OMG Standard for Information Exchange Framework

Standards for Responsible Information Sharing

The Information Exchange Framework™ (IEF™) is an Object Management Group® initiative to establish a family of specifications that combine to enable responsible information sharing and safeguarding (ISS) for: email exchange, file sharing, instant messaging (chat), structured messaging, and web services.

The first in this family of IEF specifications has already been published—the Information Exchange Packaging Policy Vocabulary™ (IEPPV™). This specification provides a policy vocabulary and UML® profile model for expression of user policies governing the packaging and processing of structured messages, such as: National Information Exchange Model (NIEM), Emergency Data Exchange Language (EDXL), HL7, or cyber expressions such as Structured Threat Information eXpression (STIX™), Cyber Observable eXpression (CybOX™), and Trusted Automated eXchange of Indicator Information (TAXII™).
The IEF Reference Architecture (IEF-RA) defines a common framework for integrating ISS services to deliver policy-driven data-centric ISS within a user's own technical architecture. The RA will ensure that:

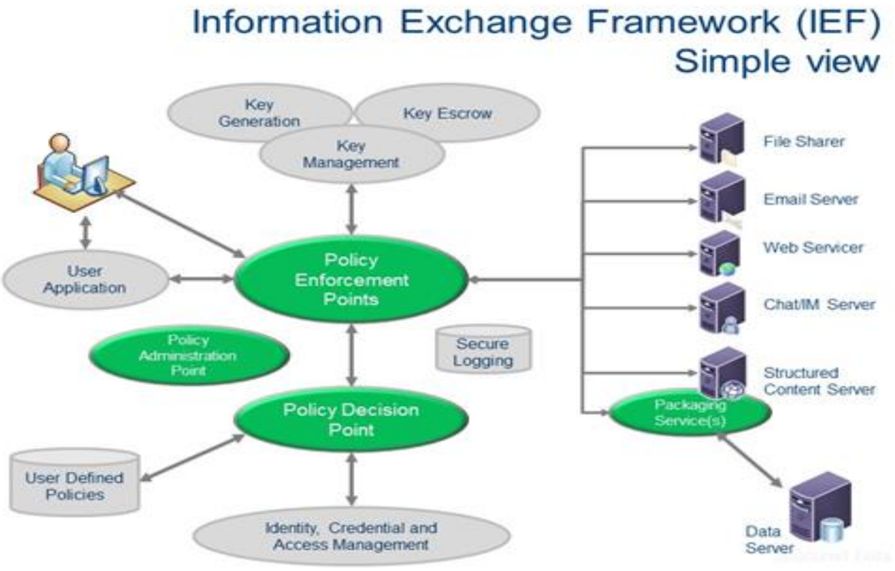
- Access and release controls reflect the sensitivity of each data and information element being shared, not simply the domain in which it resides.
- Every request for information is gated through a policy enforcement point that enforces a user–specified ISS policy.
- Information content is assembled, marked, and packaged in accordance with the data-owner's policies for a recipient/community based on assigned authorizations and privileges.
- Transactions are recorded in a tamper-resistant log to enable real-time monitoring and forensic auditing.
- Users can dynamically adapt ISS policies and controls based on variations in operational context (e.g., threat, risk, policy, location, and roles & responsibilities) and in accordance with security policy.

The third (initial submission November 2018) is the Information Exchange Packaging and Processing Service that ingests a set of IEPPV-defined policies and enforces them at runtime. A high-level set of requirements for the IEPPS can be found in the IEF RA.

G1011118

Value Proposition

• **Platform independence**: The IEF may be implemented using one or more vendor products and services that can be integrated through standardized interfaces, messages and protocols.
• **Defense-in-depth:** The IEF supports layering of information safeguards that automate user-defined ISS policies, e.g., rules and constraints, for each data and information element based on its user designated sensitivity.
• **Policy driven:** The IEF uses standard-based architecture modeling profiles and MDA to translate policy instruments (e.g., legislation, regulation, operating procedures, memoranda of understanding, and service–level agreements) into machine readable rules and constraints enforced by IEF-Packaging and Processing.
• **Data centric:** IEF services combine to enforce ISS policy on the individual or composite data elements based on their sensitivity and the authorizations of the recipient(s) to access that data.
• **Machine-speeds:** Policies for the aggregation, transformation, marking (tagging and labeling) and redaction of data and information elements are executed automatically at machine speeds without the requirement for user interaction.
• **Day-zero Capability**: Libraries of policies (models) can be maintained, translated for operations and deployed to deliver rapid ISS capability, to planned and unforeseen mission requirements.



