ASMG
ADVANCED SYSTEMS
MANAGEMENT GROUP

Information Sharing and Safeguarding

Policy Modeling for Structured Messaging

M.Abramson /E.Penwill

Contents

Introduction

The following model expands on the example provided as part of the Information Exchange Packaging Policy Vocabulary (IEPPV). It is provided to outline the key elements in the modeling profile provided in the IEPPV Specification.

Scenario

The model presents part of a policy model developed to demonstrate a policy-based data-centric service for structured messaging. To The scenario used is a fictitious event that clearly required the exchange of sensitive information between mission partners who would not normally share the information because it is protected and there is normally no 'need-to-know' or 'need-to-share'.

- Fire on a military ship in domestic waters and a collaborative response:
  - Focus on basic situational awareness (Unit position and status) and visualization, and
  - Visually present the ability to selectively share information, balancing:
    - Need-to-know, and
    - Need-to-share, and
  - Demonstrate the ability to update policies in response to an operational need;
- Demonstrate selective information sharing, based on policy, between 4 mission partners:
  - DND Headquarters,
  - Maritime Operations Centre (operated by the Navy),
  - Government Operations Centre with Public Safety, and
  - Royal Canadian Mounted Police Operations Centre; and
- Demonstrate support for multiple data formats in the same data domain PDU (primary Distribution), SOPES XML (could be converted to a NIEM IEPD).

Demonstration

- Translation of policy instruments into machine executable rules (or Policy Automation);
- Demonstrate flexibility, agility, and sustainability;
- Demonstrate the approach using standards;
  - Architectural Patterns for Information Sharing and safeguarding (e.g., IEPPV),
  - ISS Information Patterns for a specific Domain (SOPES IEDM),
  - Information Specification (MIP JC3IEDM – STANAG 5525),
  - Standardized Messaging (MIP PDU, SOPES XSD),
  - Demonstration Policy-based Packaging Service that uses the IEPPV serializations,
  - Common Object Request Broker Architecture, and
  - Standardized Distribution Mechanisms (DDS).

Policy Modeling

One option offered by the IEF is the use of UML to define information exchange agreements. The IEF offers a UML profile as one of the language implementations for the IEPPV. It is this profile that we use to illustrate the IEF approach to structured data and messaging.

The use of models, in this case UML models provides several benefits:

- A natural integration with enterprise architecture frameworks, which provides the ability to document the relationships of an information exchange specification with supporting resources (e.g., networks, security infrastructure (e.g., cryptographic services, and firewalls), platforms, systems, and services);
- Assist in the capture, maintenance, and retention of institutional memory;
- Deliver data (/metadata) that provides objective information to governance and certification processes, and enables simulation and design analytics.

Within the UML Profile, the IEPPV defines a customized set of stereotypes, tagged values and constraints that facilitate the specification of information sharing agreements that employ structured data and messages. The names of the elements in the scenario are determined by the community, agency or organization developing the policy models.

The following model presents elements of a model that was used to demonstrate the IEF/IEPPV approach. It drew on the policy model developed for the JC3IEDM, as codified in the Shared Operational Picture Exchange Services (SOPES) Information Exchange Data Model (IEDM); *http://www.omg.org/spec/SOPES/*.

Key Policy Model Elements

Information Exchange Topology

The example scenario, below, illustrates key elements of a policy model developed using the IEPPV UML Profile. The model illustrates a set of reusable data patterns that combine to define information exchange (position and status reports) for entities operating in the maritime environment around a multi-agency response to a maritime emergency.

The first figure illustrates the IES topology for four (4) Operations Centres:

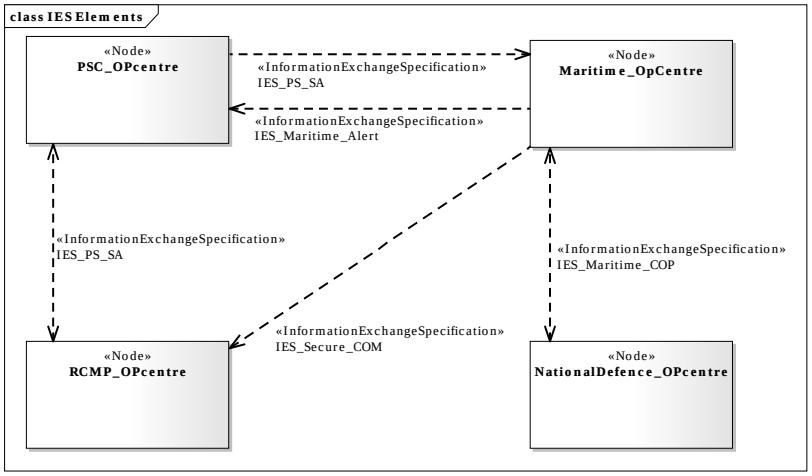
1. Government Operations Centre with Public Safety (PSC_OPCentre);
2. Maritime Operations Centre (MaritimeOPCentre);
3. Royal Canadian Mounted Police Operations Centre (RCMP_OPCentre); and
4. National Defence Operations Centre (NationalDefenceOPCentre).

These operation centres are operated by three separate government departments:

1. Department of National Defence (DND), operating:
    a. MaritimeOPCentre, and
    b. NationalDefenceOPCentre;
2. Royal Canadian Mounted Police (RCMP); and
3. Public Safety Canada (PSC).

Each of these agencies operate under a separate legislative mandate and a combination of common/shared (e.g., Information Sharing Agreements /MOUs) and individual agency rules which are policy instruments about sharing information. Under these legislative regimes, the agency leadership is

responsible for protecting their information holdings and controlling the release of information. Any release must be traceable to and in accordance with the appropriate policy instruments. Until the development of the IEPPV and its integration into an architecture framework, users did not have a framework and tools for applying policy to a specific data domain, or combination of data domains (aggregated, integrated or fused) without human intervention. As the need for inter-agency information sharing expands and with the sheer volume of the data environments, real-time human intervention is impractical. The complexity of many of the data environments complicates an already impractical strategy.



Information strategies such as NIEM, EDXL, CAP, HL7, and MIP provide an excellent first step. However, to make these XML based strategies successful, users must also be provided with the strategies, techniques, and tools to apply policies to their specific data domain, provide the data needed to trace policies to information sharing, automate the enforcement of those policy applications and then audit the transaction of each of the policies.

What is represented is the use of IEPPV Information Exchange Specifications to define operational exchanges between the Nodes. Optionally, we can also use Information Specification or Filtered semantic patterns to define these exchanges. Each approach offers different benefits to the user. (e.g., reuse of patterns) From this linkage to the operational exchanges and nodes, we get the inherent linkages to the systems, services, interfaces, ports and networks represented in other views and viewpoints.

