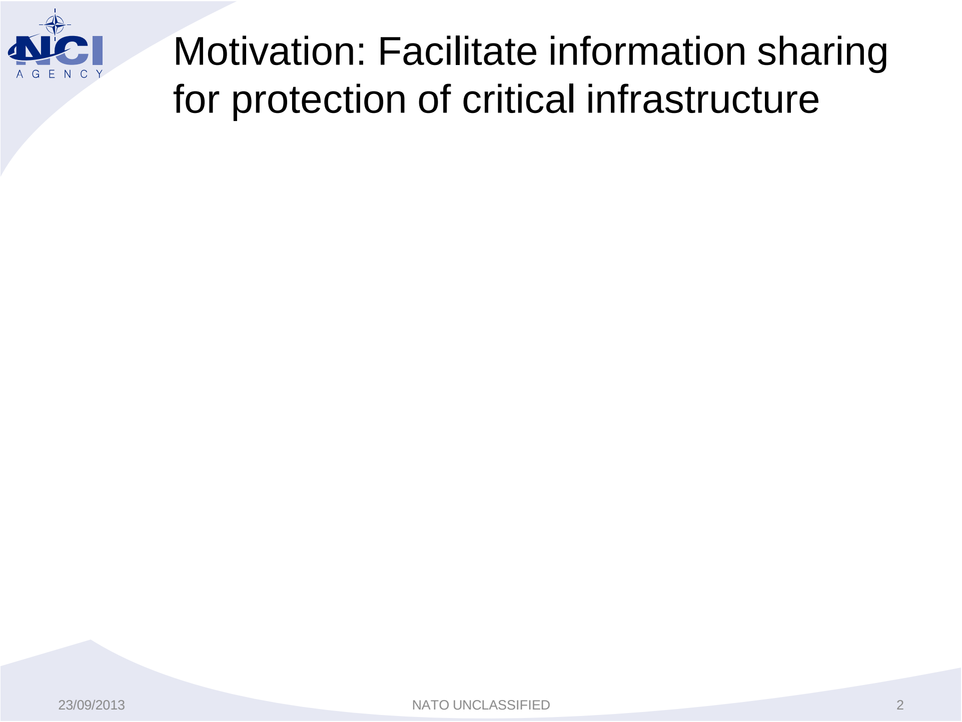
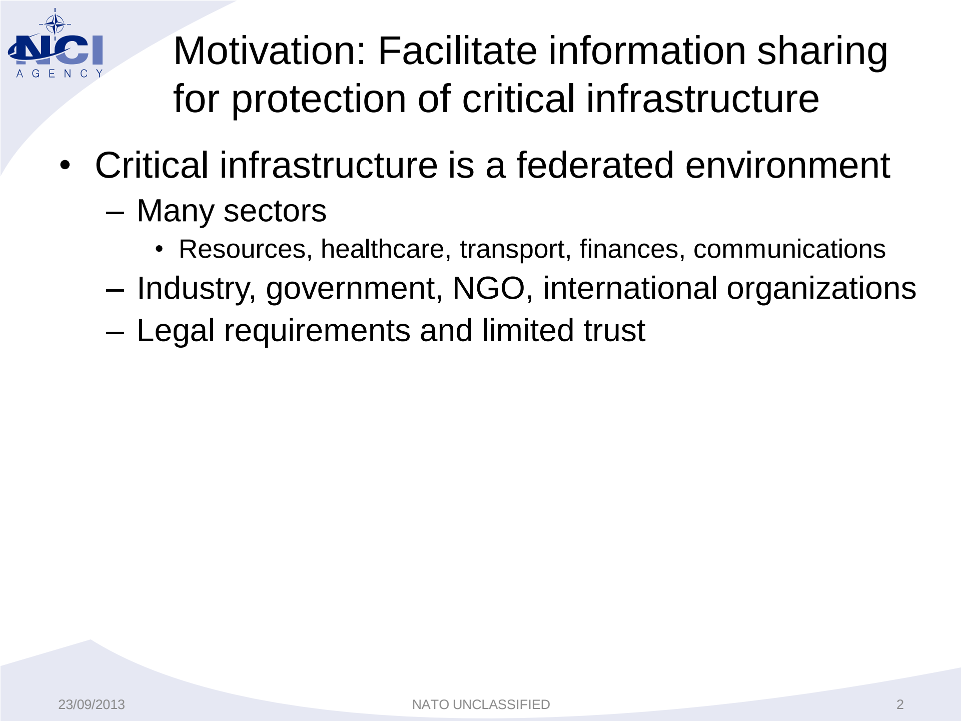
NATO Communications and Information Agency

Using NATO Labelling to support controlled information sharing between partners

Sander Oudkerk*, Konrad Wrona^
*Agent Sierra Consultancy Services
^NATO Communications and Information Agency



