	Marking	Marking	Comment		Value	Category	Value	Comment
PolicyIdentifier	XFR	XFR				NATO			
Classification	*RESTRICTED*	KÄYTTÖ RAJOITETTU Suojaustaso IV				RESTRICTED	Context	NATO	
	CONFIDENTIAL	LUOTTAMUKSELLINEN Suojaustaso III				CONFIDENTIAL	Context	NATO	
	SECRET	SALAINEN Suojaustaso II				SECRET	Context	NATO	
	TOP SECRET	ERITTÄIN SALAINEN Suojaustaso I				TOP SECRET	Context	NATO	
Releasability Category	*Releasable To*	*<XFRRelToMarking>*				Releasable To			
Releasability (NATO)	*NATO*	*NATO*				<discard>			
Releasability (Nation)	*XFR*					<discard>			
Releasability									

Figure 11: Equivalencies between a National Confidentiality metadata labelling Policy and the NATO Confidentiality metadata labelling.

[3] Some nations may make use of some additional categories. These categories will be captured by extending the template.

A.2.1.1 Policy Identifier

The national policy identifier is mapped to the NATO policy identifier.

A.2.1.2. Classifications

The national classification values are mapped to the NATO classification values in accordance with the corresponding security agreement, which is summarized in Reference [5].

When mapping to a NATO confidentiality metadata label, a Context category value is required (see section 3.4, Reference [3]). For all mappings to the NATO confidentiality metadata labelling policy from a National confidentiality metadata labelling policy, the Context value SHALL be 'NATO', as the national confidentiality metadata label is only disseminating the information to NATO, and not to an extended context.

A.2.1.3. Categories

The national confidentiality metadata labelling policy category values are mapped to the NATO confidentiality metadata labelling policies.

Specifically, the national releasability category values, if defined, are mapped to the NATO Releasable To category (see section 3.5 of Reference [3]).

For a NATO nation, both the *Releasability (NATO)* and *Releasability (Nation)* values will not be mapped to a value in the NATO Releasable to category as:

(a) dissemination to both is implied by the PolicyIdentifer of "NATO", and

(b) NATO nations do not have a valid value within the NATO *Releasable to* category.

For a non-NATO nation, both the *Releasability (NATO)* and *Releasability (Nation)* will be mapped to corresponding values in the NATO Releasable to category.

All other category values will cause the generation of an alternative confidentiality metadata label in the NATO confidentiality metadata labelling policy to fail.[4] For example, the confidentiality metadata label in Figure 12 contains a category (Additional) for which no mapping is defined and consequently there is no valid confidentiality metadata label in the NATO confidentiality metadata labelling policy.

[4] In the future, the mapping may cover other categories.

Example Marking	XFR LUOTTAMUKSELLINEN Suojaustaso III <XFRRelToMarking> NATO CLOSEHOLD
Example Confidentiality Label	<originatorConfidentialityLabel> <ConfidentialityInformation> <PolicyIdentifier>XFR</PolicyIdentifier> <Classification>CONFIDENTIAL</Classification> <Category TagName="Releasable To"> <GenericValue>NATO</GenericValue> <GenericValue>XFR</GenericValue> </Category><Category TagName="Other"> <GenericValue>CLOSEHOLD</GenericValue> </Category> </ConfidentialityInformation> </originatorConfidentialityLabel>

Figure 12: Confidentiality metadata label with no equivalent relation in the NATO Confidentiality metadata labelling Policy

A.3. NATO Confidentiality metadata labelling Policy to National Confidentiality metadata labelling Policy

The second section of the template captures the relations between the NATO confidentiality metadata labelling policy (specified in Reference [3] and the national confidentiality metadata labelling policy, specified in the first section of the template.

A.3.1. Value Domains

The value domains for the NATO Confidentiality metadata label are drawn from Reference [3], and are just the sufficient values for mapping to National confidentiality metadata labelling policies.

Specifically, the PolicyIdentifier, Classifications and the required values[5] from the Releasable To category.