Prepared by Advanced Systems Management Group Ltd. 1996-2015

The IEF targets mission domains challenged by wide variations in ISS requirements, multiple internal and external partners, significant security concerns and rapid, often unpredictable, changes in operational contexts (e.g., threat, risk, roles & responsibilities, coalition membership, scale, scope and severity). These environments are often physically separated into security enclaves in order to safeguard sensitive (e.g., classified, confidential, private and legally significant) information. This separation isolates information, often making it inaccessible and of little or no value to decision makers.

Next Step

We are happy to discuss how OMG membership will benefit your organization. Please explore our website at **www.omg.org** and when you are ready, contact us at bd-team@omg.org or call +1-781-444-0404.

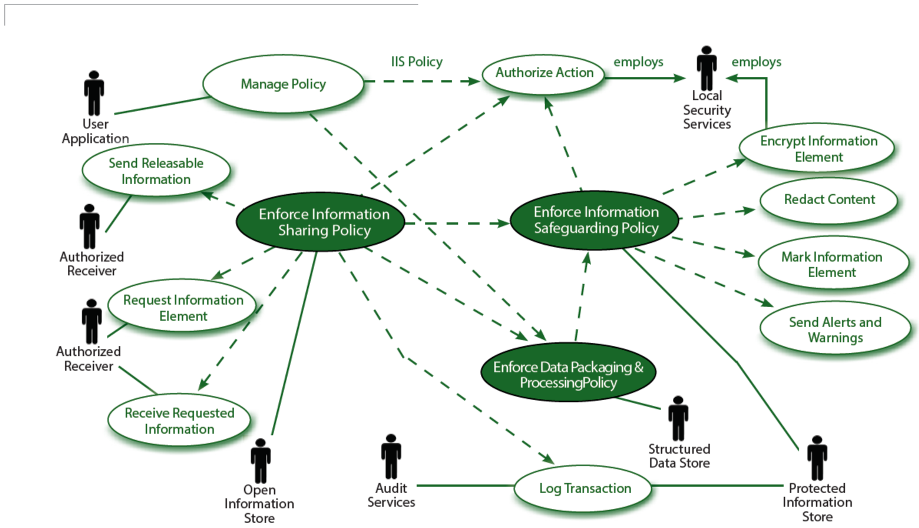
There is a high cost to maintaining separate security enclaves. Many agencies seek to collapse this environment into a single network to enable responsible information sharing:

- to improve decision making, operational planning, coordination and execution.
- to use information as capability resource or force multiplier: do more with fewer resources.
- to enhance flexibility, agility, and adaptability.
- to reduce cost and risk.

The IEF delivers the architecture and services to achieve these objectives.

Although the IEF is focused on real-time operational domains such as national security, public safety, and military operations, the multi-organizational and multi-agency domains such as law enforcement, justice, healthcare, government, financial and business services also have the requirement to responsibly share information. Delivering the new information-based services, coupled with a growing number of international regulations such as GDPR, are increasing risk for organizations that cannot demonstrate their ability to both share and safeguard client and corporate data.

IEF System Use Case



About OMG

The Object Management Group® (OMG®) is an international, open membership, not-for-profit computer industry standards consortium with representation from government, industry and academia. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries. OMG modeling standards enable powerful visual design, execution and maintenance of software and other processes. Visit **www.omg.org** for more information.

G1011118

109 Highland Ave, Needham, MA 02494 USA • Phone: +1 781-444-0404 • Fax: +1 781-444-0320;
Evening Star Building, Regis Group Office #358 • 1101 Pennsylvania Ave., Washington, D.C., 20004 USA • Phone: +1 703-231-6335