Common Object Interoperability Layer – OMG SOPES and IEF Initiatives

Architecture Based Approach to Semantic Interoperability and Information Protection

The Common Object Interoperability Layer (COIL) is a policy or rules based data service that delivers the core capabilities described as part of the Object Management Group's (OMG) Shared Operational Picture Exchange Services (SOPES) Request for Proposal (RFP) from June 2004. COIL generalizes and implements these concepts in a manner that enables its application across commercial, public, military and security applications. COIL provides a programmable, distributable data service which enforces architectural models which define data and information patterns (semantics) described in UML Class diagrams. One example of such semantics are XML information exchange messages (e.g., CAP, NIEM, EDXL) . COIL provides the following capabilities in relation to these semantics:

- To aggregate structured data to form community defined semantics;
- To de-aggregate data sets into structured sub-elements;
- To integrate or marshal data elements into community defined data patterns (semantics);
- To filter data based on domain values (e.g., category codes, tags, labels, ranges, other);
- To guard data based on information patterns, simple or complex, including multiple domain values and filters;
- To manage the release of information (semantics) based on their association to
  - Information exchange Requirements (IER),
  - Information Exchange Agreements (IEA),
  - Service Level Agreements (SLA), or
  - Communities of Interest (CoI);
- To marshal data to service an application program interface (API) that connects to user selected data store technologies;
- To marshal data to service an application program interface (API) that channels data to user selected distribution technologies and protocols;
- To trigger the aggregation and release of information, with or without user intervention, providing event triggered global update of information to each participant to an IER, IEA, SLA and/or CoI.

C4I and MARS Initiatives

In the fall of 2001 the Object Management Group (OMG) kicked off a standards initiative to develop a set of standards for information sharing and collaboration during real-world operations, involving coalition, allied and/or multi-agency resources. The initiative was named "Shared Operational Picture Exchange Services (SOPES)", and it sought to align engineering, service and technical standards to address the needs of the emergency and public security communities. The central objective for this initiative was the specification of model driven interoperability services, which exploited policy (/rules) driven technologies (e.g., intelligent agents) to tackle information management (IM) challenges of dynamic real-world environments; and accomplishing these objectives in a secure and trusted manner.

Market surveys and technology reviews continue to identify the current middleware solutions provide reasonably support to stable commercial domains (e.g., commercial applications), but:

a. Are far too rigid and brittle to effectively address rapidly changing requirements of the emergency, public security and/or military domains;

b. Do not provide the data fidelity needed to address the handling of sensitive (classified, confidential or private) information in coalition and multiagency environments; and/or

c. Were challenged by the variations in stakeholder data/information needs and rapid changes in operational context (e.g., community structure, reporting paths, roles and responsibilities, threats, risks, objectives and intent).

The SOPES problem statement sought to address:

1. A longstanding requirement for the capacity to quickly, efficiently, safely, and confidently exchange operational information amongst coalition and civil respondents in Emergency, Crisis and Major Event Operations;
2. A set of generic technical and service standards that enable information sharing at all levels of the of a response team utilizing (where possible) existing standards and specifications;
3. A set of information services that enforce community and/or agency rules governing the composition and release of information within and between heterogeneous information systems;
4. As set of information services that assure that information is collected, processed, released and stored in a manner that enforces security, confidentiality privacy, Information Assurance, and Quality of Service requirements for dynamic operating environments

In 2003 the Taskforce published a conceptual architecture (Figure 1 – 2010 version) for the proposed standards. The architecture was intended to guide the development of RFPs and the alignment of RFPS to standards being developed by other communities. The central concepts for the SOPES architecture included:

- **Architecture centered development**, to assure that interoperability specification and design is aligned to community, enterprise and system elements. And that these concepts and constructs aligned with architecture frameworks including: DODAF, MODAF, NAF, DNDAF, etc… This alignment to architecture helps to assure that interoperability specifications and design are documented and institutional memory retained – and that this information can be used to support testing and certification requirements.
- **Use of standard modeling notation**, to assure that assures that practitioners have ready access to training, there is familiarity of the constructs within the stakeholder communities, and there are off-the-shelf tools to support the process. Using models provides the opportunity to adopt Model Drive Architecture (MDA) transformations to develop the Platform Specific and Implementations.
- **Policy driven services**, to separate information exchange and information protection rules from the software applications or services comprising the exchange mechanisms. This approach has proven far more adaptive and flexible than traditional software development and maintenance. The combination model and policy drive capability provided the metadata needed to support MDA and the ability to maintain and modify policy in an operational system.
- **Reuse of architectural components**, to provide the opportunity for the for community members to share system definitions and designed and promote interoperability at all stages of development. And to deliver fully traceable architecture and design data to testing and certification processes.
- **Off-the-shelf Capability**, to develop and or align open standards to provide off- the-shelf products and services to a community challenged to muster resources for IM, IT and communication capability.

