Information Exchange Framework applied to Structured Data Environments

Solution to
Policy-driven Data-centric Information Sharing and Safeguarding

January 2019

Why integrate Information Sharing and Safeguarding?

"At the heart of the intelligence effort lies a paradox"

Intelligence is valuable only if it can be shared with consumers who need it

More sharing → enhanced risk of compromise

Need to find the best balance between adequate sharing and effective information security

"Sharing and Safeguarding are two sides of the same coin"

- This paradox exists in every domain where sensitive (Private, Confidential, Legally-Significant or classified) information needs to be shared
- Sharing and safeguarding priorities are often seen as mutually exclusive; in reality they are mutually reinforcing.
- By implementing mechanisms to strengthen protections for sensitive information one helps to build trust within the user and stakeholder communities and increase their willingness to share
- Achieving an effective balance between Sharing and Safeguarding:
  - Targets Responsible Information Sharing
  - Requires flexible, agile and adaptive mechanisms and controls during design, implementation, testing, deployment, operations and auditing
  - Represents a data management challenge more than a technology limitation.

What is the OMG IEF?

- Information Exchange Framework (IEF) is a collection of open standards developed under the Object Management Group (OMG), a global standards organization. These standards, developed over multiple years, were ratified in Brussels at the OMG quarterly meeting in June 2017. IEF consists of:
- Information Exchange Packaging Policy Vocabulary (IEPPV):
  - The policy vocabulary is a Unified Modeling Language (UML) Profile that specifies how to create a policy model based on the rules documented in a policy artifact, and associate these rules to datasets at a very granular level.
  - Rules can be associated with data elements, metadata, tags for PII or security classifications, or even data values depending on mission requirements. . This approach allows us to rapidly creation/update policies as policy instruments change, and retain the institutional knowledge in a model vs. buried in code.
  - UML based policy models are serialized for deployment into a runtime environment. Currently support XML or binary code (can be mapped to SAML/XACML assertions if needed).
- IEF Reference Architecture (IEF-RA):
  - The IEF reference architecture specifies how policy models are interpreted and implemented in a runtime environment.
  - Decisions for redaction/enrichment or sub-setting data are made based on the policies defined, and their association with attributes of the runtime environment (content, metadata, data tags, fabric, target audience and their need to know, Back end attributes, or even specific data values).
  - Final outcome is a mechanism to disseminate different subsets of the same information in different formats to support partner needs, all driven by policy conformance needs.
  - The runtime environment is mission agnostic and can be used for one or multiple missions in a shared capability configuration.
- 2 other initiatives underway within OMG:
  - Information Exchange Packaging and Processing Service (IEPPS): New specification for packaging and processing messages (already demonstrated).
  - Data Tagging: Standardized taxonomy for data tagging.

Why Share Information?

- ***Inform Decisions***
  - ***Shared Situational Awareness (Hindsight, Insight);***
  - ***Shared Intelligence (Foresight)***
- ***Enable Collaboration / Collective Action***
- ***Improve Operational Posture – higher quality information:***
  *(*Timely, Accurate, Current, Actionable, Complete, Concise, Accessible, Relevant, Consumable, Understandable, Reliable, …, **Trusted)**
- ***Resource Multiplier***
- **Foundation and Enabler of: Situational Awareness, Intelligence, Collaboration, Planning, Command (coordination), Cyber, …**

Why Share Information?

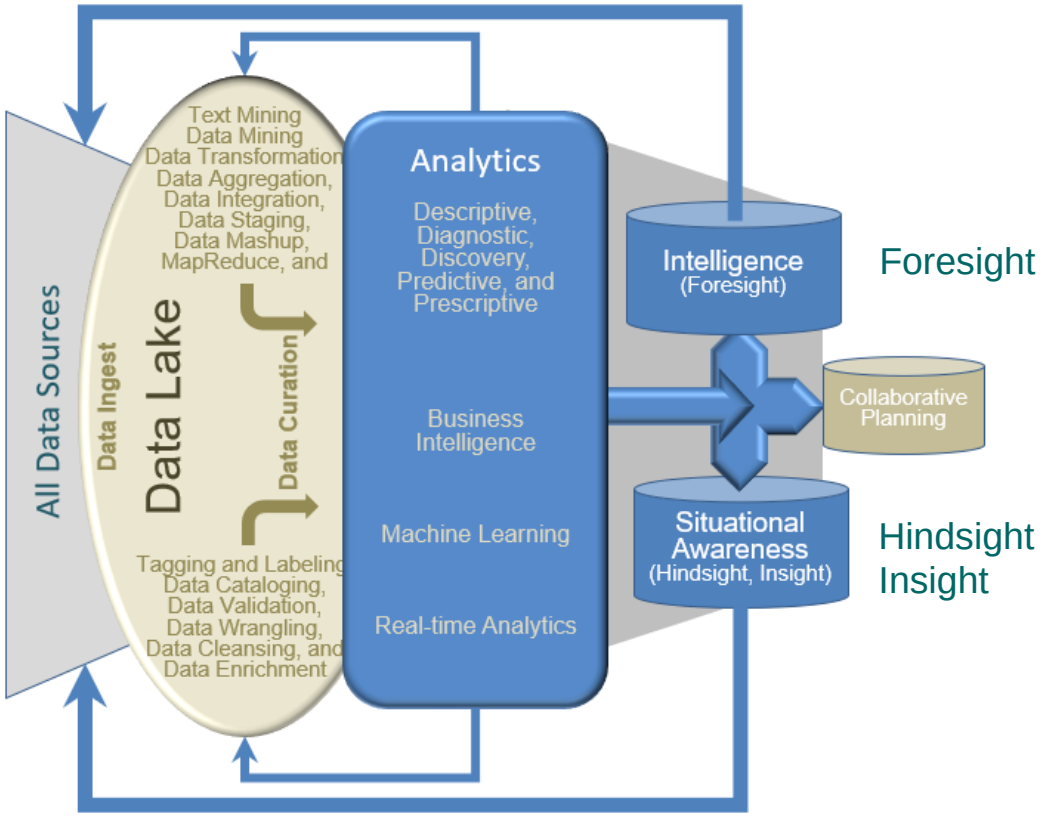
- ***Inform Decisions***
  - ***Shared Situational Awareness (Hindsight, Insight);***
  - ***Shared Intelligence (Foresight)***
- ***Enable Collaboration / Collective Action***
- ***Improve Operational Posture – higher quality information:***
  *(*Timely, Accurate, Current, Actionable, Complete, Concise, Accessible, Relevant, Consumable, Understandable, Reliable, …, **Trusted)**
- ***Resource Multiplier***
- **Foundation and Enabler of: Situational Awareness, Intelligence, Collaboration, Planning, Command (coordination), Cyber, …**

Data Collection, processing and Analysis

Data is collected from all available sources, and:

- **Tagged, labeled and catalogued to facilitate discovery, processing, sharing and safeguarding.**
- Transitioned into a form (institutional standards) that enables and facilitates processing and analytics
- Staged for analytics, machine learning, and business Intelligence services
- Analytics inform intelligence, situational awareness and planning

The ability to gather all-source data and create quality information for decision makers is the primary role of IM/IT

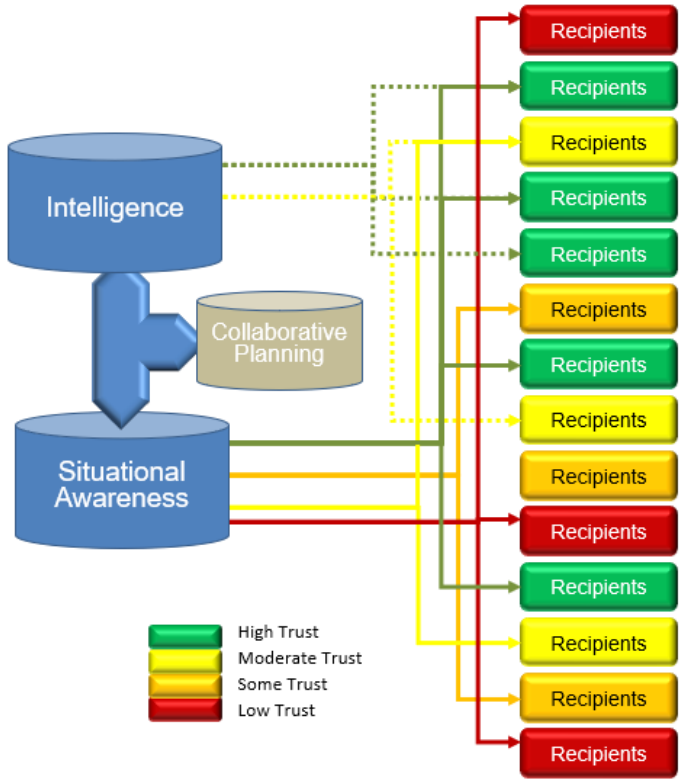


Data Sharing and Safeguarding

Once created, Situational Awareness, Intelligence and planning data is only useful if it can be shared:

- **Data and information elements must be tagged and labeled, to and facilitate discovery, processing, sharing and safeguarding**
- Data must be transformed into quality information (Timely, Accurate, Current, Actionable, Complete, Concise, Accessible, Relevant, Consumable / Understandable, Reliable, …, Trusted)
- Information must be structured and formatted in accordance with individual information sharing agreements

The ability to share information in a responsible and trusted manner is the cornerstone of a digital strategy



