Information Exchange Framework (IEF)

return to the OMG Standards

Table 1: Data sheet for Information Exchange Framework (IEF)

Title	Information Exchange Framework
Acronym	IEF
Version	1.0
OMG Document Number	formal/19-12-01
Release Date	October 2019
About Specification	https://www.omg.org/spec/IEF-RA/1.0/About-IEF-RA/
Document	URI

> **Note**: The following is an excerpt from the actual document. It is provided here as a convenience and is not authoritative. Refer to the original document as the authoritative reference.

Scope

The Information Exchange Framework (IEF) is an OMG initiative to develop a family of specifications for policy-driven, data-centric information sharing and safeguarding (ISS) services. These services target the automation of key policy decisions and enforcement points to enable responsible information sharing supporting real-time situational awareness across a broad range of operational scenarios. The IEF Reference Architecture (RA) guides the overall IEF effort, broadens the general understanding of domain requirements, and guides the development of ISS solutions.

The IEF RA is primarily targeting operational environments that require the ability and capacity to share information within and beyond organizational boundaries (public and private sectors) and are challenged by rapid, unpredictable changes in operational contexts (e.g., threat, risk, roles & responsibilities, scale, scope, and severity). These include:

- Military (coalition and Civilian-Military) operations
- National Security
- Public Safety
- Crisis Management
- Border Security
- Emergency Management
- Peace Keeping
- Humanitarian Assistance

Missions and operations in each of these operational domains typically have the requirement to share sensitive (private, confidential and classified) information with other agencies, other levels of government, and private and international partners. This is coupled with the requirement to:

- Address planned and non-planned missions and operations;

- Rapidly deploy and integrate a coalition/partner ISS capability;
- Rapidly adapt ISS patterns to changing operational conditions and contexts:
    - Commander’s intent (target outcomes)
    - Coalition configuration, organizational structure, roles, and responsibilities
    - Threats, risk, and severity
    - Operational stage
    - Plans and orders
    - Communication capacity.

  Although these environments are the primary focus of the IEF specifications, most of the defined features could equally support the transactional domains of a broad range of public and private sector organizations that require:

  1. The ability to exchange information in a secure and trusted manner with clients, partners, and subcontractors;
  2. The ability to selectively share elements of an information holding with individuals and agencies in conformance with legislation regulation, and policy, e.g.:
      1. Healthcare: Electronic Health Records (EHR)
      2. Finance: Banking and Insurance records
      3. Justice: Criminal Case Files
      4. Government Programs
      5. Customs and Immigration.
  3. The ability to log and audit the exchange of information holdings.

     The IEF initiative will, through adoption or development of a series of open standards, define:

      1. A service integration layer that integrates user-specified security components into a Policy-driven Data-centric Information Sharing and Safeguarding capability
      2. Integration layer components include:
          1. Policy Administration Points (PAP)
          2. Policy Enforcement Points (PEP)
          3. Policy Decision Points (PDP)
          4. Policy-based Packaging Services (PPS)
          5. Secure Messaging Bus (SMB)
          6. Security Service Gateway (SSG)
      3. IEF Policy Vocabularies, include:
          1. Decision Request and Response Vocabulary
          2. Packaging Policy Vocabulary (PPV)
          3. Decision Policy Vocabulary (DPV)
      4. Policy Development and Management Environment

         =-