As illustrated, the example scenario includes four (4) nodes (operation centres) and five (5) different Information Exchange Specifications (IES):

1. Public Safety Situational Awareness (IES_PS_SA);
2. Maritime Alerts and Warnings (IES_Maritime_Alert);
3. Police Situational Awareness (IES_Police_SA);

The information environment selected for the example model is based on two separate but complementary data standards: the JC3IEDM (STANAG 5525: containing 273 Entities & 1493 Attributes) used as the foundation for NATO coalition situational awareness; and the SOPES IEDM that provides a standard set of data patterns for interaction with the JC3IEDM representing 192 data patterns in 16 subject areas. The use of the JC3IEDM and SOPES models demonstrates that the approach also has the ability to subset a large, complex and highly normalized data environment – employing only those facets pertinent to the mission or an individual role or function. Providing this capability reduces the need to proliferate fit to purpose databased and spreadsheets, and increases opportunities to integrate/fuse information covering multiple subject areas (e.g., planning, logistics, and situational awareness) into a shared/integrated data environment.

This figure integrates the IEPPV and the Operational View 3 (OV-3) of the Unified Profile for DODAF and MODAF and a broader description of the operational Architecture. It is this integration with architecture frameworks and tools that provide:

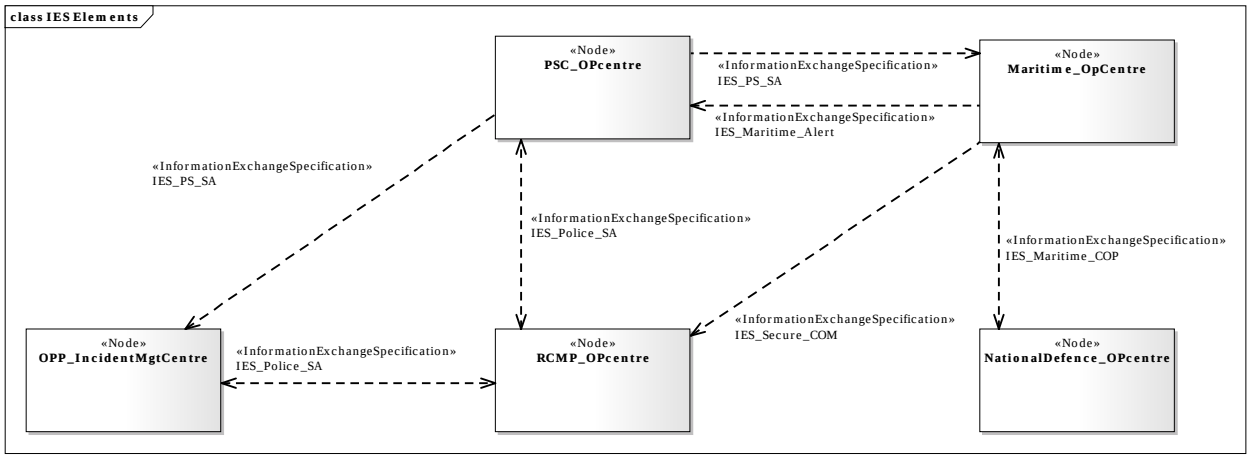
1. The traceability of policy models to requirements and policy instruments, missions and operations;

2. The alignment to other entities in the enterprise (e.g., solutions, networks, nodes, systems, applications, and interfaces);

3. The metadata needed to enable analytics, modeling and simulation and auditing; and

4. The retention of institutional knowledge.

4. Secure Communication Channel between National Defence and the Royal Canadian Mounted Police (RCMP) (IES_Secur_Com); and
5. Maritime Common Operating Picture (IES_Maritime_COP).



From this initial operational configuration, the user can reuse IES patterns to rapidly extend the sharing community. In this case two IES agreements (IES_PS_SA & IES_Police_SA) are reused to integrate an Ontario Provincial Police (OPP) Incident Management Centre (OPP_IncidentMgtCentre).

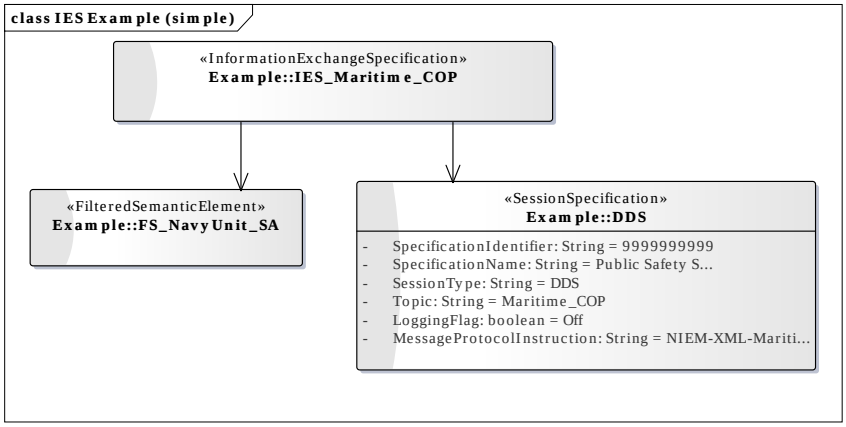
Information Exchange Specification (IES)

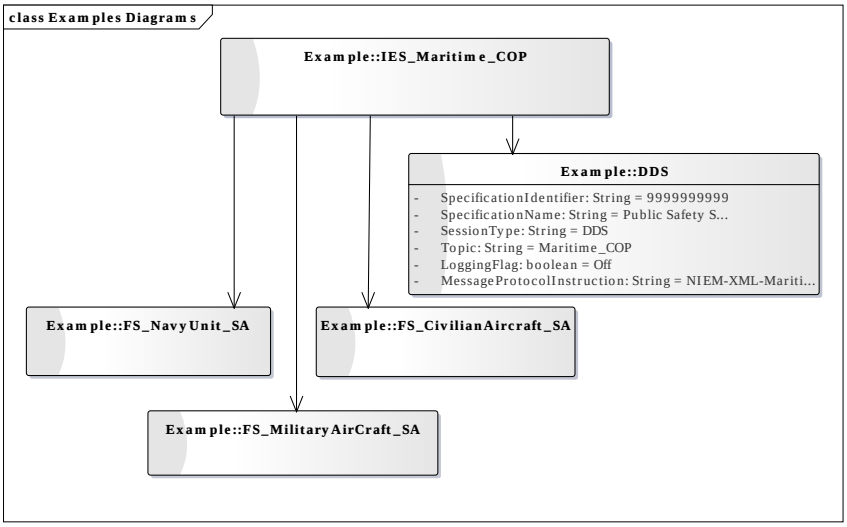
An IES enables a user to assign one or more information elements (e.g., message or filtered semantic) to a specific session or communication channel. The information element defines rules for packaging and processing a releasable and semantically complete set of data. The session defines the interface, middleware and protocols the policies authorize to carry the information from the producer to authorized recipient(s).