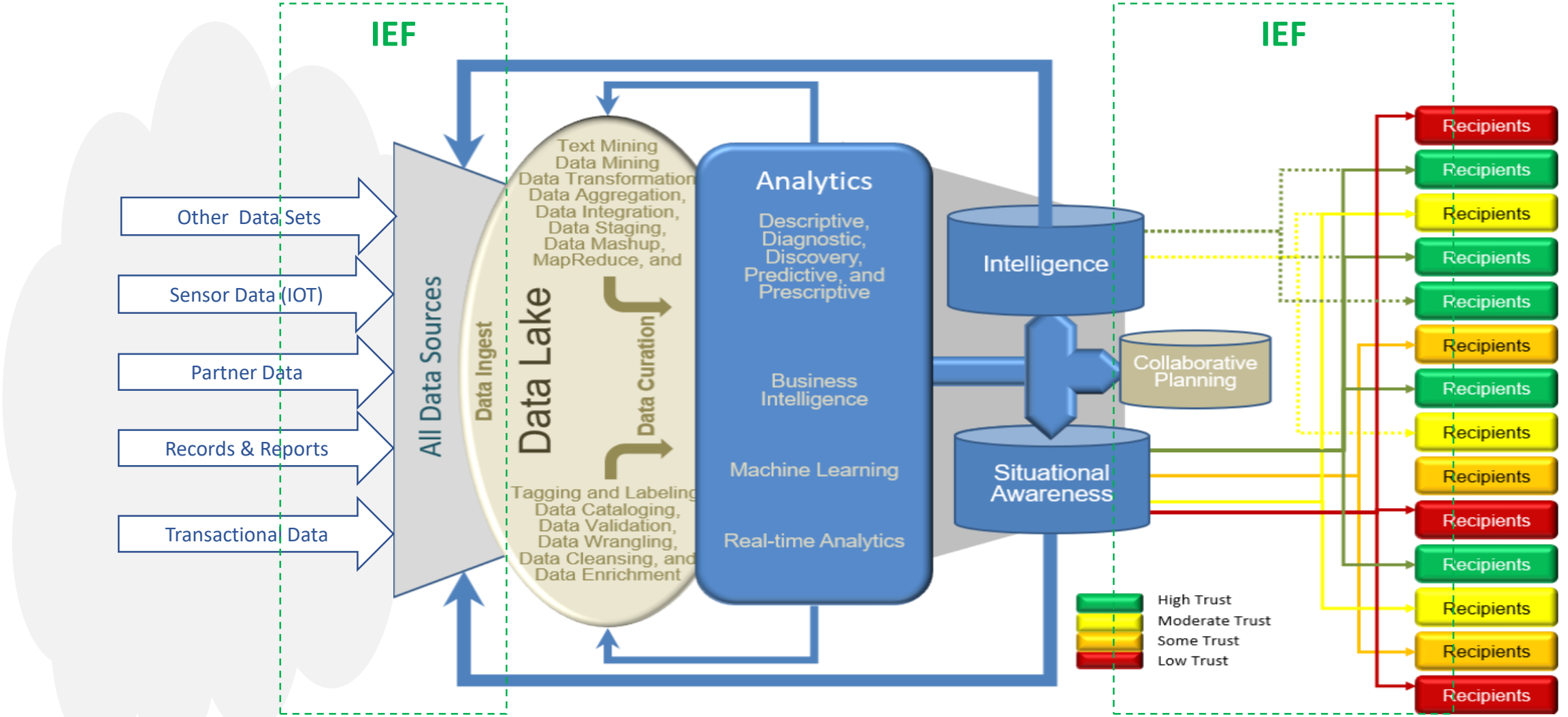
Responsible Sharing

Maximizing the sharing and availability of information of information, while simultaneously protecting sensitive (private, confidential, legally-significant and classified) information from unauthorized access, use, release, or manipulation.

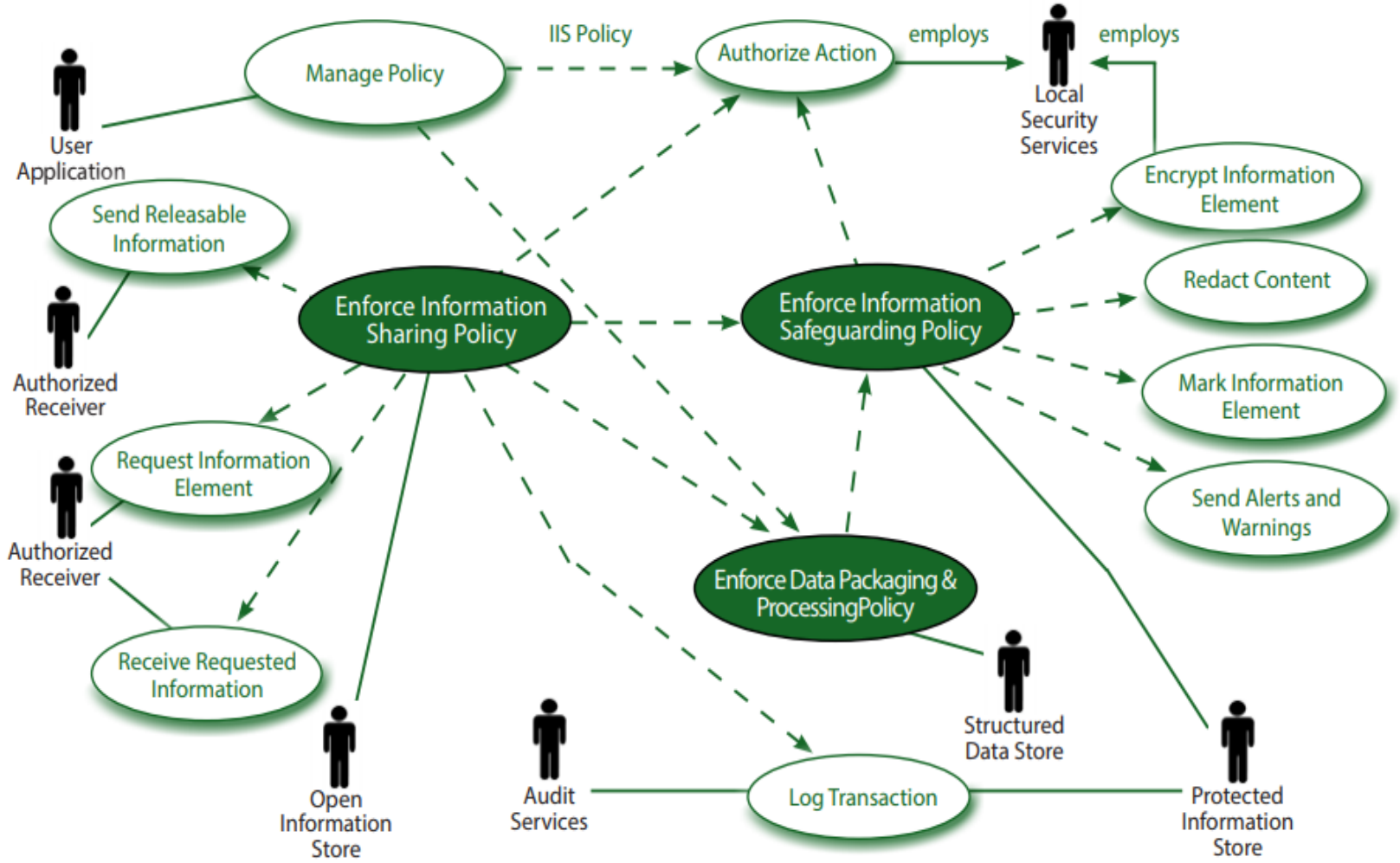
Quality Information

Provision of information that is Timely, Accurate, Current, Actionable, Complete, Concise, Accessible, Relevant, Consumable / Understandable, Reliable, **Trusted**, **etc …**

Modern Information Management on a slide



Information Exchange Framework (IEF ™) Use Case



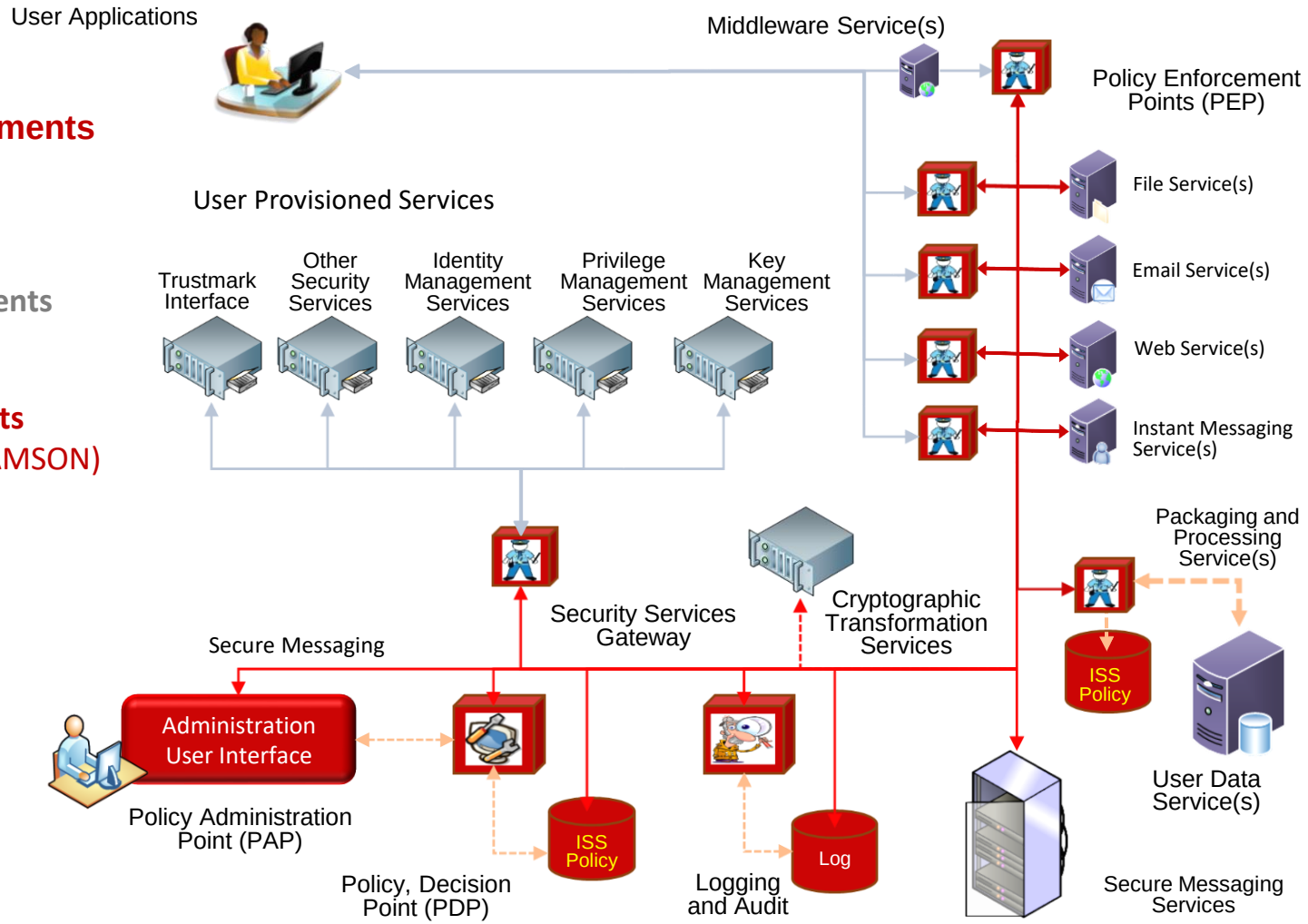
IEF Reference Architecture (IEF-RA)

(http://www.omg.org/spec/IEF-RA/)

1. **IEF-RA: Defined Elements**
   (Structured Data)

