INFORMATION EXCHANGE FRAMEWORK (IEF) REFERENCE ARCHITECTURE SPECIFICATION

December 2013
Presented by: Mike Abramson
President, Advanced Systems Management Group (ASMG) Ltd.
Co-chair OMG C4I Domain Task Force
Chair Information Exchange Framework (IEF)
• Information Exchange Framework Objectives / Requirements derived from:
  – Previous and Current IEF and SOPES activities
  – Defence Research technology Demonstration: Secure Access Management for Secret Operational Networks

• Proposed IEF Reference Architecture RFP
  – Targeting Policy-Driven Content-Centric Information Sharing and Safeguarding Capability

• Alignment of existing IEF RFPs and Specifications

• Proposed Schedule
Interoperability Targets

• **Information Sharing**: The ability to develop and maintain Shared Situational Awareness, Intelligence, Shared Knowledge and Understanding and collaboration
  - *Asymmetric*: The ability to share content with different communities, agencies or individuals conforming to legislative, regulatory, policy, contractual or service level requirements – while leveraging standard protocols, interfaces and infrastructure.
  - *Adaptive*: The ability to selectively share information content based on operational or business context: roles, relationship, risks, threats, trust.
  - *The right information is available to the right people or system at the right time.*

• **Information Safeguarding**: The ability to apply security and privacy protections to sensitive information and data elements.

**Automation**: The ability develop and certify machine computable rules that enable the deployment of automated Information Sharing and Safeguarding (ISS) Services (policy decision and enforcements points).

**Audit**: (1) The ability to trace the sharing of information implementations to Legislative, regulatory, policy, ... mandates. (2) The ability log and audit information exchange transactions.

• **"ilities"**: The ability to deliver and deploy computable ISS solutions that are adaptability, flexibility, agility, maintainability, supportability, ...

• **Interoperability Level**: Achieve Dynamic Interoperability

Focussed on but not exclusive to Public Safety, National Security, Crisis Management and Military Operations
Information Exchange Framework (IEF) Objectives

• Deliver strategies and specifications that alignment and integrate existing open-standards and enable users to develop solutions to more effectively:
  – **Share Information** (*need to share*): the ability for people, processes, and systems to work together efficiently to ensure that the right information is available to the right people or system at the right time.
  – **Safeguard Information** (*need to know*): the ability to enforce safeguards/protections that assure that information is only accessible by, or released to authorized recipients.
  – **Improve Information Quality** (*semantic interoperability*): the ability of all parties, involved in an information exchange, to properly interpret and utilize the information elements and inform decisions.
  – **Automate Policy**: the ability for users to define or generate rules:
    • that apply ISS policies to a specific domain e.g., operational and Information), and
    • That can be automated using software services (decision and enforcement points).
  – **Adapt operational changes**: the ability to alter rules and adapt to changes in operational context (e.g., threat, risk, role, severity, and scale) in a timely and effective manner.
  – **Control Life-cycle cost**: (1) maximize the availability to off-the-shelf solutions; and (2) systematic practices, processes and tools that minimize development and certification costs.

• Develop specification to address gaps in the current standards portfolio.

Collaboration between C4I DTF & MARS PTF
Information Exchange Framework (IEF) Objectives

• Deliver policy driven, content-centric strategies and standards to enable users to responsibly share information, effectively balancing between the need-to-know and the need-to-share principles.

• Defence-in-depth strategies and solutions that apply information sharing and safeguarding policies at the content (data) level.

• Advance capabilities the areas of:
  – Alignment of policy instruments to specific information domains
  – ISS Policy transformation
  – ISS Policy Automation
  – Responsible Information Sharing
  – Dynamic Interoperability

The IEF Working Group is focused on ISS for Public Safety, National Security, Crisis Management and Military Operations. Many of the concepts strategies and specification will address ISS requirements in other domain.
IEF Guiding Principles

• Target open framework and architecture:
  – open standards;
  – vendor and technology agnostic

• Promote multiple implementations integrations

• IEF overlay: services that can be deployed to an existing environment without dictating the use of new or specific applications, changing data processing routines or disrupting the current user experience or operating procedures.
IEF Requirements

• Specify Policy Vocabularies that enable the translation of policy instruments to machine readable and executable rules

• Specify decision and enforcement points that gate access to or release of information based on active enforcement of security/privacy policy

• Specify supporting services:
  – Packaging and processing
  – Policy Management
  – The logging and auditing
  – Encryption
  – Secure Storage of data/information elements (Secure Container)
  – Secure distribution/dissemination

• Enable information sharing and safeguarding across a wide range of domain specific information domains and user defined policy models
IEF Requirements