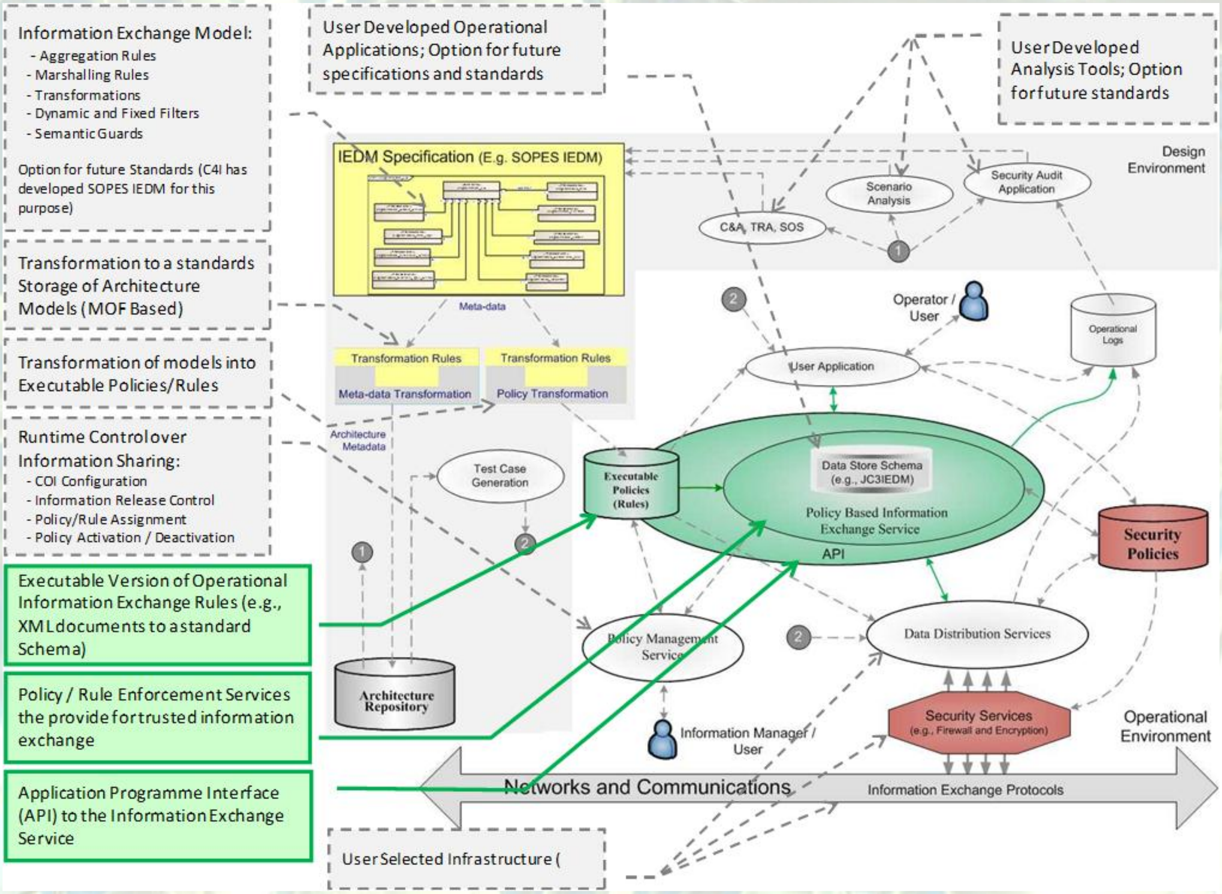
Information Exchange Model:
- Aggregation Rules
- Marshalling Rules
- Transformations
- Dynamic and Fixed Filters
- Semantic Guards
Option for future Standards (C4I has developed SOPES IEDM for this purpose)
Transformation to a standards Storage of Architecture Models (MOF Based)
Transformation of models into Executable Policies/Rules
Runtime Control over Information Sharing:
- COI Configuration
- Information Release Control
- Policy/Rule Assignment
- Policy Activation / Deactivation
Executable Version of Operational Information Exchange Rules (e.g., XML documents to a standard Schema)
Policy / Rule Enforcement Services the provide for trusted information exchange
Application Programme Interface (API) to the Information Exchange Service
User Developed Operational Applications; Option for future specifications and standards
User Developed Analysis Tools; Option for future standards
IEDM Specification (E.g. SOPES IEDM)
Meta-data
Transformation Rules
Transformation Rules
Meta-data Transformation
Policy Transformation
Architecture Metadata
Design Environment
Scenario Analysis
Security Audit Application
C&A, TRA, SOS
1
2
Operator / User
Operational Logs
User Application
Test Case Generation
Executable Policies (Rules)
Data Store Schema (e.g., JC3IEDM)
Policy Based Information Exchange Service
API
Security Policies
1
2
Policy Management Service
2
Data Distribution Services
Architecture Repository
Information Manager / User
Security Services (e.g., Firewall and Encryption)
Operational Environment
Networks and Communications
Information Exchange Protocols
User Selected Infrastructure (