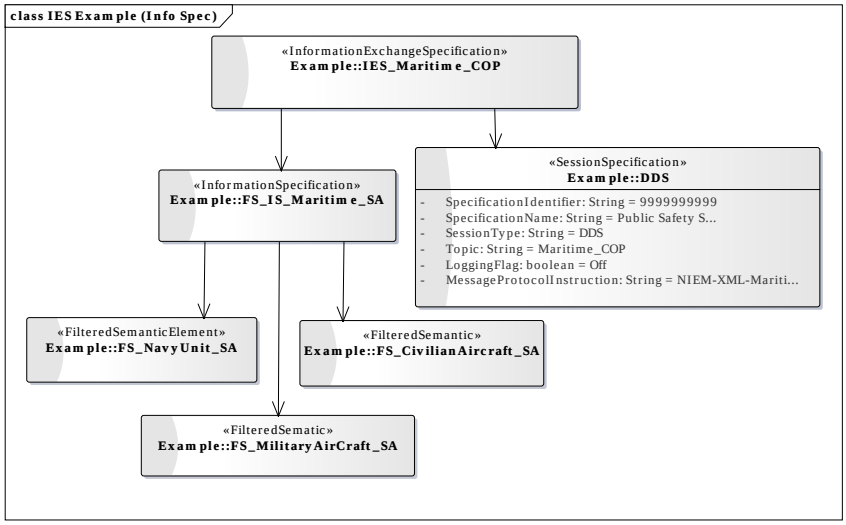
Note: The Use of the IES is an independent and optional conformance point for the IEPPV specification. If using the DODAF/UPDM there are other options in the operational and system views for documenting the characteristics of the information exchange services (e.g., Information Exchange Requirements or port characteristics). The IES is provided for IEPPV implementations that do not offer integration into an architecture framework such as DODAF and profile such as UPDM.

As mentioned, the Information-Specification, Message or Filtered-Semantic can also be attached to the operational exchange.

The following figure illustrates the simplest IES structure. In this case, the IES assigns a single Filtered-Semantic-Element to a DDS Topic that carries a NIEM XML document using the PS_SA Schema. The PS_SA schema would be further documented in a NIEM IEPD (Information Exchange Package Documentation), the prescribed process and possibly the UML Profile for NIEM (or NIEM Profile). In this instance, the user is expecting the session, or services linked to that session, will structure and format the data set assembled through the Filtered-Semantic-Element in accordance with the NIEM-XML-Maritime_COP schema.





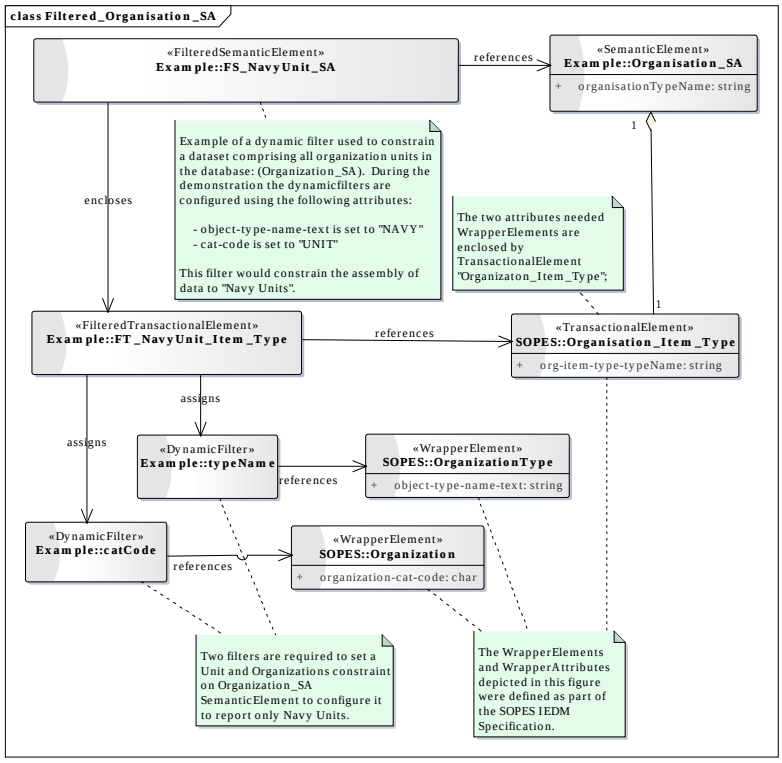


When executed by the IEF Policy-based Packaging Service (IEPPS) the FilteredSemantic (FS_NavyUnit_SA) results in the assembly (aggregation, transformation, Tagging/labeling and filtering) of data and information elements describing a Navy Unit position and status. The resulting data assembly would then be sent to the Session_1 services to structure and format the XML document and then to the DDS writer for the Maritime_COP Topic.

The simple pattern from the previous figure can be extended. Multiple information elements (FilteredSemanticElement) can be linked directly to an IES (upper) or grouped as an Information Specification (lower). Each of these patterns will result in the identical exchange of information. If the data is requested, or a data change in the underlying data triggers the release of updates, the information element will be assembled and placed into the session. The benefit of using the Information Specification is the provision of a reusable pattern that can be linked to multiple session types, resulting in the same data servicing multiple agreements: delivering event driven (data change) global

updates (all authorized recipients get the data in the agreed format) increasing the flexibility and utility of the models.

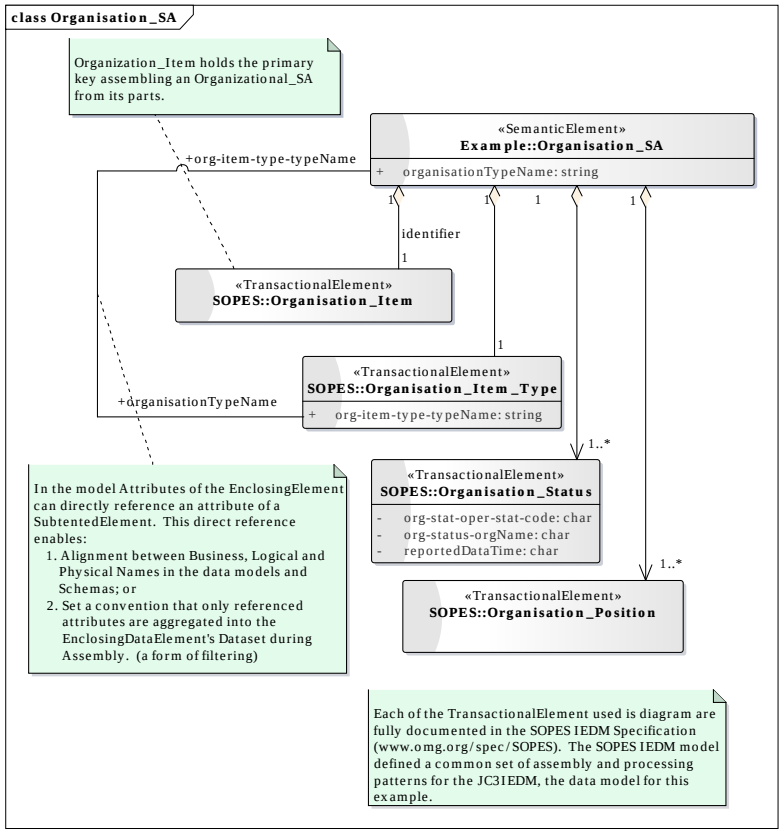
An Information Specification can be used to define standard information sharing requirements that may require different messaging protocols by domain (e.g., situational awareness, logistics, supply, and operational planning) or recipient (e.g., coalition partner, other government department, private sector). The grouping of messages can then be assigned to different sessions (e.g., different distribution services, message protocols, and quality of Service (QoS)) in order to service multiple partners or communities.