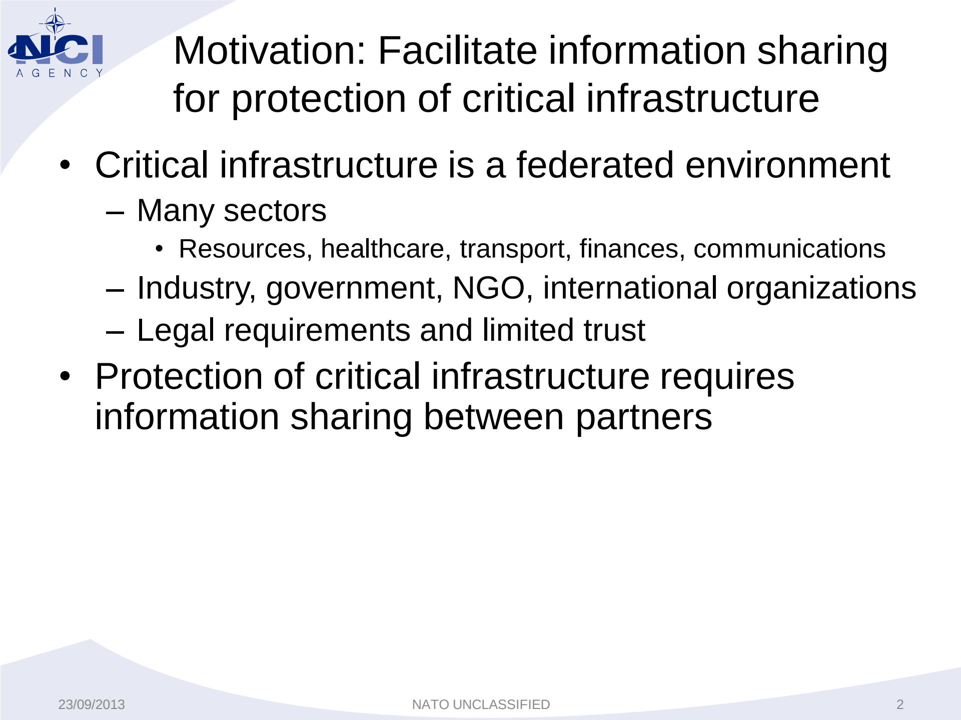
Motivation: Facilitate information sharing for protection of critical infrastructure



Motivation: Facilitate information sharing for protection of critical infrastructure

- Critical infrastructure is a federated environment
  - – Many sectors
    - Resources, healthcare, transport, finances, communications
  - – Industry, government, NGO, international organizations
  - – Legal requirements and limited trust

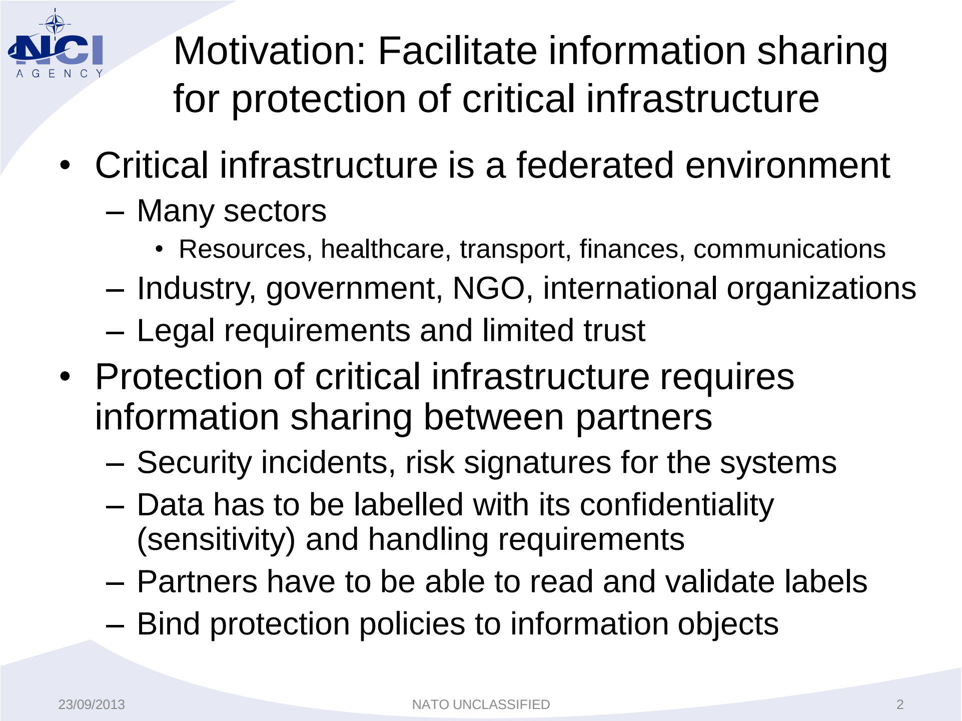
23/09/2013 NATO UNCLASSIFIED 2



Motivation: Facilitate information sharing for protection of critical infrastructure