2. **User Provisioned Elements**

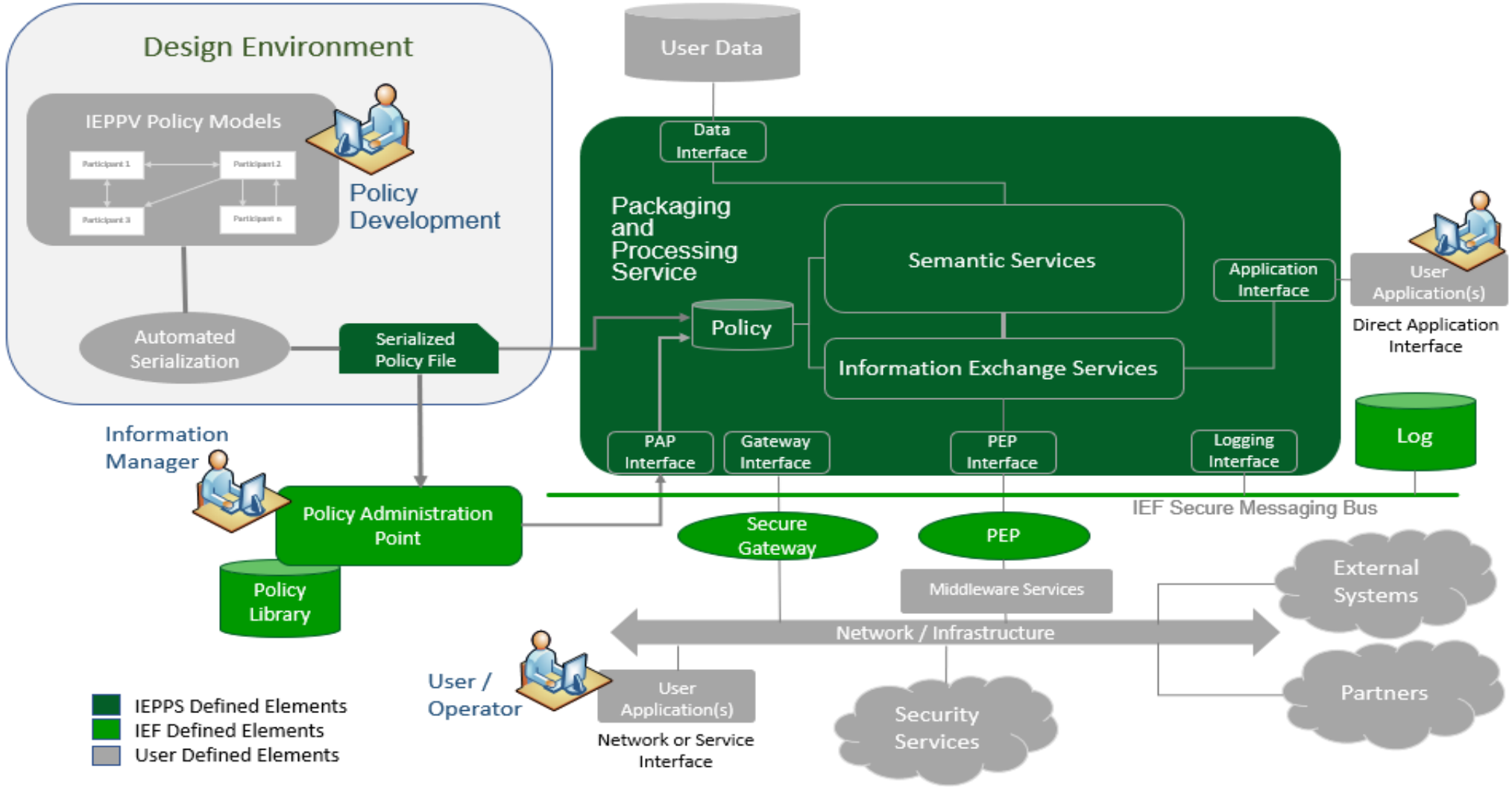
3. **IEF RA Defined Elements**
   (Unstructured Data - SAMSON)



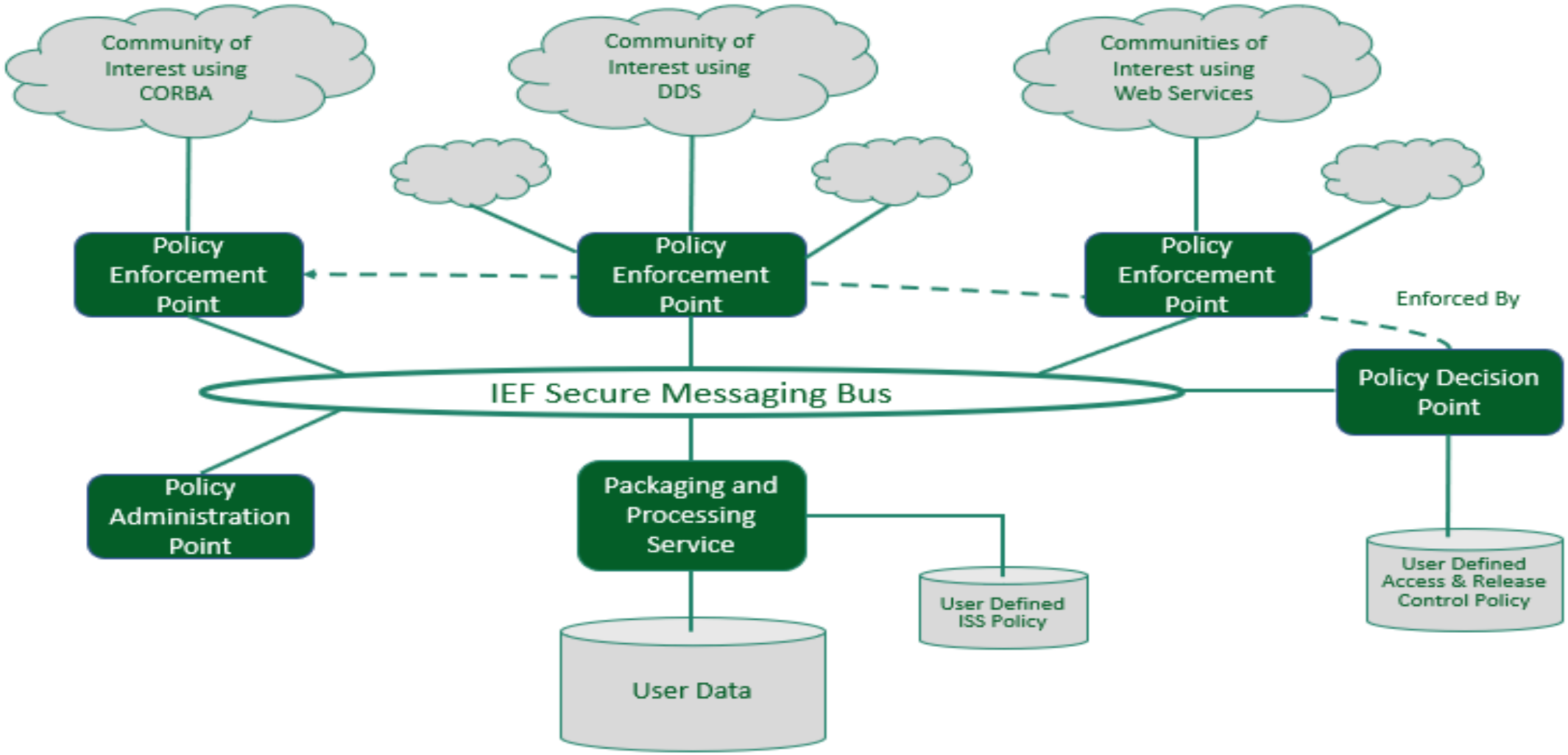
Keys to a Solutions Success

- ✓Separate Business, IM and IT Concerns
- ✓Augment and not replace user applications and infrastructure
- ✓Increase flexibility, adaptability and agility during development and operations
  - ➢ Model driven architecture / Use of MBSE
    (Traceability: Business Need ←→ Operations; Retention of Institutional Memory; Deduction in Programming Requirement)
  - ➢ Rule-based applications / Separate business rules form the code
  - ➢ Run load of business rules
  - ➢ Runtime administration of rules
    (increased flexibility, adaptability and agility)
- ✓Enhanced logging and auditing.
  (Able to demonstrate responsible, Trusted and Auditable; Real-time Monitoring; Forensic Auditing)
- ✓Integration of open standards

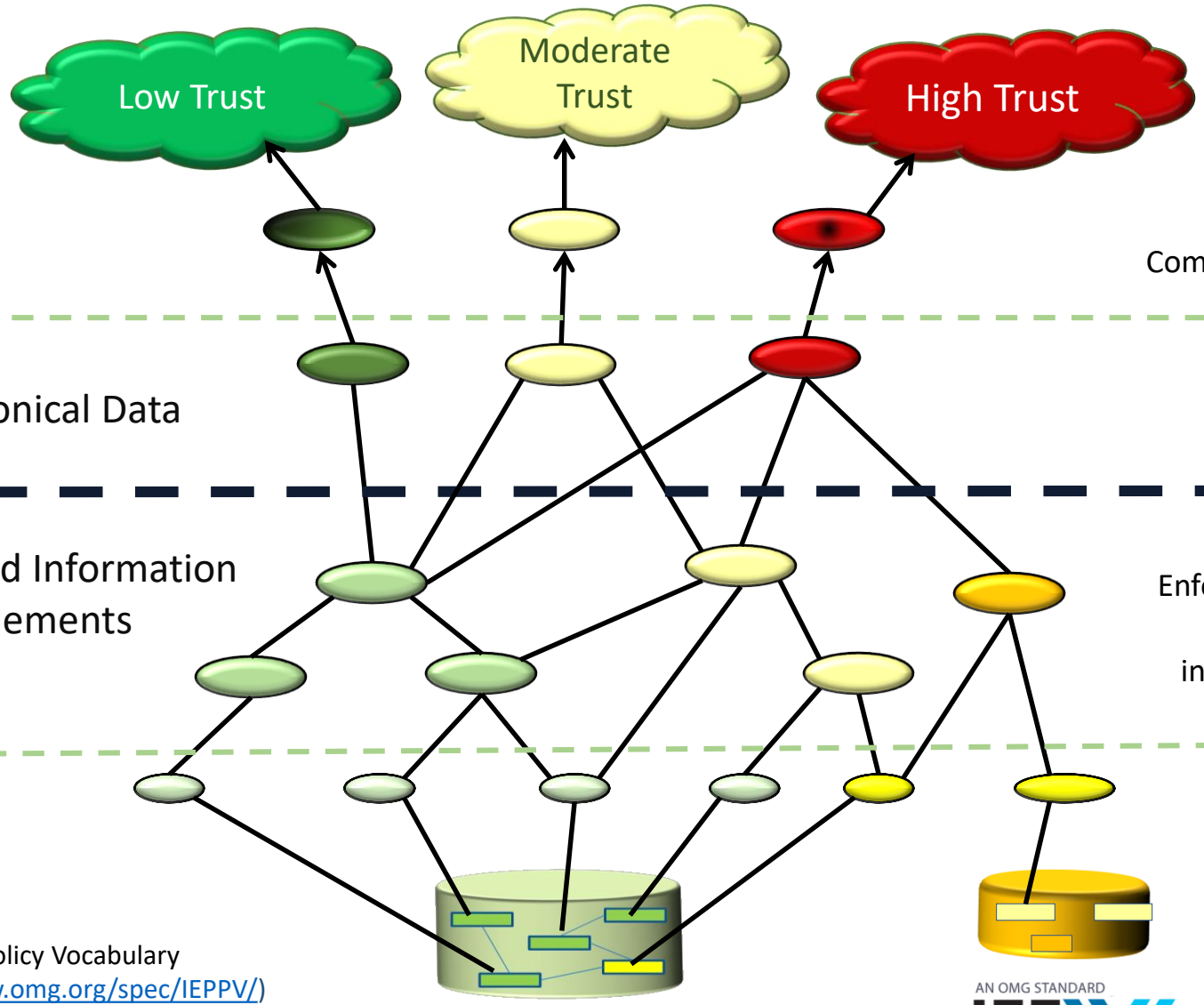
Integrated View



Multiple Integration Channels



Separate Semantic Models to Address Data Protection



IES Layer

Linking the Information to the Communication Channel (Format/Technology)

