Information Exchange Policy Automation

Information Exchange Framework (IEF)

December 5th, 2011

Presented by: Mike Abramson
President, Advanced Systems Management Group
Special Adviser on public safety/security Open Interoperability Standards to Centre for Security Sciences (CSS)
Architect to Chief Force Development Canadian Department of National Defence
Co-chair OMG C4I Domain Task Force
Chair IEF Working Group
Co-chair Emergency, Crisis and Major Event Working Group
Presentation

- Operational Challenges To Delivering Broad-based Information Sharing

- IEF Objectives

- Brief IEF Overview

- Questions
Information Sharing and Protection

- Data Aggregation and Information Protection Services
- Adaptive Release-ability Controls

Organizations:
- Organization 1
- Organization 2
- Organization 3

Shared Semantics / Ontological Commitment
Flexible and Adaptive Policy Enforcement Services
Adaptive Col-Based Data Distribution

Information Protection & Security
- Data Distribution Services
- Communication Infrastructure

Data Filters and Semantic Guards
Release-able Data
Sharable Data

Internal Data
Multiple Sessions/Channels

Prepared by Advanced Systems Management Group Ltd.
Interoperability Challenges

- Enforcing information sharing policies, rules and constraints during dynamic real-world operations
- Adapting to dynamic asymmetric threats
- Adapting to increasing demand for information across multi-agency operations
- Addressing Operational challenges caused by data overload
- Enabling the release of information based on levels of trust and operational context
- Tagging and Labelling of system generated exchanges
- Improving the information quality:
  - **Accuracy**: semantics to accurately convey the perceived situation.
  - **Relevance**: information tailored to specific requirements of the mission, role, task or situation at hand.
  - **Timeliness**: information flow required to support key processes, including decision making.
  - **Usability**: information presented in a common, easily understood format.
  - **Completeness**: information that provides all necessary (or available) information needed to make decisions.
  - **Brevity**: information tailored to the level-of-detail required to make decisions and reduce data overload.
  - **Trustworthiness**: information quality and content can be trusted by stakeholders, decision makers and users.
  - **Protected**: Information is protected from inadvertent or Malicious Release or use.

- Certifying and accrediting Information Sharing Systems and Services
- Managing the underpinning institutional knowledge and memory
Design Challenges

- Translating legislative mandates, policy and Information Sharing Agreements

- Transforming Information Sharing and Protection policies into system/software enforceable rules
  - Standardized Vocabulary
  - Modeling Practices and Profiles (Architecture and MDA)
  - Operational Services to Manage and Enforce the Policies
  - Off the Shelf Tools (COTS)

- Development and maintenance cycles keep pace operational needs:
  - New, changing and asymmetric threats
  - Shifting Operational Coalitions and Contexts
  - Continuous evolution of Legislation, Policy, SOPs, Technology

- Certifying Information Sharing Capability for Operations

- Control Life-cycle costs

- Retain, maintain and exploit Institutional knowledge and memory
Support missing from the TLA AFs

- Linking Information Exchange Requirements to the Data Sources
- Logical Interface Specification that defines the rules governing:
  - The Aggregation, protection & Release of Information
  - The Acceptance, processing and marshalling of data
- MDA for Architecture Driven Interoperability and Model Driven Architecture (MDA)
- Foundation for Information Protection Specifications

TLA AF: Three Letter Acronym Architecture Frameworks
NIEM is a primary Target for IEF Policy Enforcement

But there is much more

Levels of Interoperability
1. Technical Interoperability
2. Syntactic Interoperability
3. Semantic Interoperability
4. Pragmatic
5. Dynamic
6. Conceptual

Types of Information Sharing
1. Event Drive Global Update

Levels of Interoperability
1. Technical Interoperability
2. Syntactic Interoperability
3. Semantic Interoperability
4. Pragmatic
5. Dynamic
6. Conceptual

Communications from Gigabits to Bits per second.
Understanding Information Sharing Requirements

Data in Use

- Often Rigid and Brittle
- Often Difficult to Maintain and Adapt
- Typically Non-Responsive to Operations

Data in Transit

- Community Specifications
- Extract, Transform, Load or Application Code
- Often Pier-to-Pier
- Often Task/Organization Specific
- Often Stove-piped

Data at Rest

- Operational Data
- Organizations often lose Institutional knowledge and Memory of Business Rules
IEF Targeting the Capture and Enforcement of Data Owner Business Rules

