Janusnet

Closing the Metadata Capability Gap

Making Security Controls Interoperable across Enterprise and Coalition Boundaries with Trusted Metadata.

Greg Colla · CTO · August 2026

DAFITC BREAKOUT SESSION

Presentation Overview

Metadata Fragmentation and Delivery Risk

The Capability Gap

The Trusted Metadata Layer in Enterprise Architecture

Use cases

Deployment methodologies

Key takeaways

Presentation collateral

janusnet.com/dafitc

Janusnet

WHY NOW

janusnet.com/dafitc

Metadata Fragmentation is Now a Program Delivery Risk

DCS and Zero Trust depend on authoritative resource attributes; current estates still mix visual, proprietary, externalised, and standards-based representations.

Standards Direction



DoW MEM defines labels. STANAG 4774 / 4778 / 5636 and ACP 240 define a path from labels to interoperable enforcement.

Zero Trust Data Pillar



ABAC requires trusted classification, releasability, caveat, originator, and policy attributes.

Boundary Assurance



Raise the Bar drives deterministic, auditable CDS decisions rather than manual exceptions.

Protected Exchange



ZTDF packages policy metadata; weak source attributes become protected ambiguity.

The delivery consequence

PMOs

Accreditation delays, rework, integration overruns, and incompatible components discovered late.

Information Architects

Fragmented information models and duplicated policy mappings across systems.

Security Architects

ABAC, DLP, CDS, DRM, and gateways cannot rely on consistent resource attributes.

The issue is not a shortage of security products;
It is a shortage of authoritative, interoperable attributes flowing consistently between those products.

Janusnet

PROBLEM DEFINITION

janusnet.com/dafitc

The Capability Gap is Broken Interoperability — not Missing Labels

Two systems can both support classification and still fail when policy meaning, representation, or binding diverges.

Policy Intent

Information objects carry authoritative, machine-readable classification and handling attributes that persist and drive deterministic decisions.



Metadata Reality

Visual markings, tenant IDs, custom properties, repository indexes, transport headers, and legacy formats.

Metadata Disparity

Applications, endpoints, email, collaboration tools, repositories, and scripts retain different representations.

Local vs. Cross-Domain

A label usable inside one tenant may be opaque to coalition gateways, guards, federation services, and mission partners.

Labeling vs. Enforcement

Labels create value only when PDPs, PEPs, DLP, CDS, and storage controls consume trusted attributes.

Does the receiver understand the policy? Can it parse the format? Can it preserve and verify the binding?

Janusnet

ENTERPRISE PATH

janusnet.com/dafitc

Metadata Breaks at Hand-Offs — not only at the Boundary

The same file may move through endpoints, collaboration, records, messaging, and cross-domain controls before reaching a mission partner.

Endpoint



Create, save, download, scripts

Applications



Office, email, chat, portals

Repositories



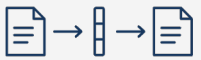
File shares, EDRMS, archives

Gateways



Messaging, API, export

CDS / Guard



Validate, release, route, audit

Coalition



STANAG receiving domain

Authority Loss

Visual markings or inferred context replace an authoritative attribute.

Semantic Drift

Tenant identifiers no longer express the receiving policy vocabulary.

Binding Loss

Repository or transport context is stripped as location or format changes.

Enforcement Ambiguity

Controls reject, accept unsafely, or escalate to manual review.

A DCS architecture fails when one layer writes metadata that the next cannot read, validate, translate, or rebind.

Janusnet

LEGACY & MIXED ENVIRONMENTS

janusnet.com/dafitc

Why legacy and mixed environments amplify the problem

Defence enterprises rarely migrate from a blank slate — accumulated content and application generations compound the metadata gap.

Modern Files

Embedded, machine-readable metadata travels with the object.

Legacy Files

Visual markings only — no authoritative metadata to extract.

Records & Externalized Systems

Classification lives in an index or platform field, not the file itself.

Mixed Policy Vocabularies

National, NATO, coalition, and vendor-specific schemes coexist without reliable translation.

ABAC

File, message, and repository access decisions need trusted resource attributes.