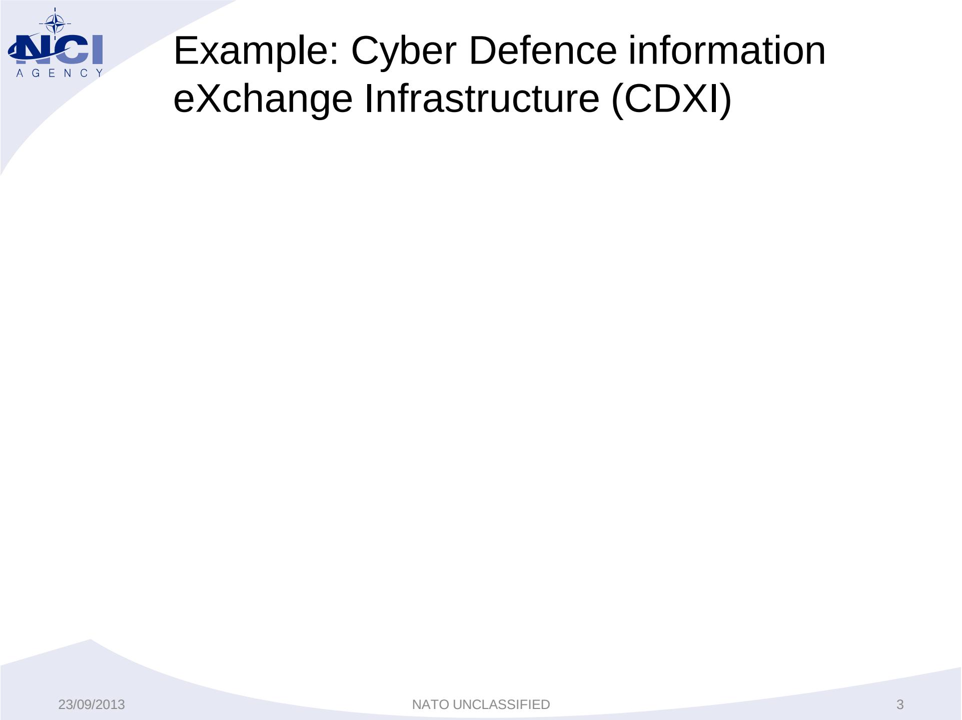
- Critical infrastructure is a federated environment
  - – Many sectors
    - Resources, healthcare, transport, finances, communications
  - – Industry, government, NGO, international organizations
  - – Legal requirements and limited trust
- Protection of critical infrastructure requires information sharing between partners

23/09/2013 NATO UNCLASSIFIED 2



Motivation: Facilitate information sharing for protection of critical infrastructure

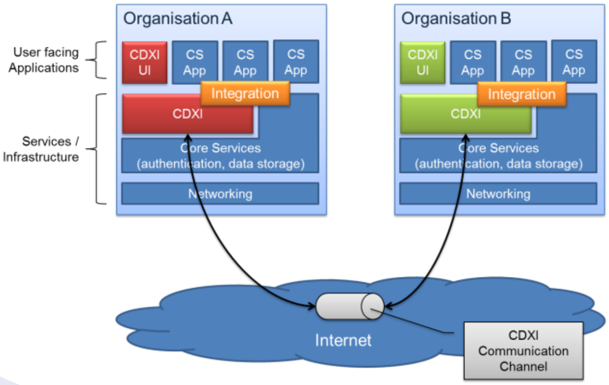
- Critical infrastructure is a federated environment
  - Many sectors
    - Resources, healthcare, transport, finances, communications
  - Industry, government, NGO, international organizations
  - Legal requirements and limited trust
- Protection of critical infrastructure requires information sharing between partners
  - Security incidents, risk signatures for the systems
  - Data has to be labelled with its confidentiality (sensitivity) and handling requirements
  - Partners have to be able to read and validate labels
  - Bind protection policies to information objects



Example: Cyber Defence information eXchange Infrastructure (CDXI)

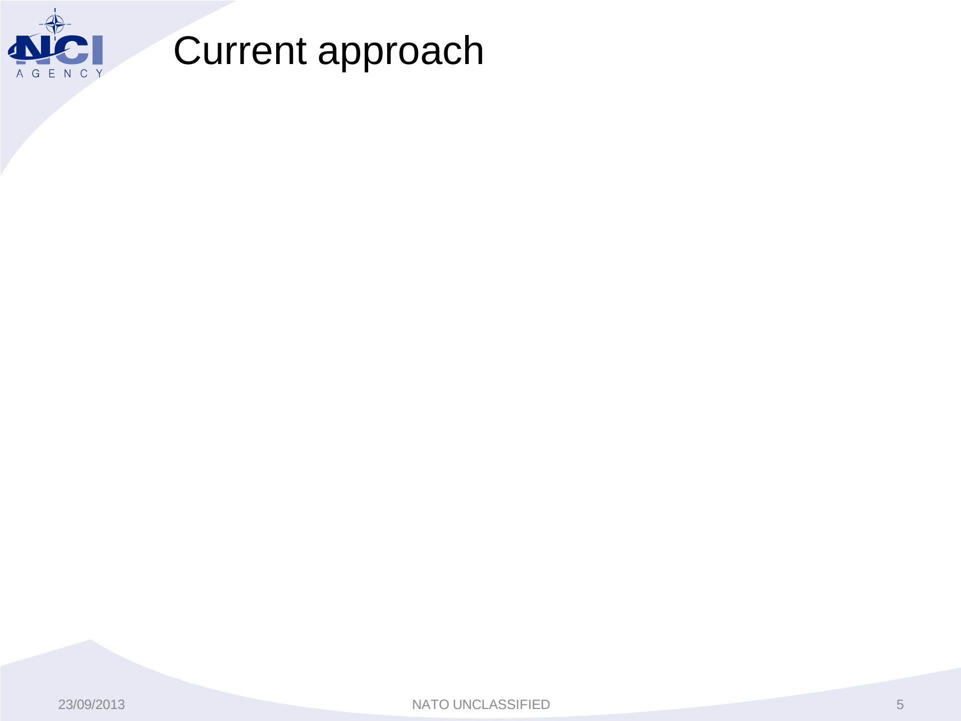
Example: Cyber Defence information eXchange Infrastructure (CDXI)