FilteredSemantic & FilteredTransactional

The FilteredSemantic groups or encloses a set of run-time configurable filters that overlay Semantic Transactional Elements. The use of filter overlays allow users to define a single data pattern for each message type – and then tailor that pattern for the specific security, QoS, recipient or community need. The Filtered Semantic and Filtered Transactional combine to identify which attributes in the Semantic Element pattern can be configured at runtime – to tailor the assembly to those items releasable to the user or community.

As illustrated above, the FilteredTransactionalElement references a single TransactionalElement from which it draws its internal patterns. The filters are assigned to attributes within the TransactionalElements in the EnclosingSematicElement (e.g., NavyUnit_SA). It is the subtended FilteredTransactionalElement that assigns the filters to the attributes



within the Semantic Pattern.

The FilteredTransactionalElement assigns runtime (user configurable) filters to a specific TransactionalElement enclosed by the SemanticElement. In this case, NavyUnit data is derived from the SemanticElement (Organization). An "Organization" is a generic Semantic Pattern used to assemble data pertaining to an organization contained within an instance of a JC3IEDM database. To limit (filter/redact) the assembly process to specific "units", a type of organization, and further restrict that to a Navy Unit, one needs ability to configure two specific domain filters:

1. cat-code in Wrapper Element "Organization"; and
2. object-type-name-text in WrapperElement "OrganizationType.

In order to restrict the reports to only those from NAVY UNITS:

1. The object-type-name-text must be set to "NAVY"; and
2. The cat-code must be set to "UNIT".

Both of these WrapperElements are contained within one TransactionalElement, "Organization_Item_Type". Thus, only one FilteredTransactionalElement is needed.

Note: *The exclusive use of static filters would require a separate Semantic Element to be developed and deployed for each type of UNIT and provide no flexibility for the User. By using a Filtered Semantic Element, only one pattern needs to be deployed and the specific reporting pattern can be established at runtime. The latter provides greater flexibility and agility but requires more knowledge and effort from operators. The IEF leaves the selection of the approach to the determination of the user.*

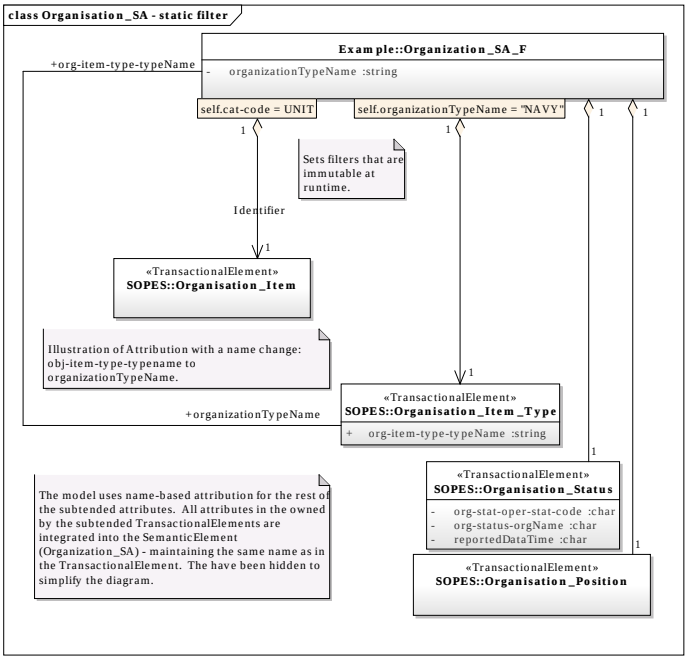
Static filters can also be applied to the Transactional Element aggregation arc. It performs the same function during the aggregation of the subtended elements in the semantic pattern. Static filtering at the transactional level may be of interest to information assurance, security and privacy specialists who may want to restrict the aggregation of sensitive elements on the data set as early in the process as possible. Filtering the transactional and wrapper elements at the lowest level in the aggregation provides the opportunity to filter out (redact) data elements before the aggregate crosses a specific sensitivity threshold.

SemanticElement

A Semantic Element groups or encloses a set of TransactionalElements (Data Patterns) that in combination define a set of rules for assembling a complete and meaningful dataset for the stakeholder (user or community); e.g., Organization: rules for assembling data pertaining to all organizations maintained in an instance of a JC3IEDM database). Within the context of the JC3IEDM, a Unit is a type of Organization. The types of information reported on any organization is specified or defined by the stakeholders. For the purpose of this example, only tombstone data, status and position are reported or exchanged.

The Transactionals needed to assemble organization information are drawn from the SOPES IEDM specification:

- OrganizationalItem (SOPES IEDM Sub-clause 10.14.7);
- Organization Item_Type (SOPES IEDM Sub-clause 10.14.8);
- Organizational_Status (SOPES IEDM Sub-clause 10.14.14); and
- Organizational Position (SOPES IEDM Sub-clause 10.14.12).



SemanticElement (staticFilters)

The user has the option to embed the filters in the semantic patterns and create a static pattern that reports position and status on all NavyUnits. This approach would provide no flexibility for the operator to change the reporting or reuse the pattern to report on other types of units in the environment. Noting that the Organizational_SA, without any filters, would report on any organization (including units) in the environment. The user could, if required, set additional filter options to be configured at runtime (as above) and further restrict the reporting on NavyUnits.

As illustrated, in the static form of filtering, the "aggregation" arcs from the Subtended Element (Organizational_Item and Organizational_Item_Type) have been qualified. This will restrict the assembly of data elements to only those that have a cat-code of "UNIT" and OrganizationTypeName of "NAVY". This form of filtering would yield the same results and the Filter Semantic Element (NavyUnit_Item_Type) after it is configured in the runtime environment.