Semantic Layer

Groups the datasets into meaningful and releasable datasets

Transactional Layer

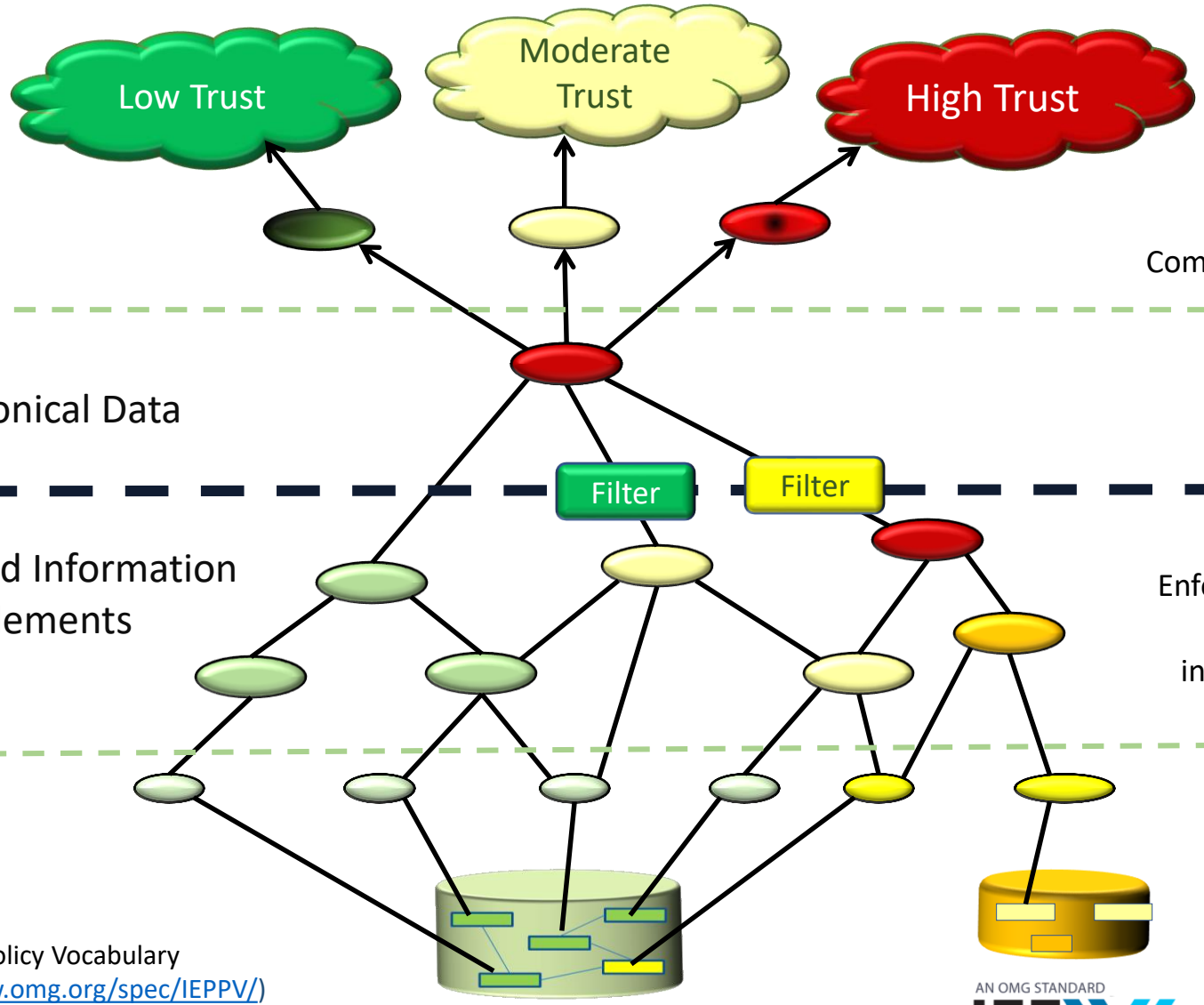
Enforces rules for aggregating, transforming, marking, and redacting data and information elements in conformance to policy instruments.

Foundation Layer

Links policy model to Physical Data Element

Packaging Policy Vocabulary
(http://www.omg.org/spec/IEPPV/)

Overlaying Redaction Filters to Provide Data Protection



Community Focus

Local Focus

Canonical Data

Data and Information Elements

IES Layer

Linking the Information to the Communication Channel (Format/Technology)

Semantic Layer

Groups the datasets into meaningful and releasable datasets

Transactional Layer

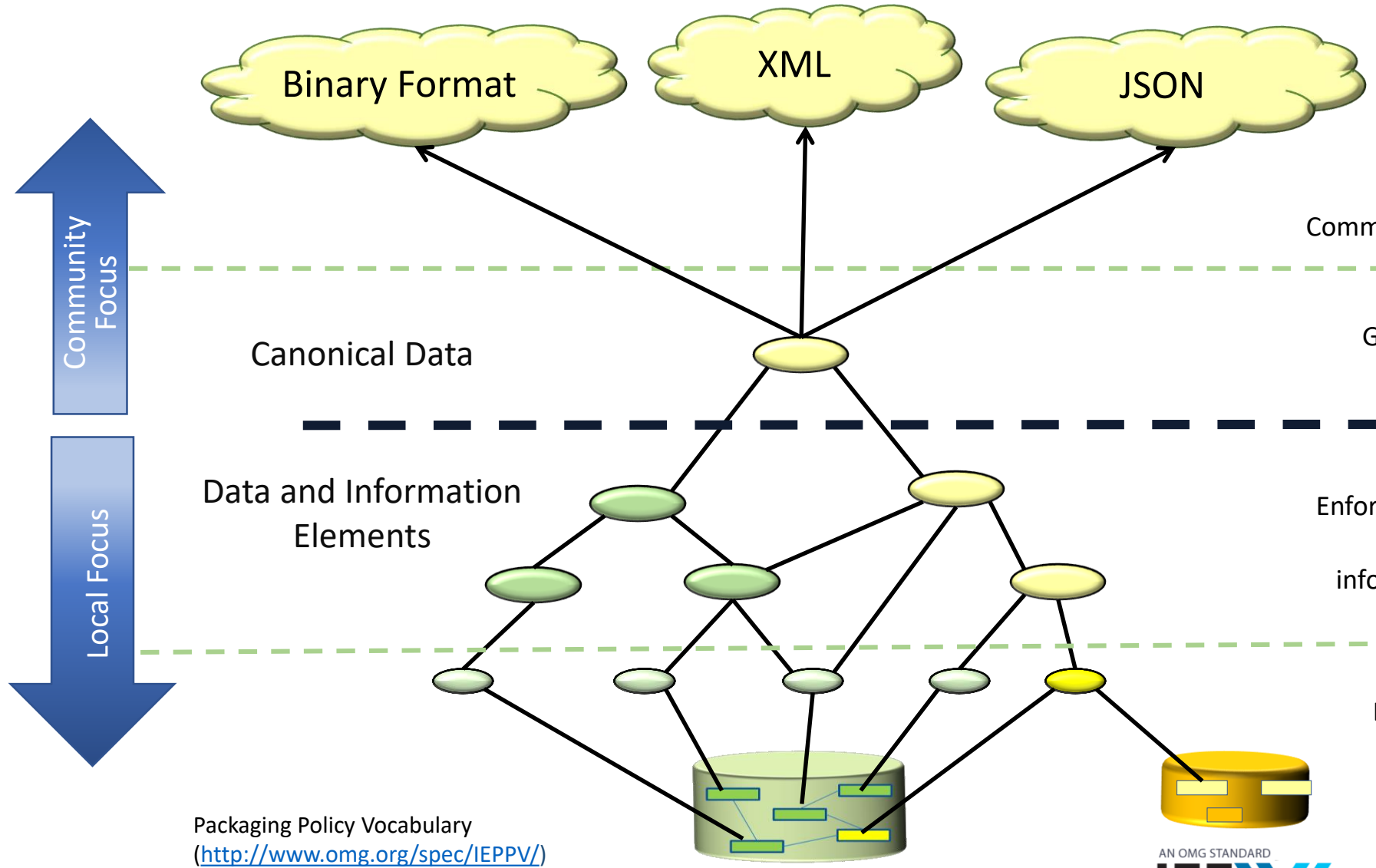
Enforces rules for aggregating, transforming, marking, and redacting data and information elements in conformance to policy instruments.

Foundation Layer

Links policy model to Physical Data Element

Packaging Policy Vocabulary
(http://www.omg.org/spec/IEPPV/)

Formatting and Protocols Applied at the IES Layer



IES Layer

Linking the Information to the Communication Channel (Format/Technology)

Semantic Layer

Groups the datasets into meaningful and releasable datasets

Transactional Layer

Enforces rules for aggregating, transforming, marking, and redacting data and information elements in conformance to policy instruments.

Foundation Layer

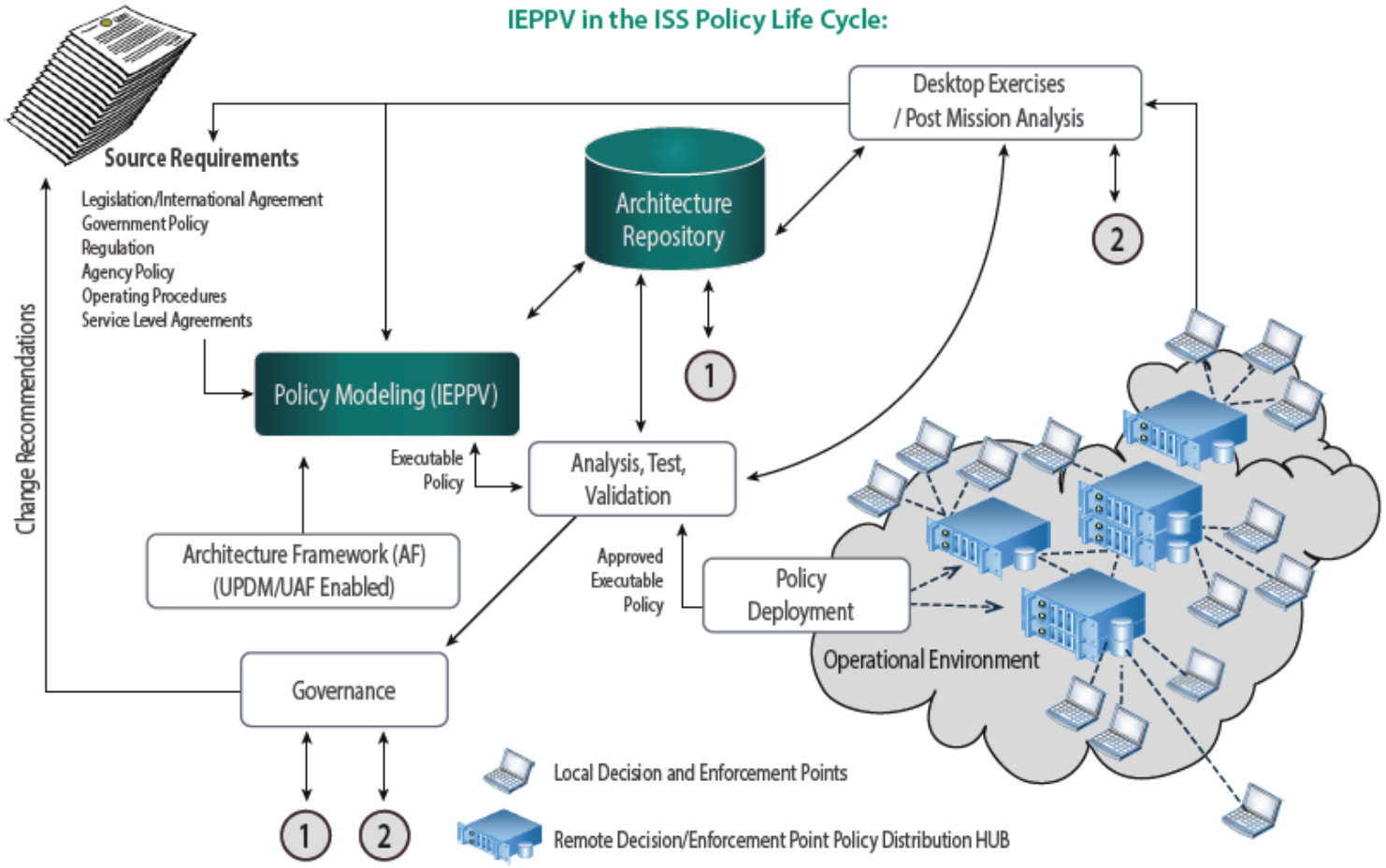
Links policy model to Physical Data Element