- Future capability to manage, exchange and exploit cyber security information for NATO, NATO Nations, partners, and industry

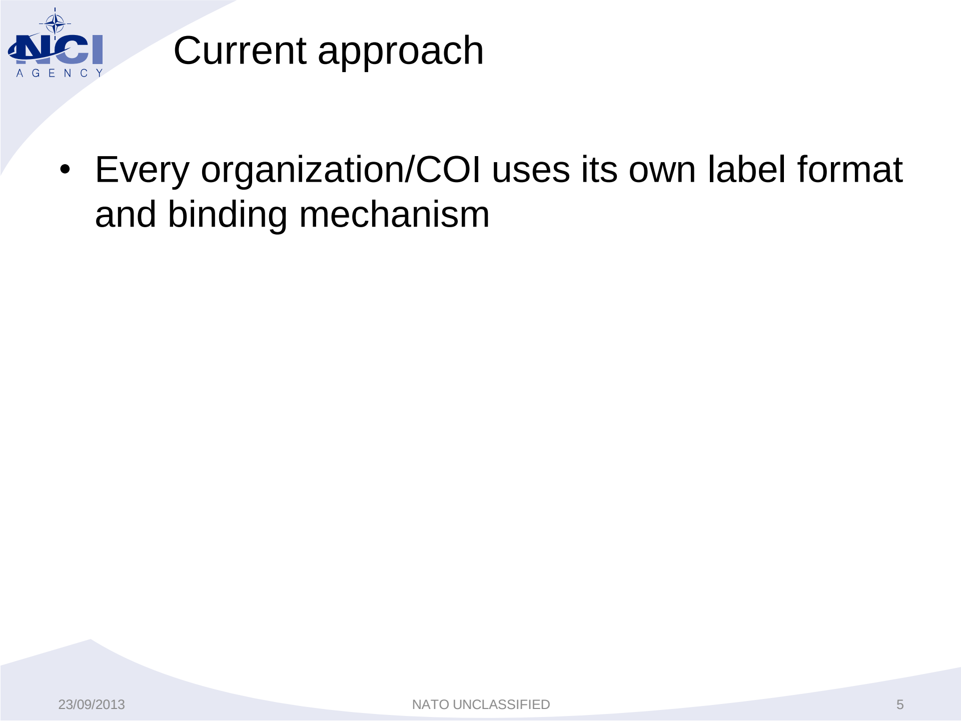


Labelling requirements within CDXI

- Provide the ability to define custom labels
- Labels used to make access control decisions
- Apply labels to many different types of data
  - vulnerabilities, incidents, threats, attack patterns
- Standardized syntax and binding mechanism
  - Need to be able to read and validate label
  - Need to be able to determine association between label and information object
  - One solution enables communication with all partners



Current approach



Current approach

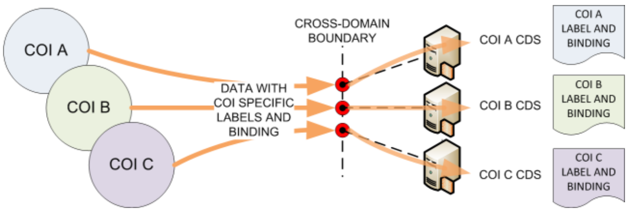
- Every organization/COI uses its own label format and binding mechanism

Current approach

- Every organization/COI uses its own label format and binding mechanism
  - We either need a separate policy enforcement point (PEP) for each exchange link, or must implement support for all COIs in one PEP

Current approach

- Every organization/COI uses its own label format and binding mechanism
  - We either need a separate policy enforcement point (PEP) for each exchange link, or must implement support for all COIs in one PEP
  - This leads to challenges in the area of management and implementation assurance



COI A

COI B

COI C

DATA WITH COI SPECIFIC LABELS AND BINDING

CROSS-DOMAIN BOUNDARY

COI A CDS

COI B CDS

COI C CDS

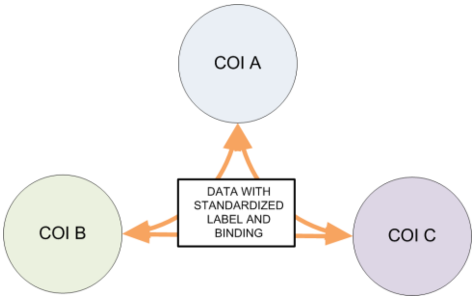
COI A LABEL AND BINDING

COI B LABEL AND BINDING

COI C LABEL AND BINDING

Standardized NATO Labelling

- Standardized label format and binding mechanism
- Liberty in selection and extending of label values
  - Not limited to confidentiality, can include any metadata



Standardized NATO Labelling

Standardized NATO Labelling

- Defines XML containers to encode sensitivity marking values into an XML formatted label (which is called a Confidentiality Label)

Standardized NATO Labelling

- Defines XML containers to encode sensitivity marking values into an XML formatted label (which is called a Confidentiality Label)
- Defines a binding mechanism providing fine-grained labelling

Standardized NATO Labelling

- Defines XML containers to encode sensitivity marking values into an XML formatted label (which is called a Confidentiality Label)
- Defines a binding mechanism providing fine-grained labelling
- Designed to be application/data format agnostic