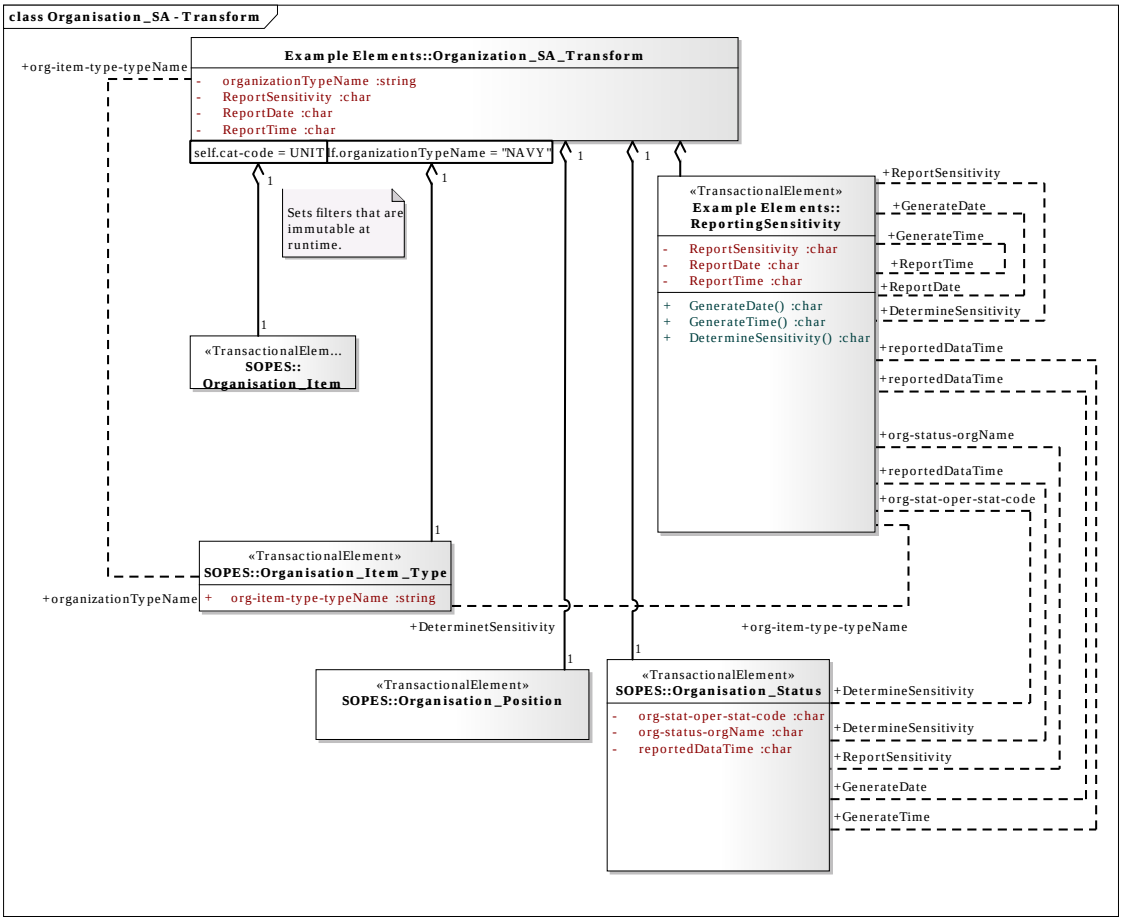
SemanticElement (with Markings and Transformations)

In practice, the aggregation of data may be performed:

- Based on common names (tags) in the tag-value paring of the attributes in the enclosing and enclosed element;
- Based on the total aggregation of all attributes in the enclosed element; or
- Based on a fully attributed model as illustrated below.

Fully attributing the model enables the user to selectively aggregate attributes, change the naming convention of attributes (e.g., from physical, to logical, business names) as they are aggregating, transform data values or mark data aggregates (e.g., embed/bind security, privacy tags; constraints and/or warning orders).

The IEPPV provides data transforms during the aggregation of a transactional. In the example (below), the policy model includes three (3) transformations. Two are used to extract the data and the time from the "reportedDateTime" attribute in the SOPES IEDM Organization_Status Transactional Element. The two (2) transforms (i.e., UML Operation) are named ReportDate() and a ReportTime(). The policy model also required the generation of a reporting sensitivity mark. The DetermineSensitivity() transform computes the sensitivity of the reporting data based on the OrganizationName (org-item-type-typeName),its reportedDateTime ; and its status (org-stat-oper-stat-code). The commutation of the sensitivity would be modeled in UML in the same manner as any operational algorithm. This mark is then used to filter the aggregation of organization data to redact the package of data assembled.