Packaging Policy Vocabulary
(http://www.omg.org/spec/IEPPV/)

Policy Life-cycle – Separating Concerns

- Networks and Platforms can be deployed independent of applications (e.g., Cloud, On-prem, Hybrid)
- Application are developed to enforce policies (rules and constraints) based on standardized policy models and rapidly deployed to deployed infrastructure
- Policies are defined by the business - based on user / business / operational needs - and deployed to the applications as data sets that are ingested at runtime.
- Libraries of policy models can be maintained and deployed as needed

Policy, Applications and IT have separate life-cycles

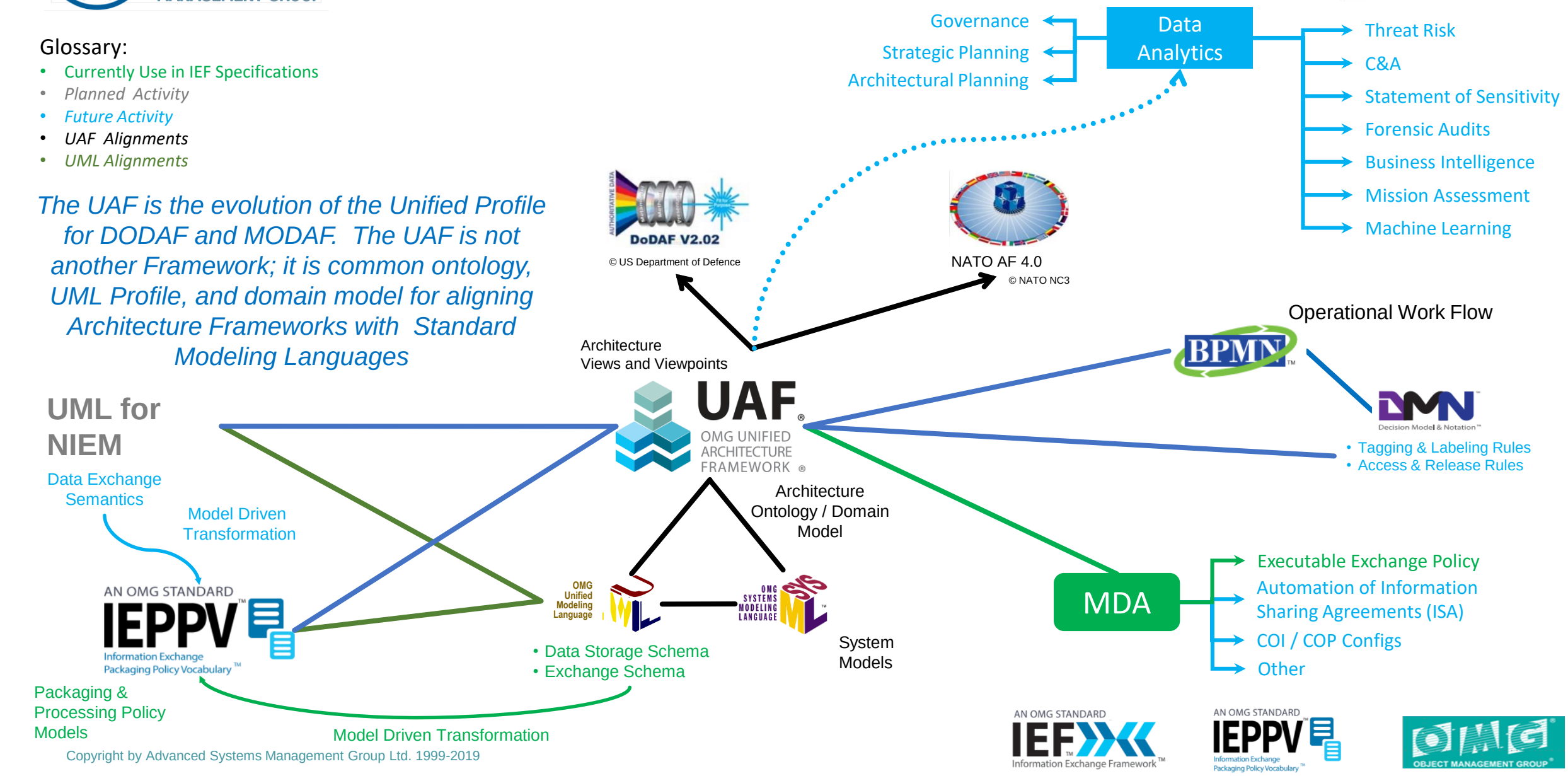


Architecture Driven Information Sharing and Safeguarding

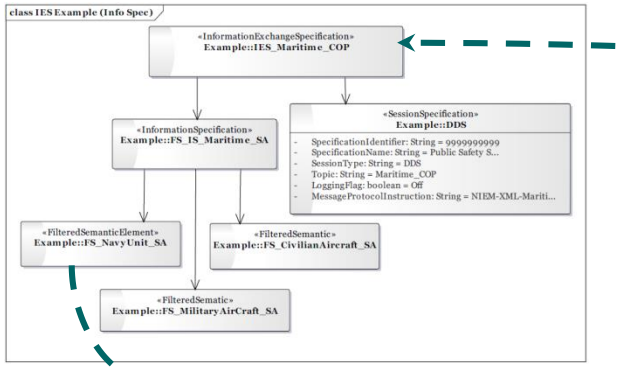
Glossary:

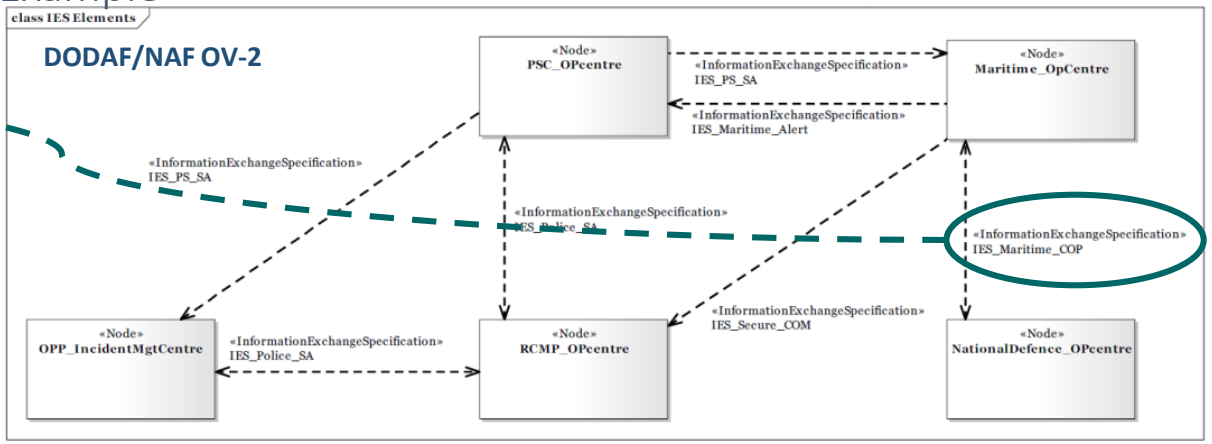
- Currently Use in IEF Specifications
- *Planned Activity*
- *Future Activity*
- *UAF Alignments*
- *UML Alignments*

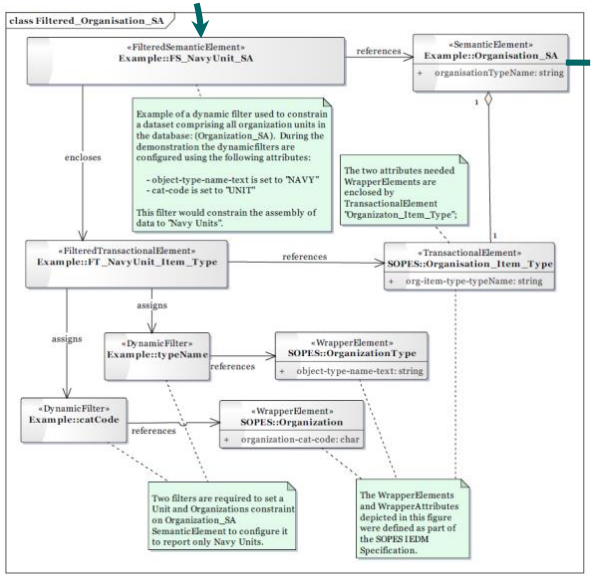
The UAF is the evolution of the Unified Profile for DODAF and MODAF. The UAF is not another Framework; it is common ontology, UML Profile, and domain model for aligning Architecture Frameworks with Standard Modeling Languages

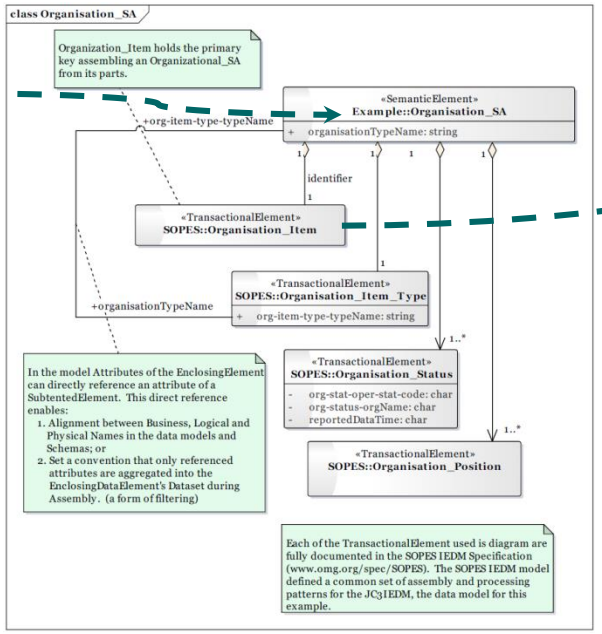


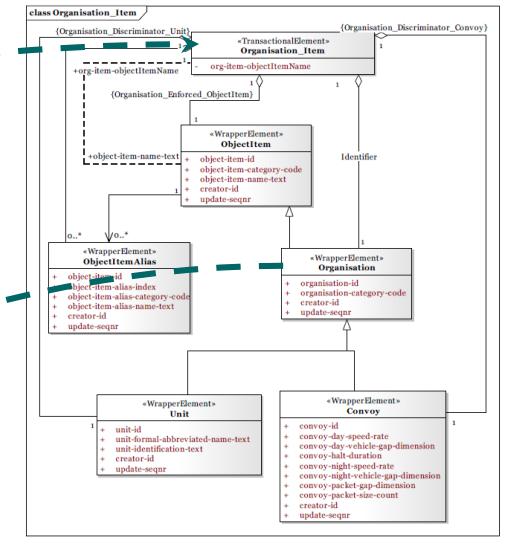
Architecture provides Full Traceability IER to Data Element STANAG 5525 Example