• Policy Driven:
  – Common ISS policy vocabularies (Transformation to multiple policy and scripting (e.g., Middleware, ETL and Security) Language Implementations)
  – Architecture based transformation of policy instruments to serialized (machine readable and enforceable) rules
    • Traceable to policy-instruments (e.g., Legislation, Regulation, Government & Agency Policy, Memorandum of understanding and Service Level Agreements)
    • Automated MDA Transforms
  – Decision and Enforcement Points (e.g., A
  – Automated Information packaging – tailored to the recipients credentials, including information Assembly, Transformation, Tagging/labeling/marking, Redaction / filtering and formatting

• Content-centric:
  – Policies enforced at the data and information levels in addition to the traditional enforcement at the Application, Platform and Network Levels
  – Policies enforced during the assemble of information element

• Well-defined interfaces using standards based open, standard protocols
• Run-time policy management and administration
• Transaction level logging and auditing
• Secure storage and transport
Define architecture concepts, elements, interfaces that enable:

- **Information Assurance (IA):**
  - **Confidentiality:** Access Controls, Encryption, Recipient based Redaction;
  - **Integrity:** encryption of information elements (at rest in transit); transaction auditing
  - **Availability:** Responsible sharing; integration with existing information systems
  - **Audit, Accountability and Non-Repudiation:** transaction logging and auditing

- **Integration of discrete IA Services to deliver content-based accesses control:**
  - Identification and Authentication
  - credentials and attributes for recipients (Network, System/Service, Individual, Role, Organization and community)
  - Access control
  - Tagging, Labelling and Marking
  - Information packaging

- **Policy-driven, content-based decision and enforcement points**
IEF Requirements

Minimal Service Areas

- **Access and Release Control**
  - *Content Centric policy enforcement*
    - Packaging (context and recipient sensitive)
    - Release
    - Dissemination
- **Strong Authentication**
- **Cross-agency identity and credentialing/attribution services**
- **Manual and automated Tagging and labeling services**
- **Secure storage and transport Policy**
- **Decision and enforcement points for:**
  - Files
  - Instant Messaging
  - Email
  - Structured Messaging (e.g., NIEM)
  - Web Services
  - Real-time (e.g., DDS)
- **Trusted Reporting, Logging and auditing**

- **Packaging and Process Services**
  - See Information Exchange Policy-based Packaging Services RFP
  - See Information Exchange Packaging Policy Vocabulary (IEPPV) Revised Submission

- **Tagging/Labeling/ Marking**
- **Secure Storage**
- **Encryption**
Service Guidelines

- **Vendor / technology neutral**
  - Elements/components can be implemented using multiple vendors, solutions, products or implementations
  - Ability to leverage existing safeguarding and security solutions
  - Enable the exchange of services that provide equivalent capability

- **Extensible:**
  - Aligns core concepts, capabilities and interfaces
  - Promotes innovation of capabilities around a core interoperable capability
  - Enables the integration of new/enhances information safeguarding services without the need to redesign or redeploy the entire safeguarding overlay

- **Reuse**
  - Integrate/apply existing standards wherever possible
Reference Architecture Requirements

The IEF Reference Architecture seeks to identify concepts, practices, elements for Information Sharing and Safeguarding capability needed to promote responsible information sharing.

- Document abstract architectural elements needed to satisfy IEF:
  - Objectives
  - Requirements
  - Guiding Principles

- Develop
  - Reference Architecture
  - Reference Model
  - Platform Specific Model(s)
  - Use Cases

ISS Overlay that leverages pre-existing information systems and security solutions
Submissions shall include:

- **Reference Architecture**: defines the abstract architectural elements needed to deliver policy-driven information-centric information sharing and safeguarding solutions. Architecture elements defined in a manner that is independent of the technologies, protocols, and products that may be used to implement the domain.

- **Reference Model**: Illustrates the abstract framework for understanding significant relationships amongst architectural elements. It will provide and define the unifying concepts for the IEF specifications. The reference model will not address specific standards, technologies or other concrete implementations, but provide common foundation for aligning and/or unambiguously comparing elements from different implementations.

- **Platform Specific Model(s)**: Providing one or more platform specific models; aligning the reference architecture to a specific sets of standards, tools and technologies used to implement the architecture.

- **Use cases and Concept(s) of Operation**: e.g., for file sharing, text/instant messaging, Web Service(s) and structured messaging.