Standardized NATO Labelling

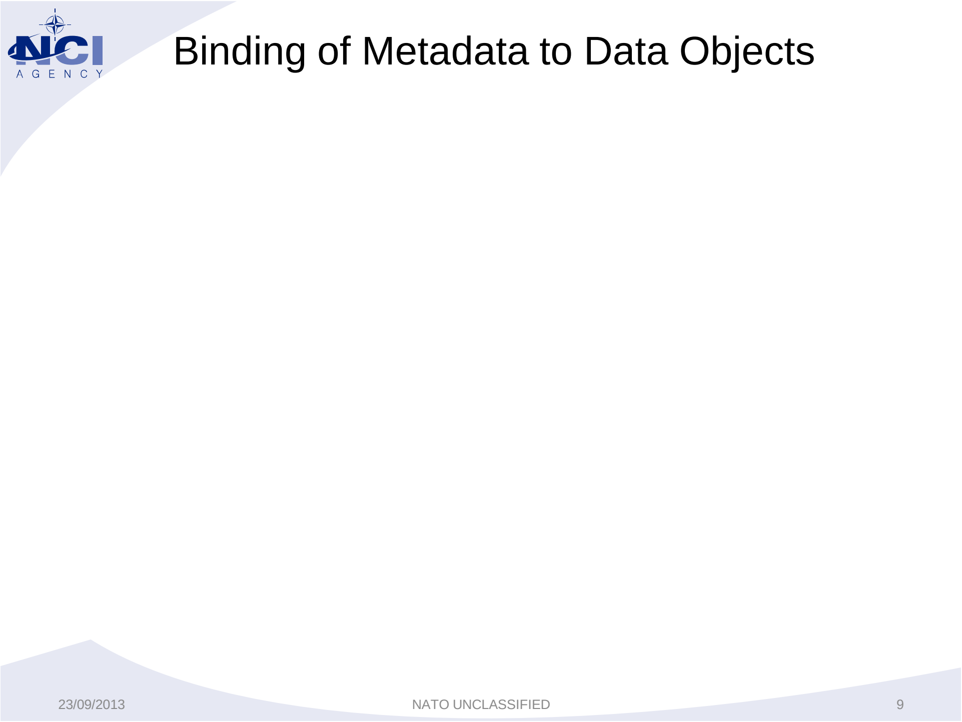
- Defines XML containers to encode sensitivity marking values into an XML formatted label (which is called a Confidentiality Label)
- Defines a binding mechanism providing fine-grained labelling
- Designed to be application/data format agnostic
- Especially suitable for release control

Standardized NATO Labelling

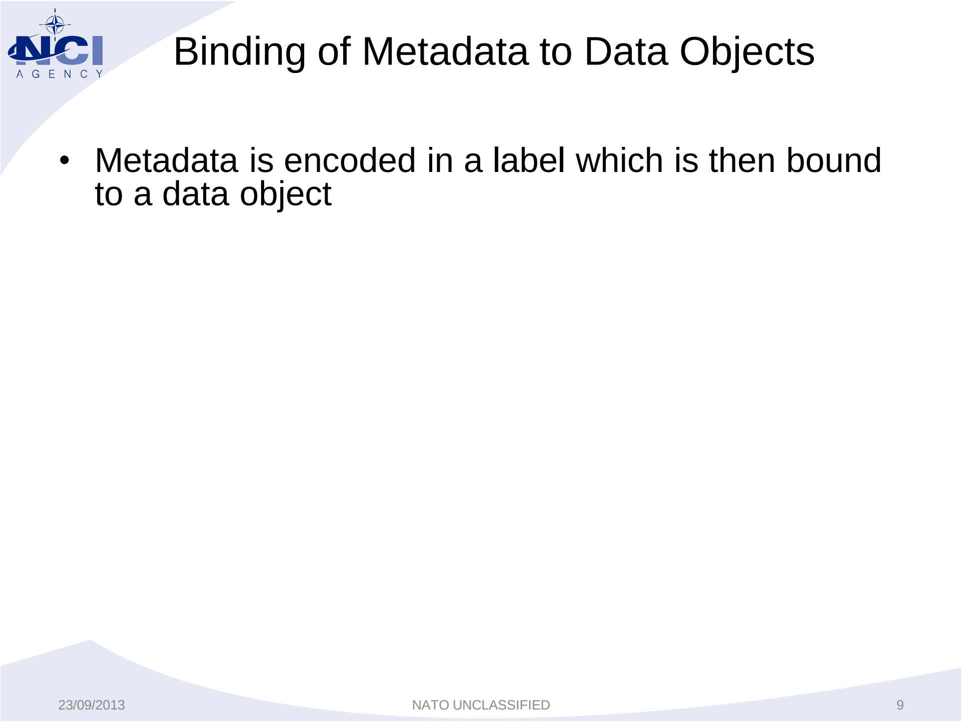
- Defines XML containers to encode sensitivity marking values into an XML formatted label (which is called a Confidentiality Label)
- Defines a binding mechanism providing fine-grained labelling
- Designed to be application/data format agnostic
- Especially suitable for release control
- Enables interoperability between organizations and COIs