DLP

Releasability and caveat controls depend on metadata the tool doesn't itself create.

CDS & Gateways

Cross-domain and coalition mediation stalls without deterministic, parseable labels.

ZTDF

The cryptographic wrapper is only as good as the source attributes it packages.

The question needs to change from “is your data labeled” to “is your data labeled consistently”.

Janusnet

ARCHITECTURAL RESPONSE

janusnet.com/dafitc

A Trusted Metadata Layer Separates Translation from Enforcement

Treat metadata interoperability as enterprise security infrastructure — not a feature embedded repeatedly in every tool.

Endpoint	Vendor Labels	Email	Repositories	Legacy	Coalition
create, save, download	MIP and custom properties	headers and attachments	indexes and exports	visual and externalised context	standards-based metadata

Trusted Metadata Layer

Multi-policy comprehension • standards alignment • binding awareness • validation • translation • rebinding • PIP services • audit evidence


Read


Validate


Normalise


Translate


Rebind


Expose

Supplies trusted attributes — does not decide access or release

ABAC	DLP	Gateways	CDS / Guards	Storage	ZTDF
PDP and PEP	detection and control	routing and transformation	release enforcement	access and handling	protected-object services

Separation of concerns reduces duplicated engineering, inconsistent interpretation, and accreditation risk.

Janusnet

DESIGN PRINCIPLES

janusnet.com/dafitc

Five Principles Keep the Layer Trustworthy — and Keep it in its Lane

Architectural discipline prevents the service becoming another monolith or a hidden policy decision point.

1. Separation of Concerns



Read, validate, translate, and rebind; leave decisions to enforcement systems.

2. Policy-Aware, not Locked



Support concurrent national, NATO, FVEY, enterprise, and vendor policies.

Trusted Attributes with Preserved Semantic Meaning

5. Auditable



Evidence extraction, validation, translation, rebinding, and downstream context.

3. Binding-Aware



Understand how metadata survives objects, transports, storage, and conversion.

4. Incrementally Deployable



Insert capability at endpoint, repository, gateway, pre-guard, or ABAC PIP.

Preserve meaning, provenance, and authority while representation and operational context change.

Janusnet

USE CASE 1

janusnet.com/dafitc

Convert Purview to STANAG without Losing Meaning

Preserve semantic meaning while translating and rebinding the label so gateways, the CDS, and receiving systems can act on trusted resource attributes.

Initial State

Enterprise: Purview / MIP labels

Coalition: STANAG 4774 / 4778

Boundary: coalition-operated CDS

Mismatch: policy IDs, formats, bindings, and enforcement points

01
Send

Alice sends a Purview-labelled email and attachment to Bob. The message enters the enterprise gateway.

02
Extract

Extract MIP metadata and the attachment; identify the destination and required policy context.

03
Validate + Map

Check both policy catalogues, confirm releasability, and map the label into the coalition namespace.

04
Convert + Rebind

Convert to STANAG 4774; rebind email and attachment under STANAG 4778; then forward.

05
Enforce + Deliver

The CDS applies release, routing, inspection, and audit. Bob's systems preserve the coalition marking.

Outcome

Coalition receives trusted, enforceable metadata.

Without the Trusted Layer

The receiver sees opaque vendor identifiers or inconsistent message and attachment metadata — driving CDS rejection, manual relabeling, or unsafe acceptance, with delivery delay, weak audit evidence, and security risk.

Janusnet

USE CASE 2

janusnet.com/dafitc

Make Endpoint Downloads Authoritative at Entry

DLP can inspect or block content, but it does not create the authoritative metadata layer required downstream.

Initial Condition

A file arrives from a partner portal, browser, application, or automated process. It may carry visual markings, partial metadata, proprietary labels — or no machine-readable security metadata.

Control point: create, save, download, and automated generation events.

01

Detect + Extract

Capture metadata, markings, origin, context, source, and permitted classification hints.

02

Validate + Resolve

Check policy catalogues. Missing or ambiguous attributes trigger user or workflow resolution.

03

Write + Evidence

Bind authoritative metadata to the file and record the classification and binding decision.