Data Owner Business Rules:
- Transactional Patterns
  - Aggregation (Construction) Plans
  - Processing (Marshalling) Plans
  - Domain Filtering Rules
    - Security and Privacy
    - Quality of Service
    - Context Specialization
  - Data and Structure Transformation Rules

Information Protection:
- Semantic Guards
- Tag and Label Filtering
- Tear Lines
- Tag and Label Enforcement
- Domain Processing and Rule

Data Storage Rules:
- Data Owner Semantics
- Data Owner Vocabulary and Taxonomy
- Data Owner Tags and Labels
- Data Owner Business Rules, Structures

Community Specifications

Reusable Transactional Patterns
IEF Objectives

- Alignment of standards to support the development and sustainment of semantic interoperability
- Focus on information content rather than mechanisms for distribution
- Separate business rules from the software applications and services that enforce them, providing:
  - increased flexibility, adaptability and agility
  - Increased the retention of institutional knowledge and Memory
  - Increase traceability and audit-ability of information sharing and protection solutions
- IE Policy Enforcement Support for multiple communities (NIEM, CAP, MIP, …)
- Model Driven Architecture (MDA) services
- Simple approach to modeling messaging, semantic and transactional patterns
IEF Key Concepts

• Reusable Information Patterns Describing the rules for:
  ▫ Information Sharing Contract
  ▫ Message
  ▫ Semantic
  ▫ Data Transactional Patterns
    • Data Aggregation and Marshalling
    • Data Transformation
    • Domain Filters (Static and Dynamic (alterable at Runtime))
  ▫ Semantic Guards (protected Semantic Patterns)

• Simple Extensible Notations

• Transformable into Executable Rules (MDA Process)

• Direct Alignment to Architecture Frameworks

• Open Standards / Open Architecture / Open Source
Where are the Policies

Information System

Metadata and Publishing Policies

LEXS

NIEM

Shared Middleware or Registry/Repository Infrastructure

Information System

Data Aggregation, Information Protection, & Release-ability Policy

Exchange Semantics, Syntax, Structure, Vocabulary & Business Use Case

Enforce Access and Distribution Policies

Receipt Actions & Acknowledgements

Information Sharing, Protection and Release-ability Policies

Metadata and Publishing Policies

Policy Management Services

Prepared by Advanced Systems Management Group Ltd.
Information Exchange Framework

The Clear or white elements on the diagram identify services that the IEPES may interoperate with depending on the Use Cases for the implementation.

The Dark or Blue elements with the white text refer to services within the environment that the IEPES must interoperate.

The 3 packages identify the 3 currently planned EF RFPs.

Prepared by Advanced Systems Management Group Ltd.
IEF Life-cycle Concept

Architecture Models
- Transformation Rules
- Meta-data Transformation
- Policy Transformation

Design Environment
- Scenario Analysis
- Security Audit Application

Governance
- C&A, TRA, SOS

Operator / User
- User Application

Policy Language

Operational Logs

Operational Environment

Security Policies

IEF Components

Networks and Communications

Information Exchange Protocols

Prepared by Advanced Systems Management Group Ltd.
MDA for IEF

Architecture and Engineering Domain

Source of Information Stating Requirements:
1. Legislation;
2. International Agreements;
3. Mission Profile;
4. Memorandum of Understanding;
5. Operating Procedures; and
6. Other

Source of Information Protection Requirements:
1. Legislation;
2. Mission Profile;
3. International Agreements;
4. Memorandum of Understanding; and
5. Policy;

Operational Domain

Information Distribution Services

Community Of Interest

Information Exchanges wrapped in the appropriate Protocols

Contract and Session Policy Enforcement

MDA Tools

IEF UML Profile UML Profile for NITEM

Operational Data

User Application

Glossary

API: Application Program Interface
BPMN: Business Process Modeling Notation
COA: Computer Object Model (Operational Group, Security Domain, etc.)
CMMI: Capability Maturity Model Integration
EDM: End-Node Data Distribution Service
IEF: Information Exchange Framework
IEFL: Information Exchange Policy Enforcement Services
IETL: Information Exchange Policy Language (IEFL Protocol Specific Model)
EPML: Information Policy Management Language
IPM: Information Policy Management Service
MIIA: Model-Driven Architecture
SOA: Service Oriented Architecture
SOAAL: SOA Modeling Language
SOPEP: Shared Operational Policy Exchange Services
XML: eXtensible Markup Language
XML: XML Schema Definition

Additional Messaging Protocol Specifications:
- Common Messaging Protocol (CMP)
- Common Messaging Protocol Definition (CMP-PD)
- Emergency Data Exchange Language (EDEX)
- Protocol Data Units (PDUs)
Take Away