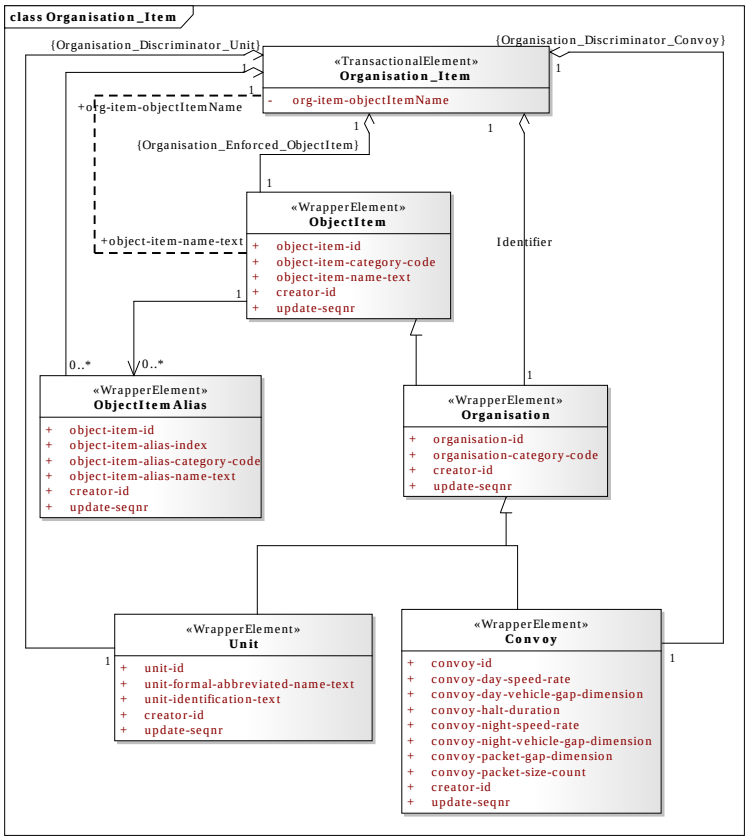


TransactionalElement

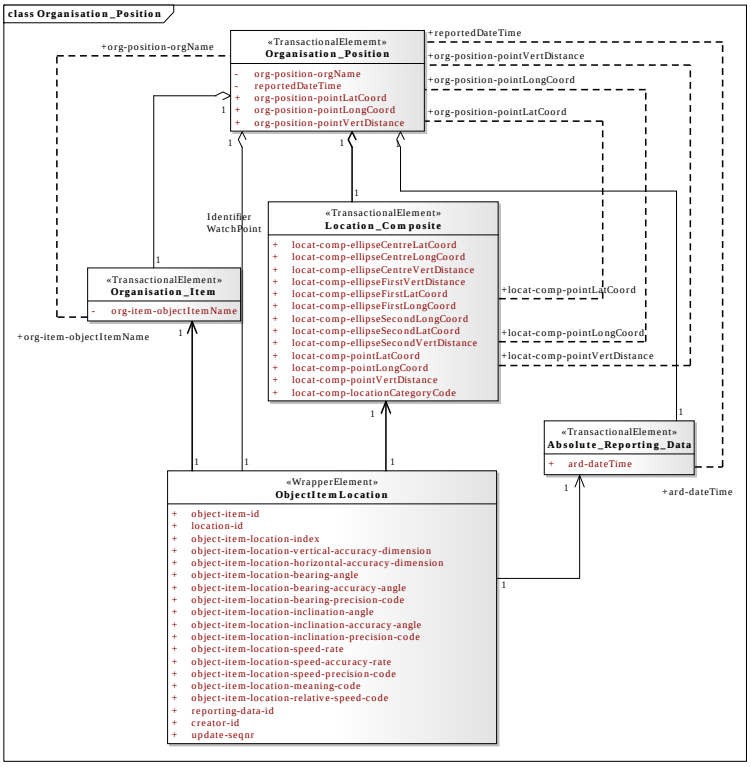
From this point the model builds up data patterns that assemble (aggregate, transform, mark and filter) the data elements and attributes from the underlying data model. The examples present were taken from the SOPES IEDM. Only the Stereotypes were changed to reflect the new IEPPV vocabulary. The changes in stereotype naming convention had no impact on the underlying concepts.

Organization_Item

The "Organization_Item" represents one of 192 reusable TransactionalElements in 16 subject areas defined by the SOPES IEDM for the JC3IEDM. It illustrates a



TransactionalElement that aggregates data directly from the tables in the database through the WrapperElements (described below).



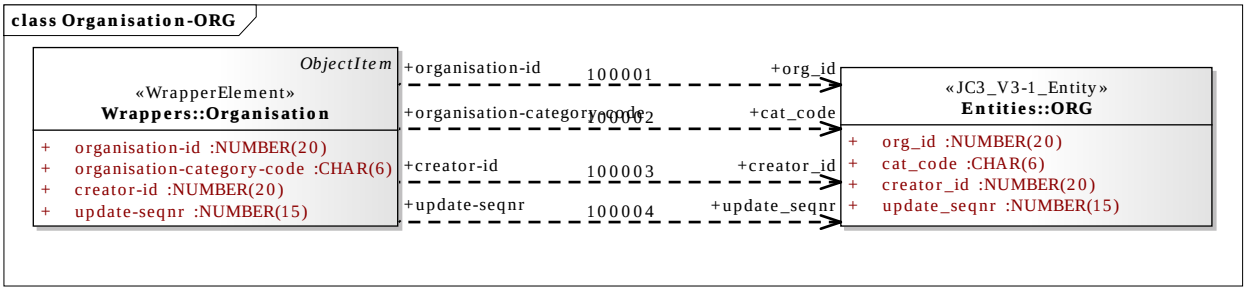
Organization Position

As with the Organization_Item, the Organization_Position has been taken from the SOPES IEDM. It illustrates the hierarchical nature of the IEPPV modeling patterns and TransactionalElements can enclose both TransactionalElement and Wrapper Elements in the same pattern.

WrapperElement

The following Figure illustrates the mapping of a WrapperElement and the physical table definition of the JC3IEDM. This mapping enables a transformation of physical names in the database to the logical name in the policy models. The only functions assigned to a WrapperElement at runtime are Read (Get) and Write (Put) against the one table they are mapped to. The order in which the tables must be written to avoid referential conflicts is derived from the TransactionalElements during the translation of the model to machine executable rules/instructions, and encoded in the rule set.

As illustrated, WrapperElements makes direct reference to the physical tables in the JC3IEDM and connects the assemble rules, represented by the semantic and transactional patterns, to the actual DataElements in the environment.



Using the Message Construct

Within the IEPPV context, a message (structured message) is the process of aggregating multiple information elements. The IEPPV provides a hierarchy of messaging structures that allow users to package different combinations of information elements in increasing levels of complexity.

Table 1 - Additional Messaging Elements

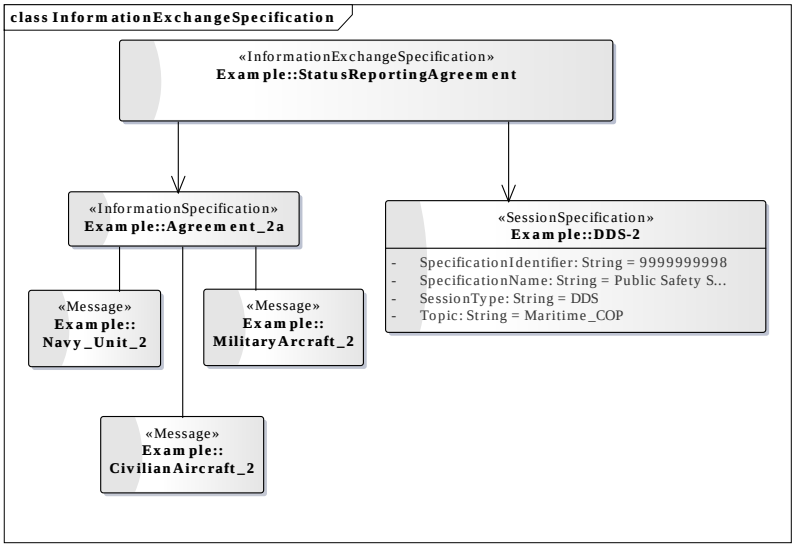
Message Element	Sub-element	CP-2a	CP-2b	CP-2c	Uses a FilteredSemanticElement as the constructor
Message		1	1	1	
Message Metadata		1	1	1	Yes
Submitter Metadata			1	1	Yes
Information Payload		1	0	0	Yes
Information Package		0	1	1..n	
	Information Package Metadata		1	1	Yes
	Information Payload		1	1	Yes
	Digest		1	1	Yes
	Attachment Summary			1	
	Linkages			1	
	Narrative Text			1	
	Rendering Instruction		1	1	
Attachment		0..1	0..n	0..n	

Information Exchange Specification & Information Specification

The Information Exchange Specification plays the same roles as illustrated above. In the model the FilteredSemanticElement is replaced by a Message. The Message construct enables the user to:

- Add markings (/metadata) to the message;
  - Security Tags;
  - Privacy Tags,
  - Warning Orders;
  - Other Restrictions;
  - Key Token(s).
- Add unstructured attachments; and
- Rendering or release instructions for the individual messages.