- **Other Supporting Elements** (e.g., Policy Vocabularies)
• Model comprising the abstract architectural elements in the Reference Architecture

• Policy-Driven Content Centric
  – Access Control Services
  – Information Packaging and Processing Services

• Information Assurance Services
  – Identity Management
  – Credential/Attribute Management

• Trusted Auditing

• Well defined Interfaces (as needed)
  – Dissemination Services
  – Platform/Network Security Services
  – Platform / Network Services
  – Communications
IEF Reference Architecture Requirements

• Define Architecture Elements, Interfaces and unifying concepts to enable:
  – Enable responsible information sharing across multiple enclaves on a single network:
    • Multi-Caveated Single Security Level *(Mandatory)*
  – Enable a common holistic / unified sharing-safeguarding model for multiple information dissemination types:
    • files,
    • email messages,
    • instant Messaging,
    • chat room sessions,
    • web objects, and
    • structure messages (e.g., NIEM Messages)
    • Real-time (e.g., DDS)
  – Enable the integration of existing user information systems and infrastructure
  – Enable multiple platform specific implementations
IEF Reference Architecture  Optional Requirements

• Define Architecture Elements, Interfaces and unifying concepts to enable:
  – Enable responsible information sharing across multiple enclaves on a single network:
    • Multi-Level Security *(Optional)*

• Define Architecture Elements, Interfaces and unifying concepts to enable:
  – Policy development
  – Policy Transformation
  – Policy Testing and Certification
  – Policy Dissemination
Reference Architecture Discussion Points

• Describe the use of policy-driven capabilities promote flexibility, adaptability and agility

• Describe how policy-driven, content-centric ISS enables a defence-in-depth

• Describe how the Reference Architecture will enable the development of solutions to:
  – Responsible Information Sharing
  – ISS Policy Automation
  – Multi-Caveated ISS on a single network
    • Security Caveated (e.g., eyes-only, no-foreign 5-eyes, and NATO)
    • Private
    • Confidential
    • Legally Significant
  – (Optional) Multi-level ISS on a single network
  – Will enhance ISS policy automation
  – Will leverage open standards & which standards
  – Will enable innovation
  – Will promote industry collaboratively in the development of technology & solutions

• Identify and describe gaps in current standards portfolio needed to address all elements in
• Implementation agnostic policy and rules vocabularies

• MDA transforms to serial rules
  – Policy Languages (e.g., XACML, SAML)
  – ETL Scripts
  – Middleware Script and Configuration

• Systematic process for translating policy instruments into machine readable and enforceable rules

• Use of modeling and simulation and analytics to test, validate and certify policy transformations

• Architecture data available for:
  – Modeling and Simulation (M&S)
  – Governance and oversight (business analytics and decision support)
  – Assurance and certification (analytics)
  – Post missions analysis (M&S, analytics, decision support)

• Policy Management and Administration
  – Dissemination to decision and enforcement points
  – Central, distributed or Local administration

• Retention of institutional memory
Requirement: Selective Information Sharing

Using Standards Exchange Semantics (e.g., NIEM) and Adaptive Filtering to Enabling Recipient Selective Sharing of Information

Policy Automation for Semantic Assembly and Adaptive Filtering
Policy-based Packaging Service(s)

- Service or set of services that automate information packaging policy developed using the IEPPV
  - **Contract factory** (formats and releases messages)
  - **Information Factory** (packages data)
  - **Interfaces**
    - Rules Import
    - Management
    - Configuration File
    - Externals Service
    - Application
    - Logging
    - Session(s) to Dissemination Services
  - **IEF Service & Factory Controller**
  - **Policy/Rules Store**

- Information Exchange Specification
  - **Information Specification**
    - **SemanticElement**
    - **TransactionalElement**
      - Assembly
      - Transformation
      - Redaction/Filtering
    - **WrapperElement**
  - **Distribution Specification**
• ISS Overlay that leverages pre-existing information systems and security solutions
• Content-Centric policy enforcement
  - Packaging (context and recipient sensitive)
  - Release
  - Dissemination
• Strong Authentication
• Cross-agency identity and credentialing/attribution services
• Manual and automated Tagging and labeling services
• Secure storage and transport Policy
• Decision and enforcement points for:
  - Files
  - Instant Messaging
  - Email
  - Structured Messaging (e.g., NIEM)
  - Web Services
  - Real-time
• Trusted Reporting, Logging and auditing
Questions and Answers

Information Exchange Framework
September 2013

Mike Abramson,
President Advanced Systems Management Group (ASMG) Ltd.
Co-Chair C4I DTF
Chair IEF WG
265 Carling Ave, Suite 630, Ottawa, Ontario, K1S2E1
Fax: 613-231-2556
Phone: 613-567-7097 x222
Email: abramson@asmg-ltd.com