	NATO Confidentiality Labelling Policy			
	Value	**Marking (en)**	**Marking (fr)**	**Comment**
PolicyIdentifier	NATO	NATO		
Classification	RESTRICTED	RESTRICTED	DIFFUSION RESTREINTE	
	CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIEL	
	SECRET	SECRET	SECRET	
	TOP SECRET	TOP SECRET	TRÈS SECRET	
Releasability Category	Releasable to	Releasable to		
Releasability	CHE			

Figure 13: NATO Confidentiality metadata labelling Policy Valued Domains for Mapping

[5] Providing all the valid values in the template significantly increases it complexity and many national confidentiality metadata labelling policies may only have a sparse mapping.

The template does not contain the other NATO confidentiality metadata labelling categories as they are not considered for the mapping.

A.3.2. Mapping of policy elements

The relations between the NATO value domains and the national confidentiality metadata labelling value domains are identified in section A.2.

		NATO Confidentiality Labelling Policy				To	Framland Confidentiality Labelling Policy			
								Required Category		
		Value	Marking (en)	Marking (fr)	Comment		Value	Category	Value	Comment
PolicyIdentifier		NATO	NATO				XFR			
Classification		UNCLASSIFIED	UNCLASSIFIED	SANS CLASSIFICATION			RESTRICTED	Releasable To	NATO	
								Releasable To	XFR	
		RESTRICTED	RESTRICTED	DIFFUSION RESTREINTE			RESTRICTED	Releasable To	NATO	
								Releasable To	XFR	
		CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIEL			CONFIDENTIAL	Releasable To	NATO	
								Releasable To	XFR	
		SECRET	SECRET	SECRET			SECRET	Releasable To	NATO	
								Releasable To	XFR	
		TOP SECRET	TOP SECRET	TRÈS SECRET			TOP SECRET	Releasable To	NATO	
								Releasable To	XFR	
Releasability Category		Releasable To	Releasable To				Releasable To	Releasable To		
Releasability										

Figure 14: Equivalency between NATO and National Confidentiality metadata labelling Policies

A.3.2.1. PolicyIdentifier

The NATO policy identifier is simply mapped to the national policy identifier.

A.3.2.2 Classifications

The NATO classification values are mapped to corresponding national classification values, in alignment with Reference [5].

Where Reference [5] indicates that there is no national equivalent or the security agreement does not specify explicit handling instructions, the mapping shall be the value identified for the next higher NATO classification for which a national equivalent is defined.

If the national confidentiality metadata labelling policy supports a “Releasable to” category, then the NATO classification should also be mapped to “Releasable to” category values representing both NATO and the nation.

A3.3.3 Categories

All NATO Releasable To category values with a confidentiality metadata label will be discarded unless they have a corresponding mapping in the national confidentiality labelling policy identified in section A.2. For example, the value “CHE” in the NATO Releasable To category may be mapped to a value “SWITZERLAND” in the national confidentiality metadata labelling policy.

All NATO “Context” category values will be discarded[6].

All other category set values will cause the generation of an alternative confidentiality metadata label in the national confidentiality metadata labelling policy to fail.[7]

For example, the confidentiality metadata label in Figure 15 contains a category (Administrative) for which no mapping is defined and consequently there is no valid confidentiality metadata label in the national confidentiality metadata labelling policy.

Example Confidentiality Label	<originatorConfidentialityLabel> <ConfidentialityInformation <PolicyIdentifier>**NATO**</PolicyIdentifier> <Classification>**SECRET**</Classification> <Category TagName=”**Context**”> <GenericValue>**NATO**</GenericValue> </Category> <Category TagName=”Administrative”> <GenericValue>**MEDICAL**</GenericValue> </Category> </ConfidentialityInformation> </originatorConfidentialityLabel>	

Figure 15: NATO Confidentiality metadata label Containing Unmapped Categories

[6] The Context values may be mapped to “Releasable To” values, but this is for further study.
[7] In the future, the mapping may cover categories other than “Releasable To”

ANNEX B: Mapping of Framland (XFR) and NATO Confidentiality metadata labelling policies