The ability to establish exchange agreements supporting multiple message types (e.g., NIEM IEPDs) enable users to configure communities of interest with a rich set of semantics.

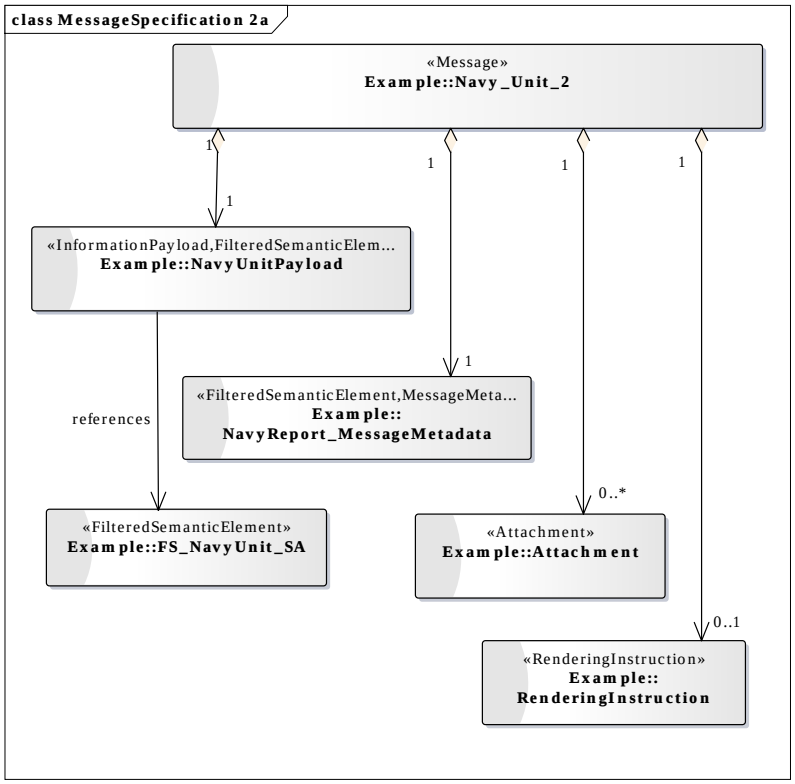


MessageSpecification

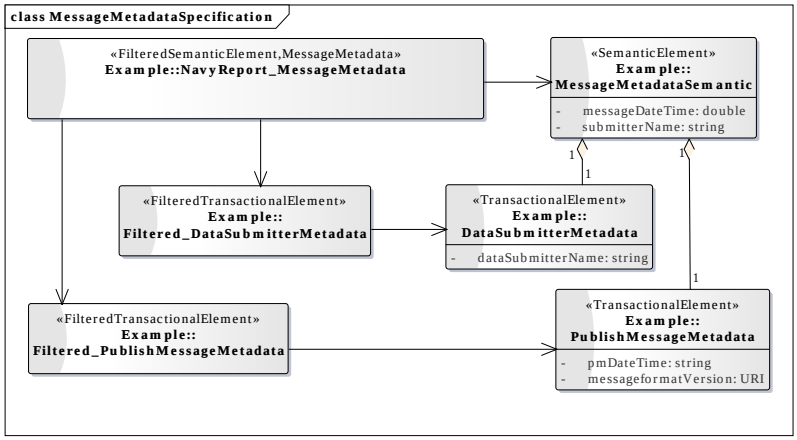
The Message specification includes:

- An InformationPayload that references a FilteredSemanticElement;
- MessageMetadata specification representing a SemanticElement that assembles the metadata for the message;
- A link to the set of attachments to the message; and
- A set of RenderingInstructions that direct the preparation of the message payload and attachments.

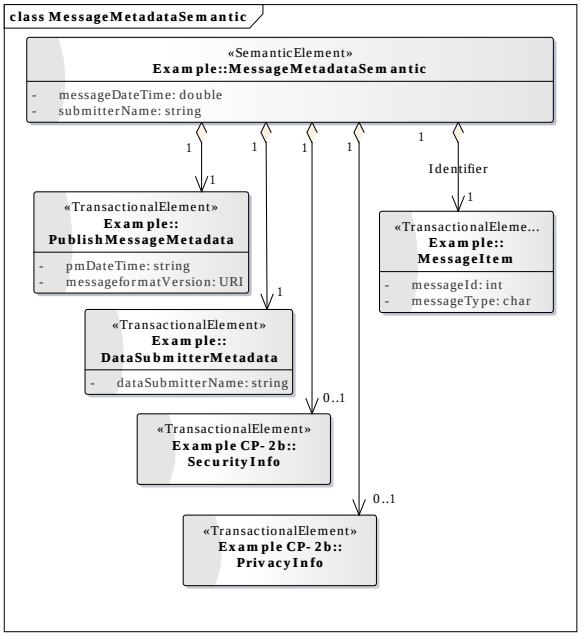
The use of the Message construct enables users to establish information exchange agreements that utilize multiple message types, each with its own: message protocol (e.g., XSD), metadata and attachment specifications, and RenderingInstructions.



MessageMetadata



The assembly of MessageMetadata is performed in the same manner as other semantic elements using a FilteredSemanticElement. As illustrated Message Metadata references MessageMetaDataSematic, which in turn aggregates DataSubmitterMetadata (TransactionalElement) and PublishMessageMetadata (TransactionalElement). These combine to assemble the metadata needed for the message. When the message is rendered (structured and formatted), the Information Payload, metadata, and attachments that were assembled separately, are integrated into the message for release.



The MessageMetadata is another use of the SemanticElement. It is used to assemble (aggregate, transform, Filter) metadata elements for a message.

Additional IEPPV Elements

The IEPPV provides the option to extend the Message construct to support a complex packaging structure.

SOPES IEDM Modeling Profile vs. IEPPV

The SOPES IEDM Specification defined a modeling profile (Annex A), that outlined the modeling techniques used to develop a standard set of data patterns for processing the JC3IEDM. The SOPES profile outlined the core elements for the UML Profile formalized in the IEPPV. The IEPPV updated some of the vocabulary (see table below), formalized several of the proposed extensions, and added the message constructs. However, if the stereotypes in the SOPES IEDM model were updated in accordance with the table below, the model would be fully conformant with the IEPPV. The SOPES models used in this paper were modified to conform to the IEPPV.