Example of an NL Confidentiality Label

```
<slab:ConfidentialityLabel
        xmlns:slab=http://www.nato.int/2012/12/nxl/xcl#human >
        <slab:ConfidentialityInformation>
                <slab:PolicyIdentifier>NATO/EAPC</slab:PolicyIdentifier>
                <slab:Classification>CONFIDENTIAL</slab:Classification>
                <slab:Category Type="RESTRICTIVE"
                        TagName="Special Category Designators">
                        <slab:GenericValue>ATOMAL</slab:GenericValue>
                        <slab:GenericValue>CRYPTO</slab:GenericValue>
                </slab:Category>
                <slab:Category Type="INFORMATIVE"
                        TagName="Administrative Markings">
                        <slab:GenericValue>MEDICAL</slab:GenericValue>
                </slab:Category>
        </slab:ConfidentialityInformation>
        <slab:CreationDateTime>
                2013-08-29T16:15:00
        </slab:CreationDateTime>
</slab:ConfidentialityLabel>
```



Binding of Metadata to Data Objects

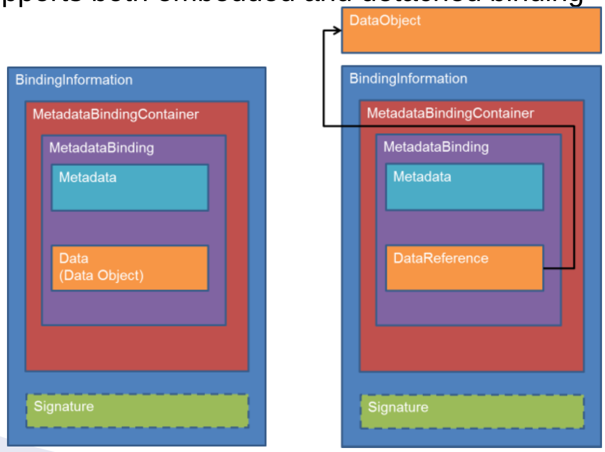


Binding of Metadata to Data Objects

- Metadata is encoded in a label which is then bound to a data object

Binding of Metadata to Data Objects

- Metadata is encoded in a label which is then bound to a data object
  - Supports both embedded and detached binding



BindingInformation

MetadataBindingContainer

MetadataBinding

Metadata

Data
(Data Object)

Signature

DataObject

BindingInformation

MetadataBindingContainer

MetadataBinding

Metadata

DataReference

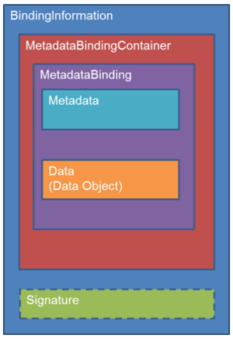
Signature

Binding of Metadata to Data Objects

- Metadata is encoded in a label which is then bound to a data object
  - Supports both embedded and detached binding
- Loose vs. strong binding

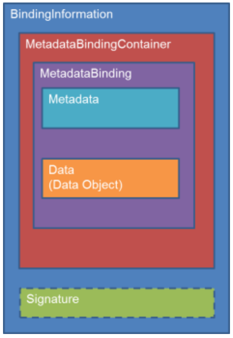
Binding of Metadata to Data Objects

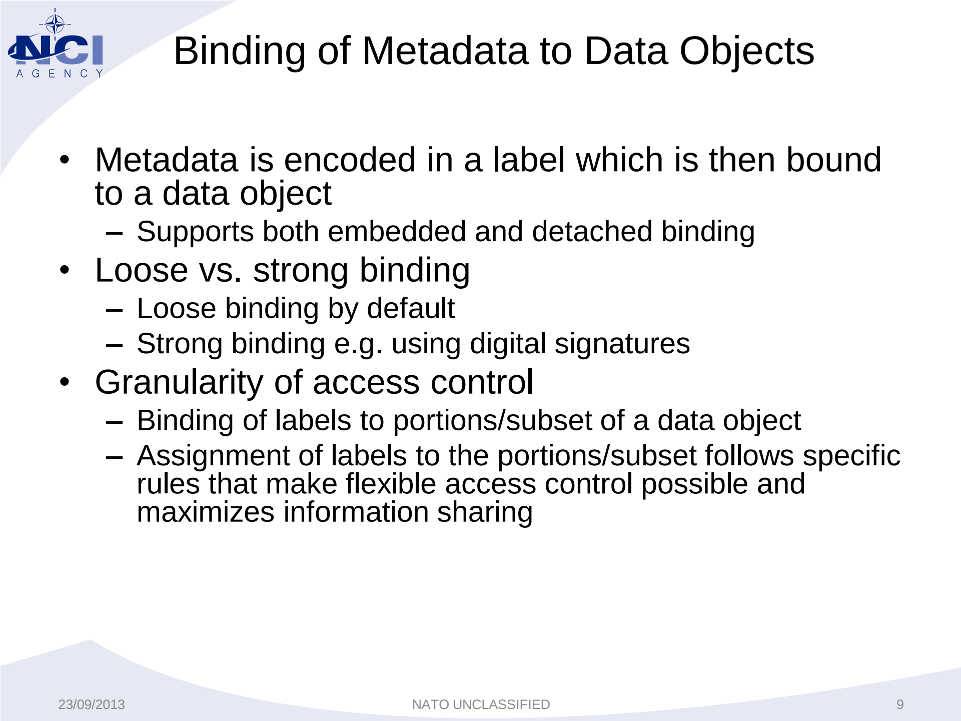
- Metadata is encoded in a label which is then bound to a data object
  - Supports both embedded and detached binding
- Loose vs. strong binding
  - Loose binding by default