Trusted Metadata Reaches every Downstream Control

Repositories, email, DLP, CDS, gateways, storage controls, and ABAC engines receive trusted attributes rather than only content inspection or visual markings.

Endpoint DLP remains valuable — as an enforcement control alongside, not instead of, a common metadata layer.

Janusnet

DEPLOYMENT PATTERNS

janusnet.com/dafitc

Deploy where Metadata Failure is Visible and Measurable

Introduce services and agents incrementally, prioritized by delivery risk and operational impact.



Endpoint Capture

Create authoritative metadata at creation, save, download, and automated generation.



Repository Integration

Synchronise index-held context with file-resident metadata so exports stay self-describing.



Gateway Translation

Translate email, attachment, API, and collaboration metadata before onward routing.



Pre-Guard Validation

Normalise and validate labels before content reaches a CDS or boundary.



ABAC PIP

Expose classification, releasability, caveats, policy, and originator attributes.



Legacy + ZTDF Readiness

Remediate legacy content and supply validated attributes to protected-object services.

Start where manual exceptions, rejected transfers, accreditation findings, or duplicated mappings are already measurable.

Janusnet

MIGRATION ROADMAP

janusnet.com/dafitc

Progress from Machine-Readable Labels to Enforceable Protected Objects

The migration can be incremental — but the metadata supply chain must be designed end to end.

Machine-Readable Labeling + Binding

Create authoritative labels and bind them to files, messages, and transports so objects remain self-describing.

Operational Metadata for Enforcement

Validate, normalise, translate, and expose attributes for ABAC, DLP, gateways, storage, and boundary mediation.

Protected-Object Exchange

Use authoritative ML2 metadata to drive ZTDF-style cryptographic protection and policy-bound sharing.

Five Program Moves

1. Stabilize policy vocabularies.
2. Label and normalise at source.
3. Normalize at integration points.
4. Expose attributes to enforcement.
5. Introduce protected exchange.

ML3 packages metadata; it cannot repair weak foundations.

Include metadata validation test points in milestones, boundary readiness reviews, and accreditation evidence plans.

Janusnet

EVALUATION SCORECARD

janusnet.com/dafitc

Evaluate the Capability as Security Infrastructure — not a Labeling Feature

Test whether metadata remains authoritative, interoperable, enforceable, and auditable across the real enterprise path.

Policy + Standards	Objects + Bindings	Integration + Enforcement	Operations + Assurance
Multi-policy: NATO, FVEY, national, enterprise, vendor.	Endpoint create, save, download, automation.	Validation and normalisation against catalogues.	Auditable extraction, mapping, translation, rebinding.
MEM, STANAG 4774, 4778, 5636 and ACP 240.	File, email, collaboration, repository formats.	PIP capability for ABAC PDPs and PEPs.	Legacy and unmediated-content remediation.
Translation fidelity and governed mappings.	Binding awareness across object and transport types.	Incremental deployment across integration points.	High availability, scale, deterministic behaviour.

Acceptance Gate	Prove representative file and message scenarios end to end — including failed validation, translation, rebinding, policy consumption, and audit output.

Use representative mission workflows, not feature checklists alone.

Janusnet

TAKEAWAY

Closing the Capability Gap: Metadata Interoperability Program Actions

Where is metadata interoperability creating the greatest delivery or accreditation risk in your environment?

janusnet.com/dafitc

Presentation collateral

PMOs	Fund metadata interoperability as a discrete work package — not a late integration detail.
Information Architects	Make the trusted metadata layer the bridge between the security model and the systems that consume it.
Security Architects	Design Zero Trust, ABAC, CDS, DLP, gateway, and ZTDF patterns around a trusted metadata supply chain.

Map the Supply Chain	Identify where metadata is created, preserved, translated, stripped, inferred, and consumed across mission workflows.
Prioritize Risk Points	Start with rejected transfers, manual releases, duplicated mappings, endpoint gaps, exports, and accreditation findings.
Prove an Increment	Pilot measurable criteria for extraction, mapping, translation, rebinding, audit, and ABAC / PIP integration.

Janusnet