Table 2 - IEPPV to SOPES IEDM Concept Mapping

#	IEPPV Concept	SOPES and UPDM Concept
1	SemanticElement	Semantic
2	TransactionalElement	Transactional
3	WrapperElement	Wrapper
4	FilteredSematicElement	FilteredSemantic

Table 2 - IEPPV to SOPES IEDM Concept Mapping

#	IEPPV Concept	SOPES and UPDM Concept
5	FilteredTransactionalElement	FilteredTransactional
6	Filter	DynamicFilter
	Filter	StaticFilter
7	InformationExchangeSpecification	Contract

For More Information

Mike Abramson, ASMG Ltd.
265 Carling Ave, Suite 630, Ottawa, Ontario, K1S2E1
Fax: 613-231-2556
Phone: 613-567-7097 x222
Cell: 613-797-8167
Email: abramson@asmg-ltd.com

Supporting data

Definitions

Adaptive Information Sharing	The ability to selectively share information content based on operational or business context (e.g., roles, relationship, risks, threats, severity, scale, and trust). This includes the ability of users (manually) or systems (automatically) to adjust active ISS policies to accommodate changes in business and operational context.
Asymmetric Information Sharing	The ability to share content with different communities, agencies or individuals conforming to legislative, regulatory, policy, contractual or service level requirements – while leveraging standard or shared protocols, interfaces and infrastructure.
Caveat	A warning or proviso of specific stipulations, conditions, or limitations to the sharing of data and information elements.
Community of Interest	A group of people interested in sharing information and knowledge in a particular topic or domain of discourse.
Data Centric	Enforce policies/rules against individual data assets; often referring to metadata or tags included within an information asset.
Decision Advantage	Enable commanders and/or decision makers, based upon information advantage and situational understanding, to make effective and informed decisions more rapidly than their adversary, thereby allowing one to dramatically increase the pace, coherence, and effectiveness of operations.

Information Advantage	Enable the provision of information needed to develop a degree of control in the information domain that permits the conduct of operations without effective opposition.
ISS Policy:	Principles, rules, and guidelines formulated or adopted by an organization to share and safeguard information holdings. They are designed to influence and determine all ISS decisions and actions, and all ISS actions take place within their boundaries.
Policy automation	The use of software services to automate the selection of a course of action (decision) and the execution of that selected course of action (execution).
Metadata	A form of structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information.
Policy	A definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions (Webster Merriam Dictionary). ISS policy guides the determination of which data elements are releasable under a given set of conditions.
Policy automation	The use of software services to automate the selection of a course of action (decision) and the execution of that selected course of action (execution). For the purpose of this paper, this refers to the actions to be taken by IEF services (including decision and enforcement points) to share and safeguard information assets.
Policy-Driven	A process through which user defined policy instruments are translated into machine readable rules (/instructions) and enforced by software services and systems. This process results in full traceability from policy instrument to implementation (policy decisions and enforcement).
Policy Instrument	Formal document describing a plan of action by an individual agency or community to handle information sharing and safeguarding (e.g., legislation, regulation, memorandum of understanding and service level agreements).
Quality Information	Provision of high-quality information tailored to the needs of the decision makers': a. **Accurate.** Information that exactly, precisely, and correctly presents availability, usability and deploy-ability of C4ISR capability, systems and services; b. **Authoritative**. information that is recognized or accepted as being true or reliable; c. **Relevant.** Information content tailored to specific needs of the decision maker; d. **Timely.** Information provided when and where it is needed to support the decision making process; e. **Usable.** Information is presented in a common functional format, easily understood by the decision makers and their supporting applications; f. **Complete.** Information that provides all necessary and relevant data (where available) to facilitate a decision;

g. **Concise**: Information is provided in a form that is brief and succinct, yet including all important information;
h. **Trusted.** Information that is accepted as authoritative by stakeholders, decision makers and users; and
i. **Secure.** Information is protected from inadvertent or Malicious Release to unauthorized persons, systems or organizations.

Releasable Data	A dataset that conforms to the policy rights of the data receiver according to the relevant policy instruments.
Responsible Information Sharing	Compliant with legislation, regulation and policy; consistent with agency strategy, policy and direction; and accountable through governance and oversight: • Maximize the volume, variety and quality of information that is discoverable and accessible by authorized users; • Protect sensitive (classified, private, confidential and legally significant) information from unauthorized access/release and tampering; • Protect information sources and processing methods; • Protect civil rights/liberties; and • Ensure that information is assured in its content, safe in transmission and use, and safeguarded from the threat of malicious acts, unauthorized use, clandestine exfiltration or compromise by remote intrusion.
Structured Data	A data set defined by fixed fields within a record or file. Relational databases and spreadsheets are examples of structured data.
Semantically Complete	Preserving the explicit meaning and intent of the information during packaging, processing and exchange.
Semi-Structured Data	A form of structured data. A data set that is not fixed in location like traditional database records, but are structured, because the data are tagged and can be accurately identified (e.g., XML Document).
Sensitive Information	Information elements identified as classified, private, confidential or legally significant.

Acronyms

DODAF	Department of Defense Architecture Framework
IEF[i]	Information Exchange Framework
IEF RA[ii]	Information Exchange Framework Reference Architecture
IEPPV[iii]	Information Exchange Packaging Policy Vocabulary
IEPPS[iv]	Information Exchange Policy-based Packaging Service(s)
IEPMS[v]	Information Exchange Policy Management Service(s)

ISE	Information Sharing Environment
ISS	Information Sharing and Safeguarding
JC3IEDM[vi]	Joint Consultation, Command, Control and Intelligence Information Exchange Data Model
MODAF	Ministry of Defense Architecture Framework
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NIEM[vii]	National Information Exchange Model
PM-ISE[viii]	Project Manager Information Sharing Environment
SOPES	Shared Operational Picture Exchange Services
SOPES IEDM[ix]	SOPES Information Exchange Data Model
UPDM[x]	Unified Profile for DODAF and MODAF

Endnotes

[i] http://www.asmg-ltd.com/sect_5a.html#Information_Exchange_Framework_%28IEF%29

[ii] IEF RA RFP, http://www.omg.org/cgi-bin/doc.cgi?c4i/2013-9-11

[iii] IEPPV, http://www.omg.org/spec/IEF-IEPPV/

[iv] IEPPS, see IEF RA, http://www.omg.org/cgi-bin/doc.cgi?mars/2014-3-17

[v] IEPMS, see IEF RA, http://www.omg.org/cgi-bin/doc.cgi?mars/2014-3-17

[vi] JC3IEDM, https://mipsite.lsec.dnd.ca/

[vii] http://www.niem.gov

[viii] http://www.ise.gov

[ix] SOPES IEDM, http://www.omg.org/spec/SOPES/

[x] UPDM, http://www.omg.org/spec/UPDM/