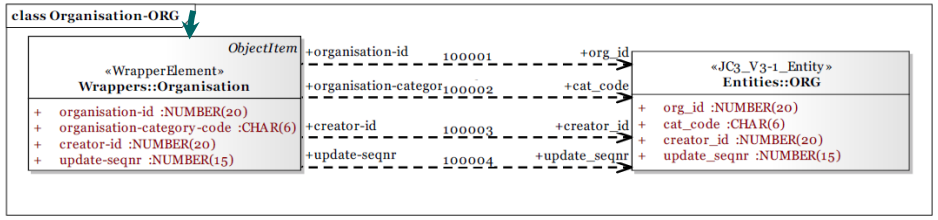












All these models are described in
[Policy Models for Structured Messaging.pdf]

Implementation Status

- IEF-RA (Beta 1) and IEPPV (V1) published by OMG, and IEPPS (initial submission) in development at OMG
- The underpinning specifications have been successfully piloted by Canada's DND and Public Safety
- Invited to presented IEF at the annual NATO TIDE SPRINT event in Norfolk in October 2018
  - NATO is exploring an interoperability exercise in June 2019 as part of the annual NATO CWIX event to demonstrate Data Centric Security around STANAG 4559.
  - Canadian DND has the testing and experimentation, and are in active discussions with J6 and other NATO partners to participate.
  - Next presentation requested at the NATO summit in Finland in January to make final decision on use cases. J6 has expressed strong interest and exploring ways to engage.
  - 2 other DoD components have expressed strong interest (active pilot discussions).
- Undergoing testing and experimentation at CWIX 2018 and 2019 in the ISR and C2 domains
- Most recently we have been approached by an AI company with a strong offering in the supply chain environment, and they are looking for OEM integration of IEF within their AI engine to control data ingestion, and disseminating outcomes based on policy definitions. They see a lot of application within government, financial and healthcare sector.
- And we agree ☺.
- Active IEF demonstrations available at the next OMG meeting in Reston (March 18-22, 2019)

Information Exchange Framework (IEF)

- Standards Specifications
  - http://www.omg.org/spec/IEPPV/
  - http://www.omg.org/spec/IEF-RA/
  - IEPPS RFP was issued Dec 2017 and currently being developed

Mike Abramson

Advanced Systems Management Group (ASMG) Ltd.
Co-Chair C4I DTF at OMG, Co-Chair IEF WG at OMG
265 Carling Ave, Suite 630, Ottawa, Ontario, K1S2E1
Phone: (613) 567-7097 x222
Email: abramson@asmg-ltd.com

Vijay Mehra

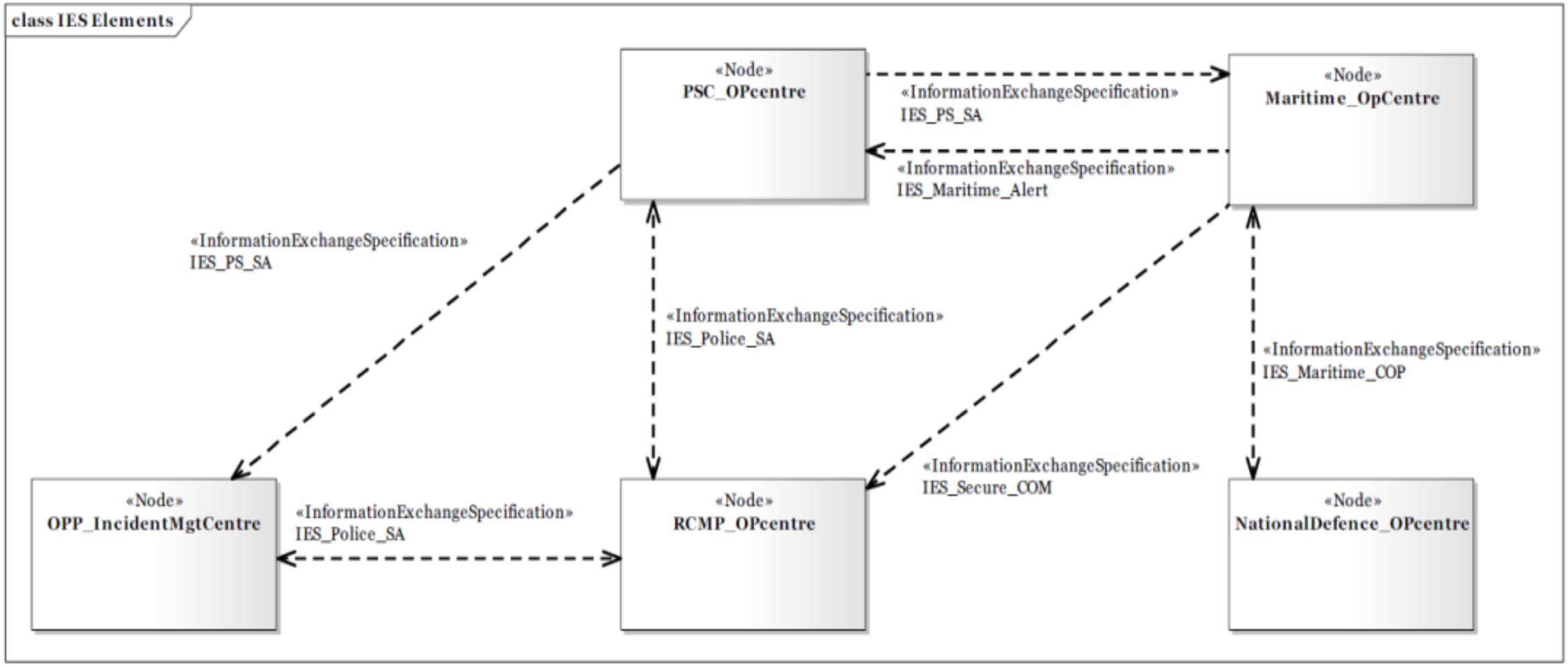
KYM Advisors
Co-Chair IEF WG at OMG
4400 Fair Lakes Ct., Suite 101A, Fairfax, VA 22033
Phone: (571) 510-0930
Email: vijay.mehra@kymadvisors.com

Back-up Slides

IEF Summary

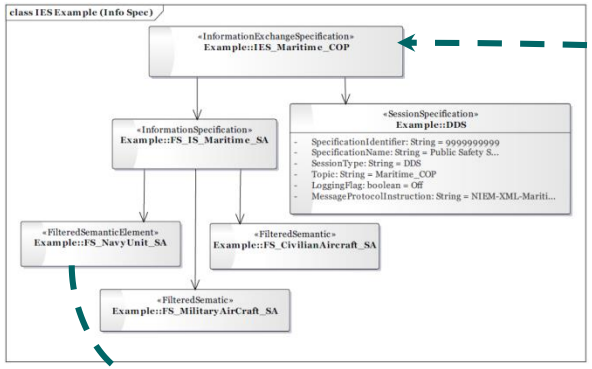
- Framework for integrating security services to provide:
  - Information sharing and Safeguarding (ISS)
  - Data Centric Security
- Policy Driven Data Centric
  - Separates Business, Information Management and Information Technology Concerns
  - Architecture Focused
  - Knowledge Retention
- Evolving set of standards
  - IEF-RA
  - IEPPV
  - IEPPS
- Based on Canadian Innovation