Figure 1 – IEF Conceptual Architecture

This conceptual architecture supports the a notional policy development cycle (Figure 2 – 2010 version). The C4I and MARS Taskforces were focusing seeking to support the growing numbers operationally-based exchange semantic specification. These specifications and standards now includes:

- Military efforts:
  - Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM)
  - Multilateral Interoperability Program (MIP) XML
  - Universal CORE (UCORE)
  - C2 CORE
- Emergency Management Information Standards
  - Common Alerting Protocol (CAP)
  - Emergency Data Exchange Language - Distribution Element (EDXL-DE)
  - Emergency Data Exchange Language - Resource Messaging (EDXL-RM)
  - Emergency Data Exchange Language - Hospital Availability Exchange (EDXL-HAVE)
  - Cyclone Warning Markup Language (CWML)
  - Tsunami Warning Markup Language (TWML)
  - People Finder Interchange Format PFIF
  - Tactical Situation Object TSO
  - Nation Information Exchange Model (NIEM)
- Geospatial Standards

  - GeoRSS
  - Geography Markup Language (GML)
  - Web Feature Service (WFS)
  - Web Mapping Service (WMS)
  - Sensor Observation Service (SOS)
  - SensorML
  - Sensor Planning Service (SPS)
- Other Evolving Standards
  - Date/Time (ISO 8601:2004 Representation of dates and times)
  - NIEM (The National Information Exchange Model (NIEM),)
  - Healthcare (HL7 (emergency Response and Public Health))

Note: This is not a complete list – each market survey identifies an increasing number of organizations developing these specifications.

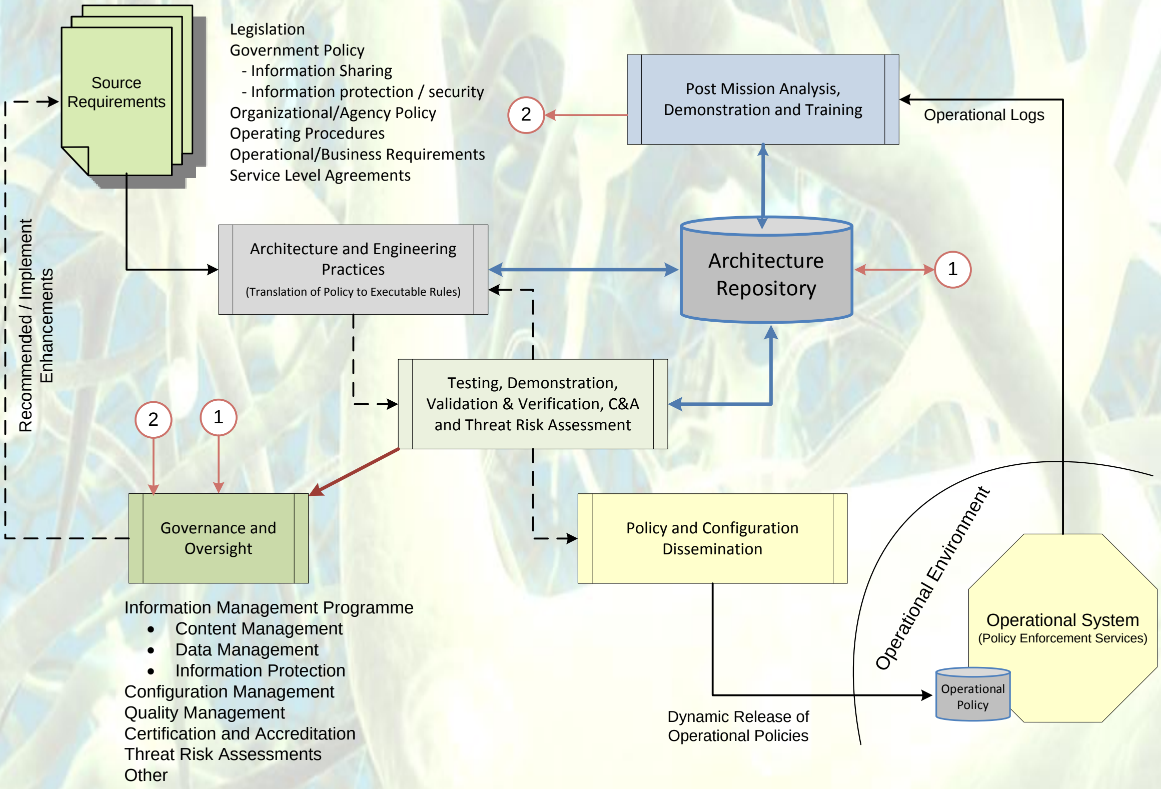
Source Requirements
Legislation
Government Policy
- Information Sharing
- Information protection / security
Organizational/Agency Policy
Operating Procedures
Operational/Business Requirements
Service Level Agreements
2
Post Mission Analysis, Demonstration and Training
Operational Logs
Architecture and Engineering Practices
(Translation of Policy to Executable Rules)
Architecture Repository
1
Recommended / Implement Enhancements
2
1
Testing, Demonstration, Validation & Verification, C&A and Threat Risk Assessment
Governance and Oversight
Policy and Configuration Dissemination
Operational Environment
Operational System
(Policy Enforcement Services)
Operational Policy
Dynamic Release of Operational Policies
Information Management Programme
• Content Management
• Data Management
• Information Protection
Configuration Management
Quality Management
Certification and Accreditation
Threat Risk Assessments
Other