- **Standards are a Community Effort**
  - They are only as good and as useful as the input requirements
  - Requirements come from
    - The User Community
    - SMEs, Vendors and Integrators
    - Academia

- **Standards Enable Interoperability, Integration and Innovation**

- **IEF is an Model Driven Approach**
  - Providing flexibility, agility and sustainability through MDA
  - Providing Institutional Knowledge Retention
  - Enabling Validation and Verification
Questions and Answers

Standards for Architecture Based Information Interoperability
October 2011

Mike Abramson
Special Adviser on public safety/security Open Interoperability Standards to Centre for Security Sciences (CSS)
Co-Chair C4I DTF
Co-Chair Emergency Management SIG
Chair IEF WG
President Advanced Systems Management Group (ASMG) Ltd.
265 Carling Ave, Suite 630, Ottawa, Ontario, K1S2E1
Fax: 613-231-2556
Phone: 613-567-7097 x222
Email: abramson@asmg-ltd.com
The IEF Approach

• Requirements → Architecture → Policy (rules) → Interoperability
  - Translate requirements documented as Legislation, Policy, MOUs, SLAs, etc. into sets of system enforceable rules - That are traceable and auditable throughout their life-cycle.

• Address requirements for strategic, operational and tactical sharing of information based on active & explicit services for:
  - The release of information to authorized recipients; and
  - Protection of information from the unauthorized release based on PRIVACY, CONFIDENTIALITY and SECURITY considerations.

• IEF to issue standards for:
  - A standardized Information Exchange Policy Vocabulary that can be used in multiple modelling and policy languages (on-going)
  - A set of standardized Policy Enforcement Services and Intelligent Agents that plug into common application and middleware frameworks (RFP Dec 2011)
  - A set of standardized Policy Management Services that enable users to manage policies throughout their life-cycles (definition, design, operations and maintenance) (RFP Jun 2012)

• And More at http://www.omg.org/public_schedule/
Process for Policy/Rule Life-cycle

- Derived from operational models
- Metadata Driven
- Separation of operational rules from the enforcement applications
- Update / extension of rules from controlled stores
- Automated transformation of models into executable rules
- Aligned to standards architecture, modelling, development, etc … best practices
IEPES Core Element as per the RFP
UPDM: Aligning AFs and Std Modeling Languages

The Latest:
UML Profile for DODAF & MODAF (UPDM) - NAF also included
Version 2.0 – Adopted June 2011

Seeking Canadian DND integration of DNDAF in version 2.x (option in V2.0 RFP):
- Information Views
- Security and Information Protection Views

Common Approach to Multi-Agency Architectures
Pedigree of the IEF Effort

   - Interoperability by Common Products

   - Interoperability by Common Data Schema & Middleware Specs

3. Multilateral Interoperability Programme

4. ATCCIS Integrated Into MIP

5. OMG C4I to move commercialization of the JC3IEDM

6. Block 4

7. SOPES → IEF
   - Interoperability by Shared Exchange Policies and Semantics

8. OGC C4I DTF RFI Summer/Fall 2001

The Evolution of the Approach / Requirements

Prepared by Advanced Systems Management Group Ltd.
Current Standards Efforts

- **IEF – Information Exchange Policy Vocabulary RFP**
  - Initial Submission February 2011
  - Proposed Language Models (UML, SAML, XACML)

- **IEF – Information Exchange Policy Enforcement Service RFP**

- **National Information Exchange Model (NIEM) Profile for UML**

- **Security Tagging and Labelling RFP**

- **UPDM 2.x**
  - Expected to start with the release of DODAF 2.03 March 2012

- **Interface Definition Language IDL V3.5 RFC**


Evolution of the IE Policy Vocabulary

Diagram name: 0 0 0 IEPV Version 1 Scope
Author: MAbramson
Creation date: 1/12/11 11:15 AM
Modification date: 3/30/11 12:35 PM
Last modified by: MAbramson
Information Exchange Framework

The three packages identify the 3 currently planned EF RFPs.

The dark or blue elements with the white text refer to services within the environment that the ISES must interoperate.

The clear or white elements on the diagram identify services that the ISES may interoperate with depending on the use cases for the implementation.

The User Defined Information Service identifies the types of services the ISES may interface with.

Determine Feasibility

Other Proposed Security Services

- Identity Management
- Access Management
- Encryption Services
- Key Management Services
- Security Registry Services
- Audit Service

Information Dissemination Services

Policy Officer
Expanding the IEF Concept