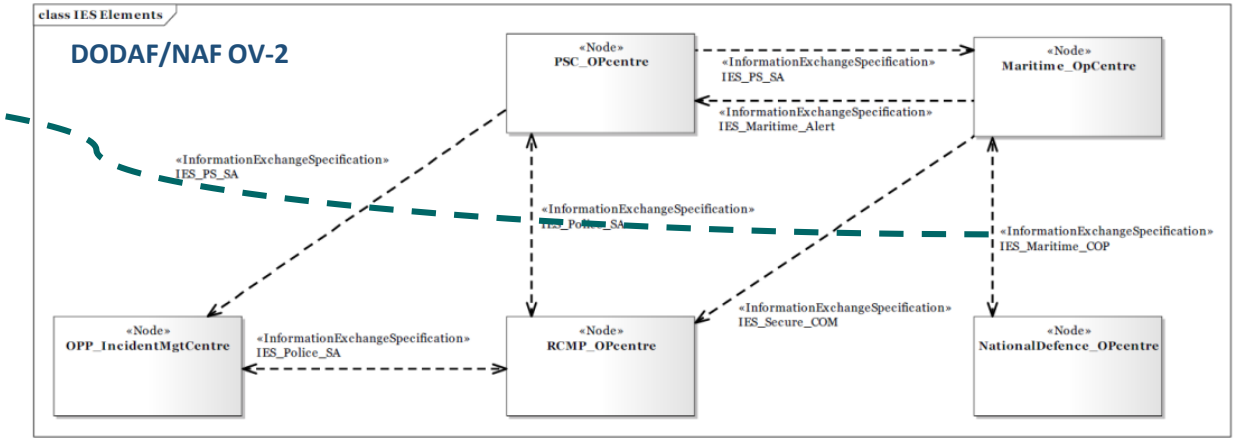
Demonstration Scenario

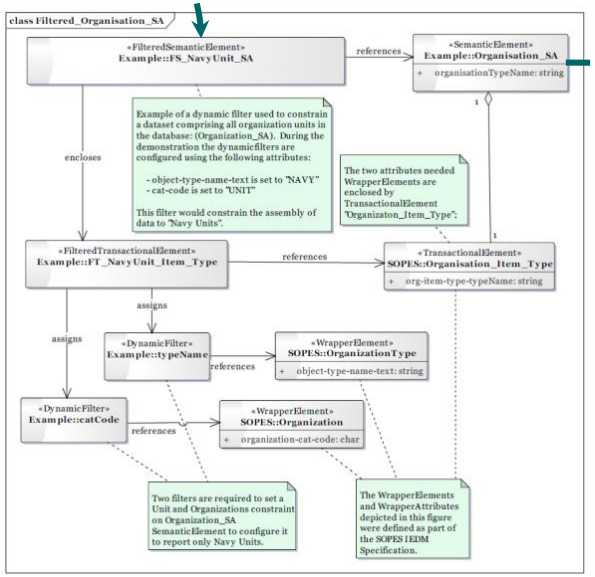


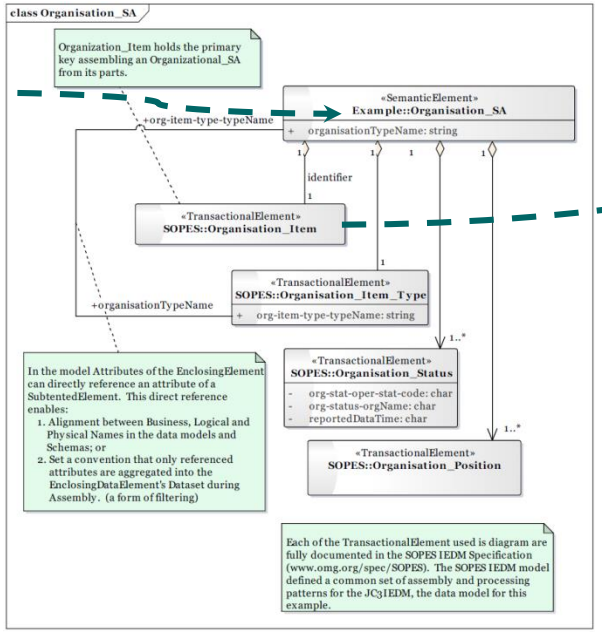
Full Traceability IER to Data Element

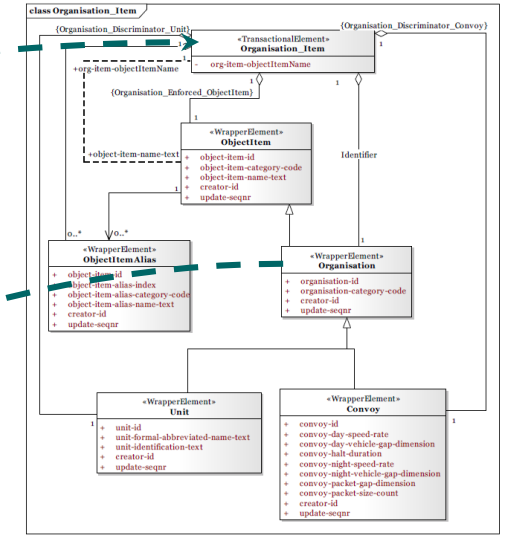
STANAG 5525 Example

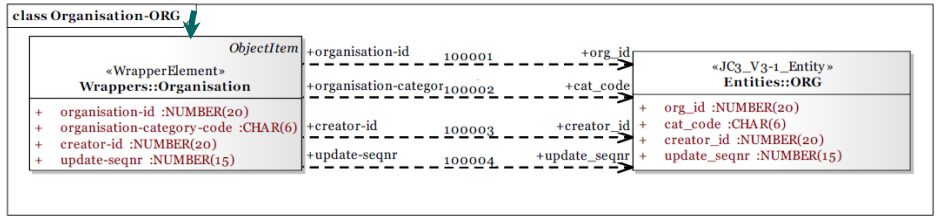






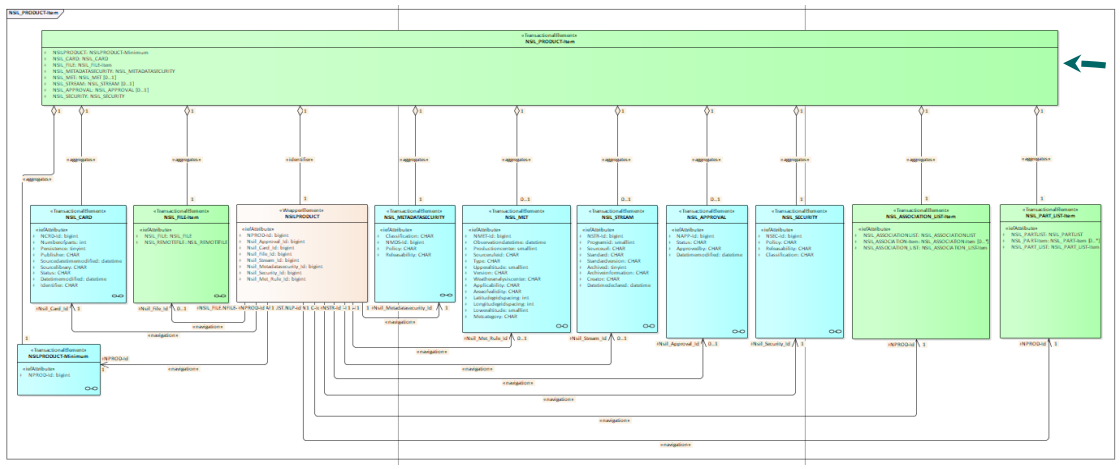






All these models are described in
[Policy Models for Structured Messaging.pdf]

Executable Model for CSD/NSIL View



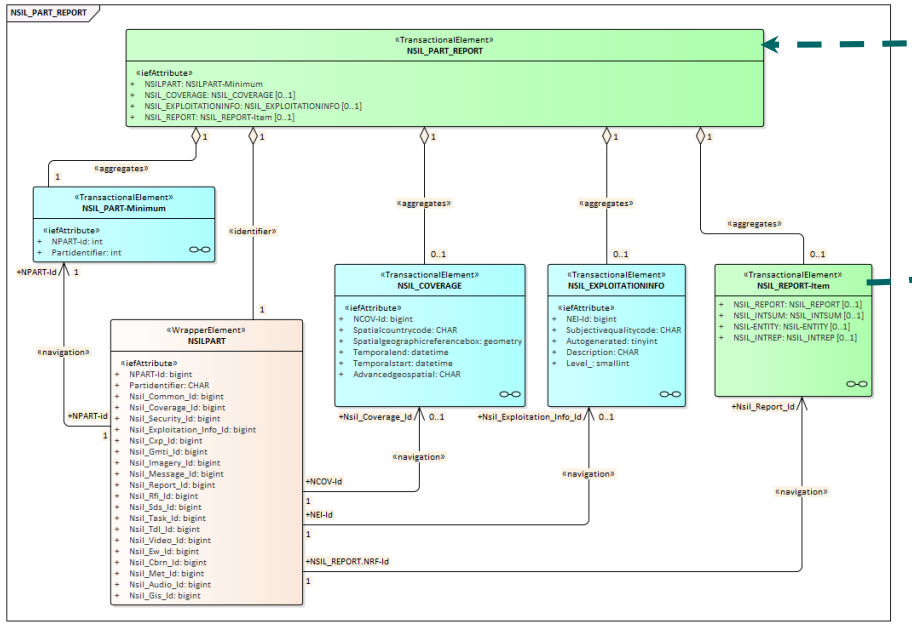
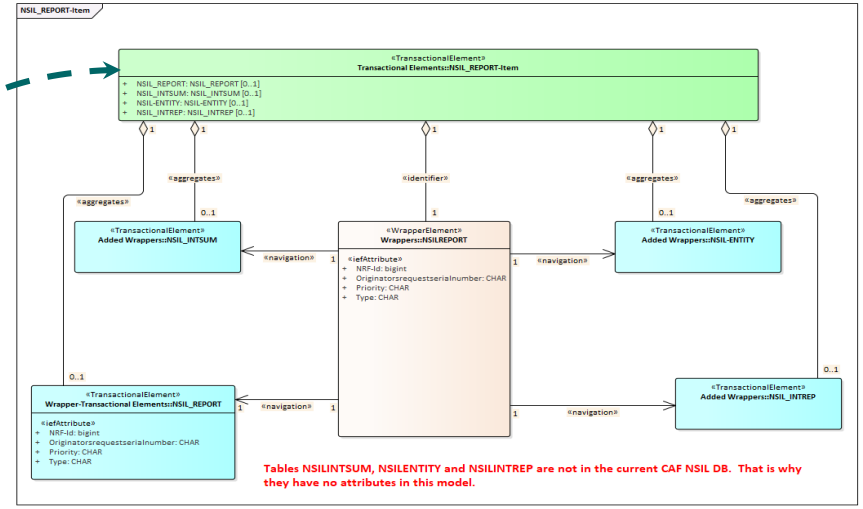
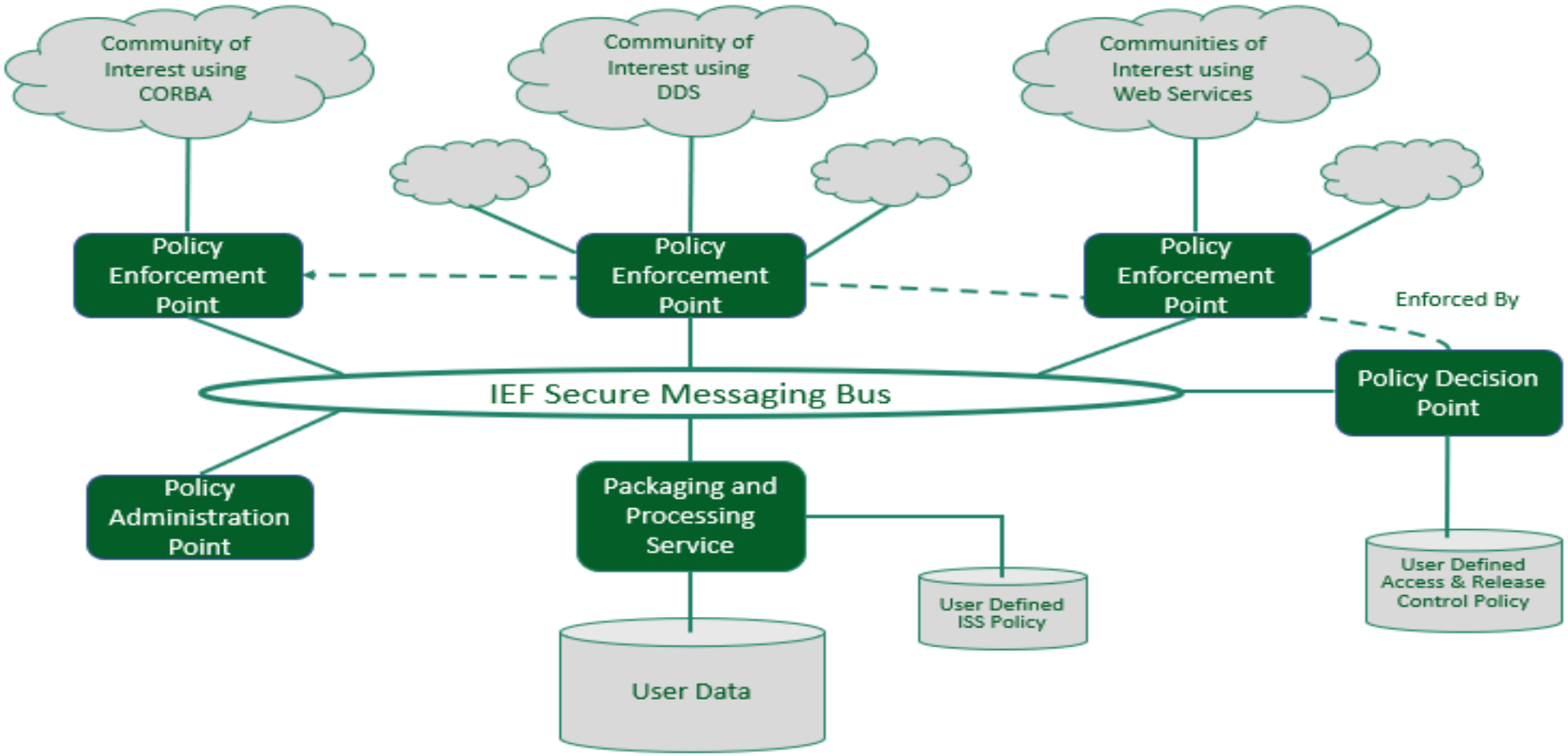