Binding of Metadata to Data Objects

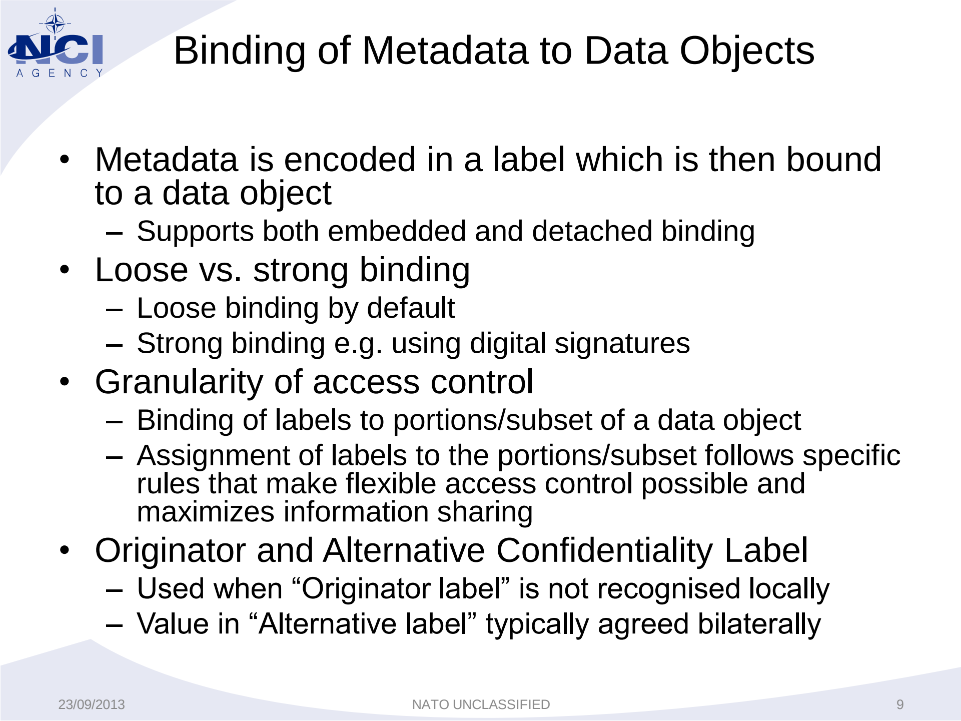
- Metadata is encoded in a label which is then bound to a data object
  - Supports both embedded and detached binding
- Loose vs. strong binding
  - Loose binding by default
  - Strong binding e.g. using digital signatures





Binding of Metadata to Data Objects

- Metadata is encoded in a label which is then bound to a data object
  - Supports both embedded and detached binding
- Loose vs. strong binding
  - Loose binding by default
  - Strong binding e.g. using digital signatures
- Granularity of access control
  - Binding of labels to portions/subset of a data object
  - Assignment of labels to the portions/subset follows specific rules that make flexible access control possible and maximizes information sharing



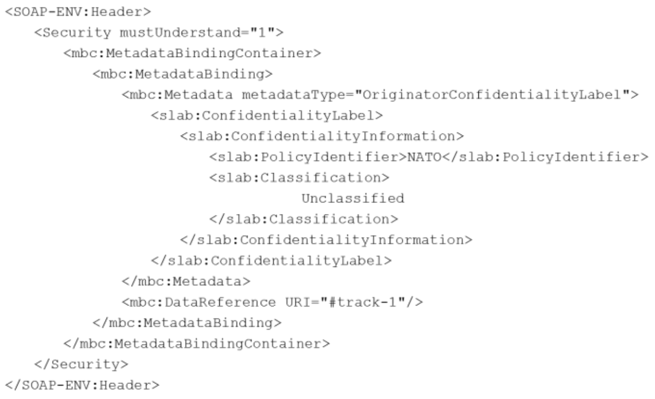
Binding of Metadata to Data Objects

- Metadata is encoded in a label which is then bound to a data object
  - Supports both embedded and detached binding
- Loose vs. strong binding
  - Loose binding by default
  - Strong binding e.g. using digital signatures
- Granularity of access control
  - Binding of labels to portions/subset of a data object
  - Assignment of labels to the portions/subset follows specific rules that make flexible access control possible and maximizes information sharing
- Originator and Alternative Confidentiality Label
  - Used when “Originator label” is not recognised locally
  - Value in “Alternative label” typically agreed bilaterally

Data format agnostic

Data format agnostic

- SOAP
  - Header



```
<SOAP-ENV:Header>
    <Security mustUnderstand="1">
        <mbc:MetadataBindingContainer>
            <mbc:MetadataBinding>
                <mbc:Metadata metadataType="OriginatorConfidentialityLabel">
                    <slab:ConfidentialityLabel>
                        <slab:ConfidentialityInformation>
                            <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
                            <slab:Classification>
                                        Unclassified
                            </slab:Classification>
                        </slab:ConfidentialityInformation>
                    </slab:ConfidentialityLabel>
                </mbc:Metadata>
                <mbc:DataReference URI="#track-1"/>
            </mbc:MetadataBinding>
        </mbc:MetadataBindingContainer>
    </Security>
</SOAP-ENV:Header>
```