Figure 2 – Policy Life-cycle

The process and technology standards adopted or developed OMG (C4I and MARS) seeks to address architecture and engineering processes, technologies and tools to facilitate the specification, design, development, implementation testing and certification of information system interoperability in multi-agency and coalition communities. The processes and products are being promoted as core elements of architecture frameworks and supporting tools. The elements of information exchange policies (Figure 3) enable:

- Model Driven Architecture processes to translate architecture models into software executable and enforceable policies (rules).
- Policy (rule) based services for:
    - Data Aggregation and marshalling,
    - Data Transformation,
    - Data and Semantic validation;
    - Information Protection (Filters and Guards),
    - Tag and label processing,
    - Selective release of information based on receiver accreditations, and
    - Adapting operations of services to real-works context and intent;
- Model based testing; and
- Analysis and decision support applications and services
    - Certification and Accreditation (C&A),
    - Threat Risk Assessment,
    - System Assurance,
    - Test Case and Data Generations,
    - Security Audit, and
    - Other

User Semantics
User Exchange Syntax

Community of Interest Exchange Agreements
Community of Interest Semantics
Community of Interest Exchange Syntax
Community of Interest Exchange Protocols

Re-useable Information Building Blocks
- Construction (Aggregation / Marshalling) Plans
- Data Transformation
- Domain Filters
- Construction Constraints

Community of Interest Taxonomy
- Domain Business Rules
- Domain Values
- Domain Attributes
- Tags and Labels
- Data Structures & Relationships

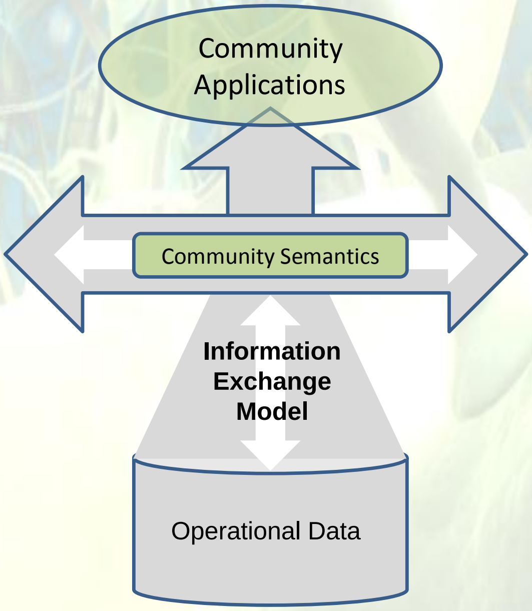

Figure 3 – Information Architecture Requirements

Progress SOPES and IEF Standardization Efforts

In late 2004 OMG C4I initiated three RFPs for standardization:

1. **SOPES Information Exchange Data Model** targets a set of reusable data patterns and constrains complying with the exchange on information using the JC3IEDM. The specification was sponsored by (Office of the Secretary of Defense (OSD) DDR&E AS&C; Office of the Secretary of Defense (OSD) Network and Information Integration (NII) [ICCTS]; US Joint Forces Command USJFCOM; NATO Consultation Command and Control Agency (NC3A); US Army, CIO G3/5/7 and 6; Institutes for Defense Analyses (IDA); Naval Undersea Warfare Center, Division Newport (NUWC); and Canadian Department of National Defence Information Management Group (IM Group), Enterprise Information Security Environment is scheduled for ratification summer 2010. The Multilateral Interoperability Programme (MIP) recognizes the United States efforts, through this specification, to broaden awareness and adoption of the JC3IEDM by industry and interfacing agencies and organizations. Beta 1 Specification can be found at http://www.omg.org/spec/SOPES/1.0/Beta1/. The Specification provides: 190+ data patterns (& constraints) covering 100% of the JC3IEDM in 16 subject area; 2 generic XSDs for the individual data patterns; java classes for the verbose XSDs; UML model; and A modeling profile for data aggregation and information protection data patterns aligned to DODAF, MODAF and NAF. This Specification will complete FTF in June 2010.

2. **SOPES Information Exchange Mechanism (IEM)**_targets a technical specification for a policy based data service and policy language. As this RFP was socialized within the OMG it was realized that the RFP had a broader application than C4I. The RFP was rescinded and moved to the Middleware and Related Services Taskforce under the Platform Technology Committee. The Information Exchange Framework (IEF) was established to take up this effort. A new RFP is scheduled to be release Fall 2010 – Named Information Exchange Service (IES – OMG Document. This RFP will be seeking:
   a. An information exchange service that enforces the semantic and business rules for the aggregation and marshalling of structured information.
   b. The functions of an application program interface (API) that enables the data service to be integrated into:
      i. User applications, functions and services,
      ii. Data Distribution Services / Middleware (e.g., CORBA, DDS, SOA and Web Services),
      iii. Logging Services, and
      iv. Enterprise or community Security Services (optional);
   c. The schema for the policies/rules enforced by the information exchange service requested in this RFP.

3. **SOPES Policy and Rules Management**_target a technical specification for a policy management service that will allow communities to disseminate and manage information exchange policies in the operational domain. As with the SOPES IEM, this RFP was moved to MARS. A new RFP is scheduled to be release Fall 2010. This RFP will be seeking:
   a. Policy Dissemination (/Distribution) Service that provide a community with the ability to exchange policies that allow them:
      i. To setup communities of interest (CoI) in peer-to-peer, broadcast and multicast distribution patterns;
      ii. ;To Define the semantics for the Communities of interest, and
      iii. To Define the information protection characteristic for the CoI;
   b. Policy Management that permits an accredited operators:
      i. To receive complete policy sets or updates to operational policy sets,
      ii. To validate and authenticate the policies for use in the CoI,
      iii. To instantiate the policies or policy updates within the IES environment,
      iv. To activate or deactivate individual policies within the IES environment,
      v. To modify selected policies within the IES environment,
      vi. Store policies locally or remotely, and
      vii. Disseminate policies within the IES operating environment.
   c. Interface with element of the IEF environment.

As illustrated in the in Conceptual Architecture and Policy life cycles there are a number of specifications to follow:

1. MDA Transformation from UML models to executable policies;
2. Transformation of metadata to Architecture Repository semantics (e.g., DM2);
3. Extended Information Protection services;
4. Pre and post mission assessments
    a. Certification and Accreditation,
    b. Threat Risk Assessments,
    c. Statements of Sensitivity,
    d. Scenario Analysis, and
    e. Security Audit;
5. Automated Test Generation; and
6. Governance and Oversight Services.

The C4I and MARS Taskforces will target those specifications directly aligned with their mandates. Other taskforces and/or standards bodies will be sought to address the others. At present, neither C4I nor MARS are seeking to develop community semantics and information requirements; these remain the responsibility of the communities.

REFERENCES AND LINKS

For more information, contact:

Mr. Jean-Claude Lecomte, VP Business Development
Advanced System Management Group Ltd.
265 Carling Avenue, Suite 630
Ottawa, Ontario K1S 2E1
Tel: 613-567-7097
Cell: 613-858-9488
Fax: 613-231-2556
Or visit our WEB SITE: **www.asmg-ltd.com**

OR

Mr. Michael (Mike) Abramson, President
Advanced System Management Group Ltd.
265 Carling Avenue, Suite 630
Ottawa, Ontario K1S 2E1
Tel: 613-567-7097 ext 222
Cell: 613-797-8167
Fax: 613-231-2556
Or visit our WEB SITE: **www.asmg-ltd.com**