Figure G- 8 NSIL_REPORT_VIEW

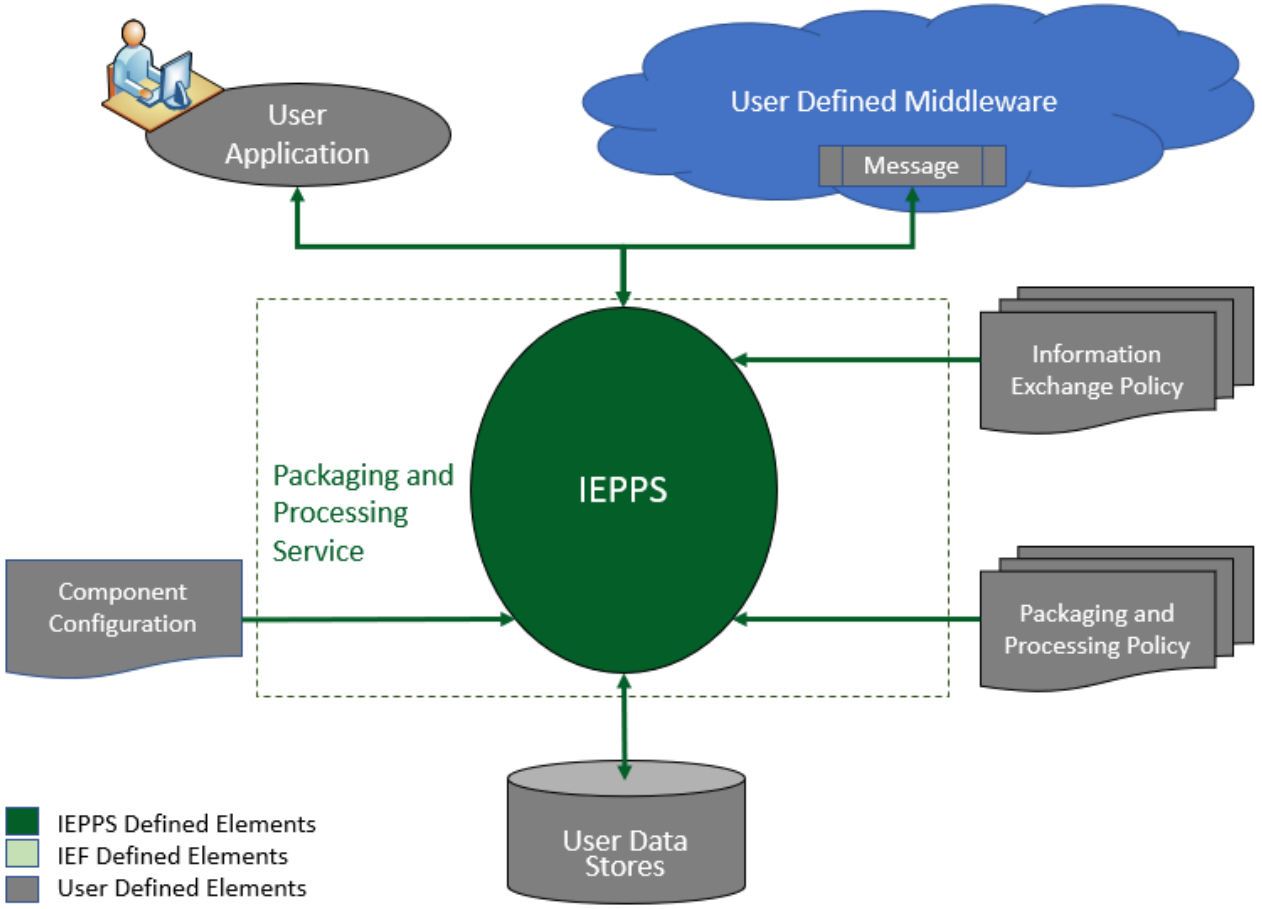


Multiple Integration Channels



Basic Packaging and Processing Services Configuration

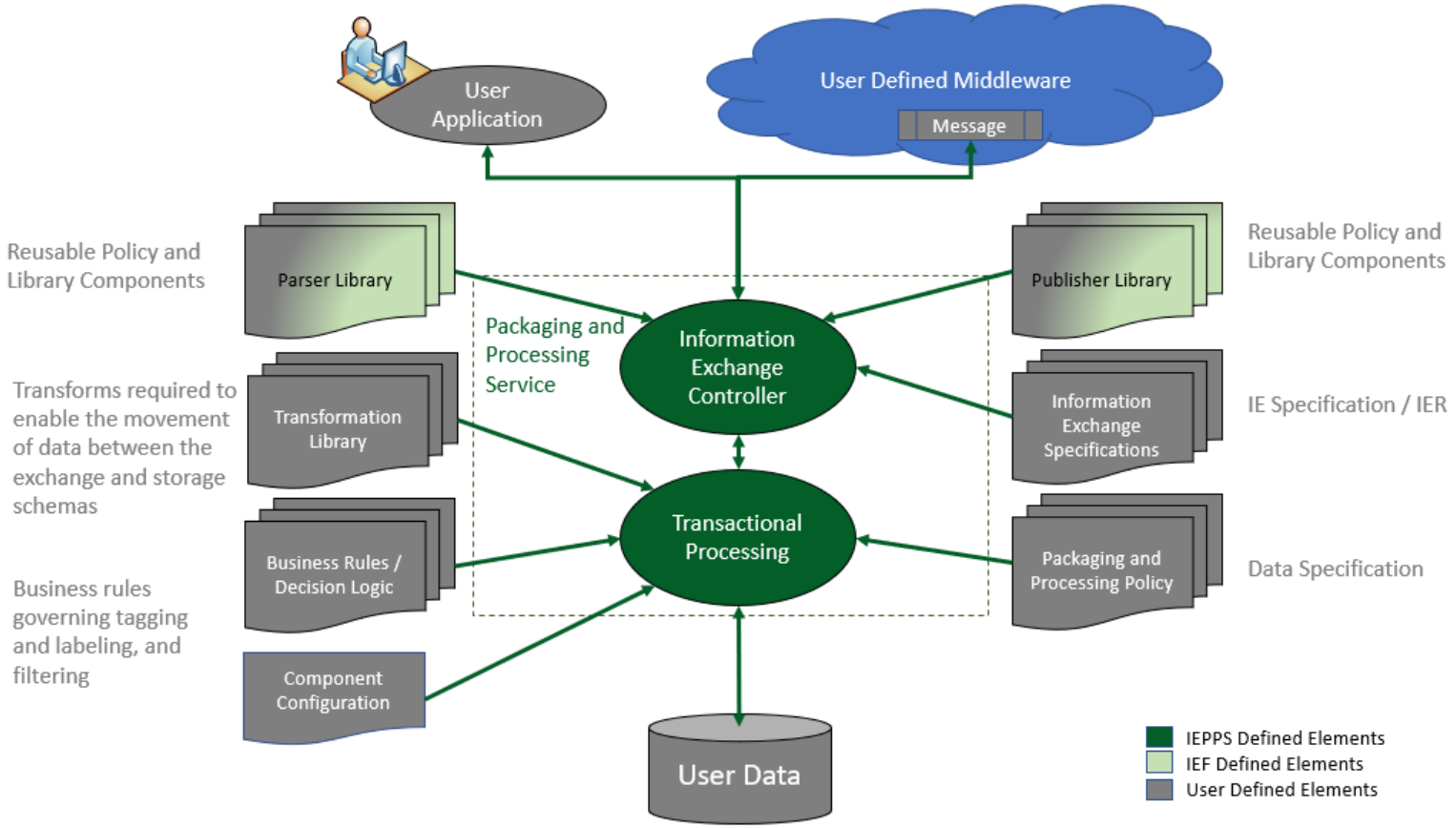
- Policy is separated from the applications implemented to enforce them
- Policies and configuration are loaded from file
- Single integrated component for enforcing information sharing and safeguarding policy



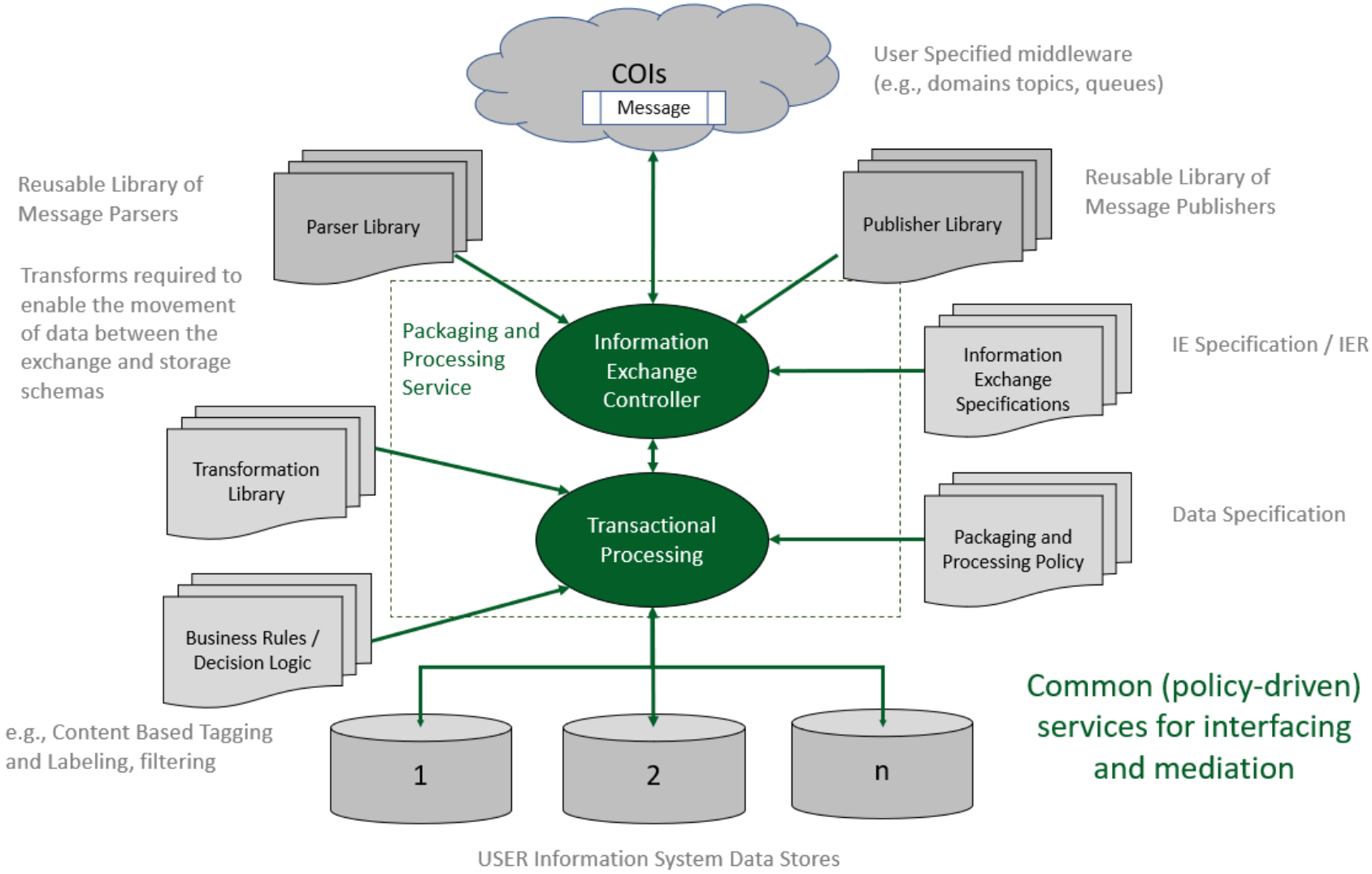
- Typical Use
  - Data service for a User

Extended Capability

- Increases user control over policies, rules and operations governing IEPPS operations
- Increased Separation of concerns
- Increased design and runtime adaptability, flexibility, and agility
- Increased use of Model Driven Architecture



Configurable to Specific Mission Requirements



Integrating IEF Access and Policy Management

- Adds additional Layers of Security
- Adds Runtime administration of Policy