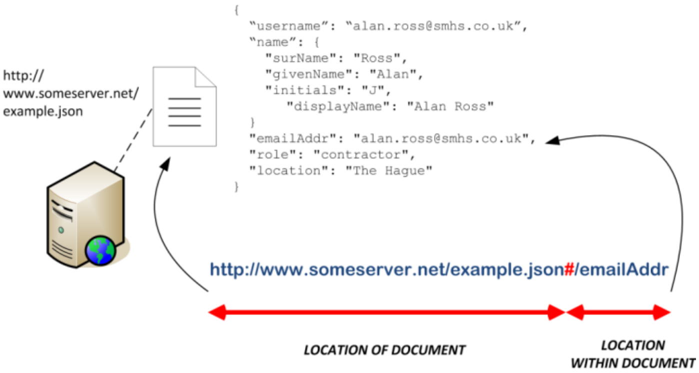
Data format agnostic

- SOAP
  - Header
  - Body

```
<SOAP-ENV:Body>
    <pullNFFIResponse>
        <nffi:NFFIMessage>
            <nffi:track Id="track-1">
                <nffi:positionalData>
                    <nffi:trackSource>
                        <nffi:transponderId>*</nffi:transponderId>
                    </nffi:trackSource>
                    <nffi:dateTime>00000000000000</nffi:dateTime>
                    <nffi:coordinates>
                        <nffi:latitude>-90</nffi:latitude>
                        <nffi:longitude>180</nffi:longitude>
                    </nffi:coordinates>
                </nffi:positionalData>
                <nffi:identificationData>
                    <nffi:unitSymbol>---------------</nffi:unitSymbol>
                    <nffi:unitShortName>*</nffi:unitShortName>
                </nffi:identificationData>
            </nffi:track>
        </nffi:NFFIMessage>
    </pullNFFIResponse>
</SOAP-ENV:Body>
```

Data format agnostic

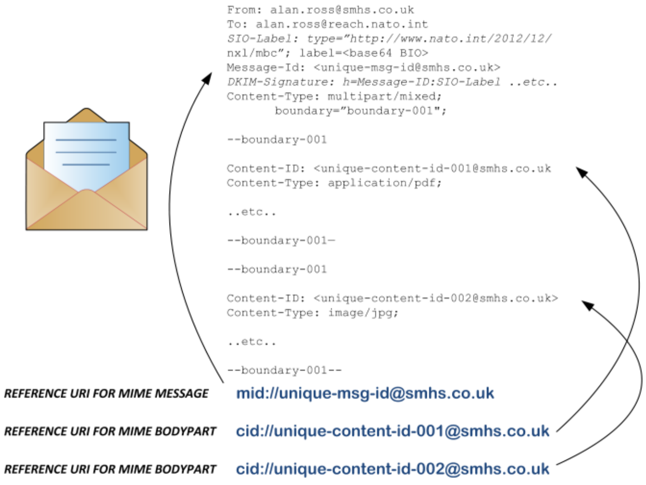
- SOAP
  - Header
  - Body
- JSON



```
{
  “username”: “alan.ross@smhs.co.uk”,
  “name”: {
    "surName": "Ross",
    "givenName": "Alan",
    "initials": "J",
       "displayName": "Alan Ross"
  }
  "emailAddr": "alan.ross@smhs.co.uk",
  "role": "contractor",
  "location": "The Hague"
}
```

Data format agnostic

- SOAP
  - Header
  - Body
- JSON
- Email



```
From: alan.ross@smhs.co.uk
To: alan.ross@reach.nato.int
SIO-Label: type="http://www.nato.int/2012/12/
nxl/mbc"; label=<base64 BIO>
Message-Id: <unique-msg-id@smhs.co.uk>
DKIM-Signature: h=Message-ID:SIO-Label ..etc..
Content-Type: multipart/mixed;
       boundary="boundary-001";

--boundary-001

Content-ID: <unique-content-id-001@smhs.co.uk
Content-Type: application/pdf;

..etc..

--boundary-001–

--boundary-001

Content-ID: <unique-content-id-002@smhs.co.uk>
Content-Type: image/jpg;

..etc..

--boundary-001--
```

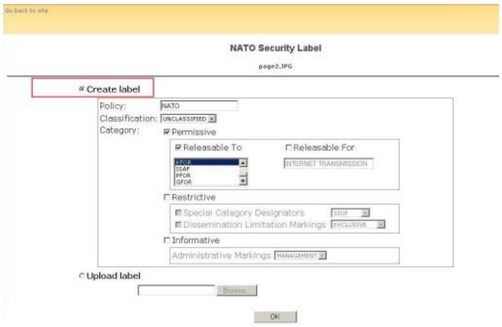
REFERENCE URI FOR MIME MESSAGE mid://unique-msg-id@smhs.co.uk

REFERENCE URI FOR MIME BODYPART cid://unique-content-id-001@smhs.co.uk

REFERENCE URI FOR MIME BODYPART cid://unique-content-id-002@smhs.co.uk

Data format agnostic

- SOAP
  - Header
  - Body
- JSON
- Email
- Sharepoint



NATO Security Label

page2.JPG

● Create label

Policy: NATO

Classification: UNCLASSIFIED

Category: ☑ Permissive

☑ Releasable To: KFOR, ISAF, PFOR, GFOR

☐ Releasable For: INTERNET TRANSMISSION

☐ Restrictive

☑ Special Category Designators: SIOP

☑ Dissemination Limitation Markings: EXCLUSIVE

☐ Informative

Administrative Markings: MANAGEMENT

○ Upload label

NCI
AGENCY
NATO
OTAN
NCI
AGENCY

Content-based Protection and Release:

From connecting forces to civil-military interaction

konrad.wrona@ncia.nato.int

23/09/2013 NATO UNCLASSIFIED 11