B.1. Framland to NATO

	Framland Confidentiality Labelling Policy				To	NATO Confidentiality Labelling Policy			
							Required Category		
	Value	Marking (fr)	Marking	Comment		Value	Category	Value	Comment
PolicyIdentifier	XFR	XFR				NATO			
Classification	*RESTRICTED*	KÄYTTÖ RAJOITETTU Suojaustaso IV				RESTRICTED	Context	NATO	
	CONFIDENTIAL	LUOTTAMUKSELLINEN Suojaustaso III				CONFIDENTIAL	Context	NATO	
	SECRET	SALAINEN Suojaustaso II				SECRET	Context	NATO	
	TOP SECRET	ERITTÄIN SALAINEN Suojaustaso I				TOP SECRET	Context	NATO	
Releasability Category	*Releasable To*	*<XFRRelToMarking>*				Releasable To			
Releasability (NATO)	*NATO*	*NATO*				<discard>			
Releasability (Nation)	XFR					<discard>			
Releasability									

Example Marking	XFR LUOTTAMUKSELLINEN Suojaustaso III <XFRRelToMarking> NATO		NATO CONFIDENTIAL
Example Confidentiality Label	<originatorConfidentialityLabel> <ConfidentialityInformation> <PolicyIdentifier>XFR</PolicyIdentifier> <Classification>CONFIDENTIAL</Classification> <Category TagName="Releasable To"> <GenericValue>NATO</GenericValue> <GenericValue>XFR</GenericValue> </Category> </ConfidentialityInformation> </originatorConfidentialityLabel>		<alternativeConfidentialityLabel> <ConfidentialityInformation> <PolicyIdentifier>**NATO**</PolicyIdentifier> <Classification>**CONFIDENTIAL**</Classification> <Category TagName="**Context**"> <GenericValue>**NATO**</GenericValue> </Category> </ConfidentialityInformation> </alternativeConfidentialityLabel>

B.2 NATO to Framland

	NATO Confidentiality Labelling Policy				To	Framland Confidentiality Labelling Policy			
							Required Category		
	Value	Marking (en)	Marking (fr)	Comment		Value	Category	Value	Comment
PolicyIdentifier	NATO	NATO				XFR			
Classification	UNCLASSIFIED	UNCLASSIFIED	SANS CLASSIFICATION			RESTRICTED	Releasable To	NATO	
							Releasable To	XFR	
	RESTRICTED	RESTRICTED	DIFFUSION RESTREINTE			RESTRICTED	Releasable To	NATO	
							Releasable To	XFR	
	CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIEL			CONFIDENTIAL	Releasable To	NATO	
							Releasable To	XFR	
	SECRET	SECRET	SECRET			SECRET	Releasable To	NATO	
							Releasable To	XFR	
	TOP SECRET	TOP SECRET	TRÈS SECRET			TOP SECRET	Releasable To	NATO	
							Releasable To	XFR	
Releasability Category	Releasable To	Releasable To				Releasable To	Releasable To		
Releasability									

Example Marking	NATO SECRET	XFR SALAINEN Suojaustaso II <XFRRelToMarking> NATO
Example Confidentiality Label	<originatorConfidentialityLabel> <ConfidentialityInformation> <PolicyIdentifier>**NATO**</PolicyIdentifier> <Classification>**SECRET**</Classification> <Category TagName="**Context**"> <GenericValue>**NATO**</GenericValue> </Category> </ConfidentialityInformation> </originatorConfidentialityLabel>	<alternativeConfidentialityLabel> <ConfidentialityInformation> <PolicyIdentifier>XFR</PolicyIdentifier> <Classification>SECRET</Classification> <Category TagName="Releasable To"> <GenericValue>NATO</GenericValue> <GenericValue>XFR</GenericValue> </Category> </ConfidentialityInformation> </alternativeConfidentialityLabel>

B.3. Notes

The mapping is derived from Reference [5] and the unclassified values derived from Reference [10].

A machine readable version of the national policy, together with mappings to the NATO policy is available at Reference IEPD:4774.4#pol-xfr.

A machine readable version of the NATO policy with mappings to the national policy is available at Reference IEPD:4774.4#pol-nato.

[Draft The nation is requested to review and update the mapping as appropriate, including both the STANAG 4774 value domains and associated markings.]

ADatP-4774.4(A)(1)

Edition A Version 1