



GFIPM & NIEF Single Sign-on Supporting all Levels of Government

Presenter: John Ruegg, Director

**LA County Information Systems Advisory Body (ISAB) &
Chair, Global Federated ID & Privilege Management (GFIPM) Delivery Team**

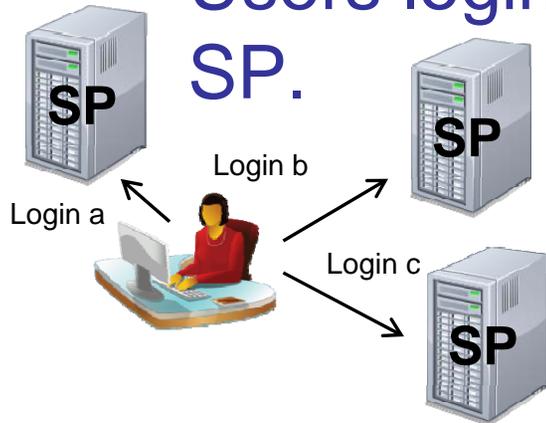
What is Federated Identity Management?

- You depend on another organization to Identify their users [GFIPM Subject role/attributes] and Authenticate them before they can connect to your System. A Trusted Identity Provider (IDP)
- Your System relies on the Identity Information provided from the IDP to make access and authorization decisions. (relying Service Provider) (SP)
- IDP's and SP's have mutual technical and policy obligations to meet for participation in the Federation.

Direct vs. Federated Authentication

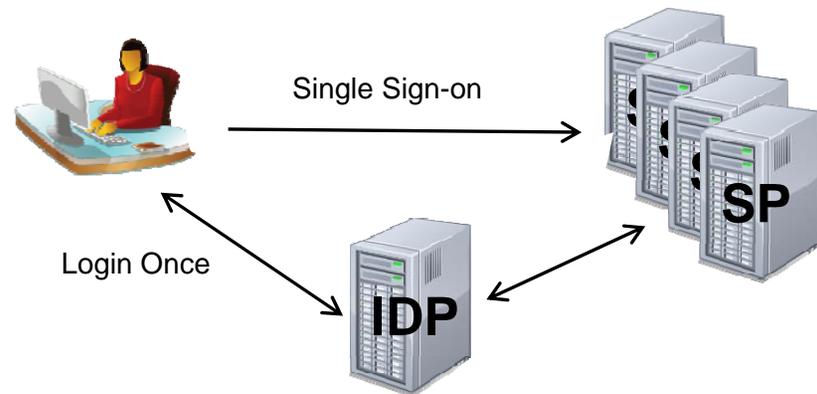
Direct

- Familiar to all Web users.
- SPs manage their own users.
- Users login to each SP.



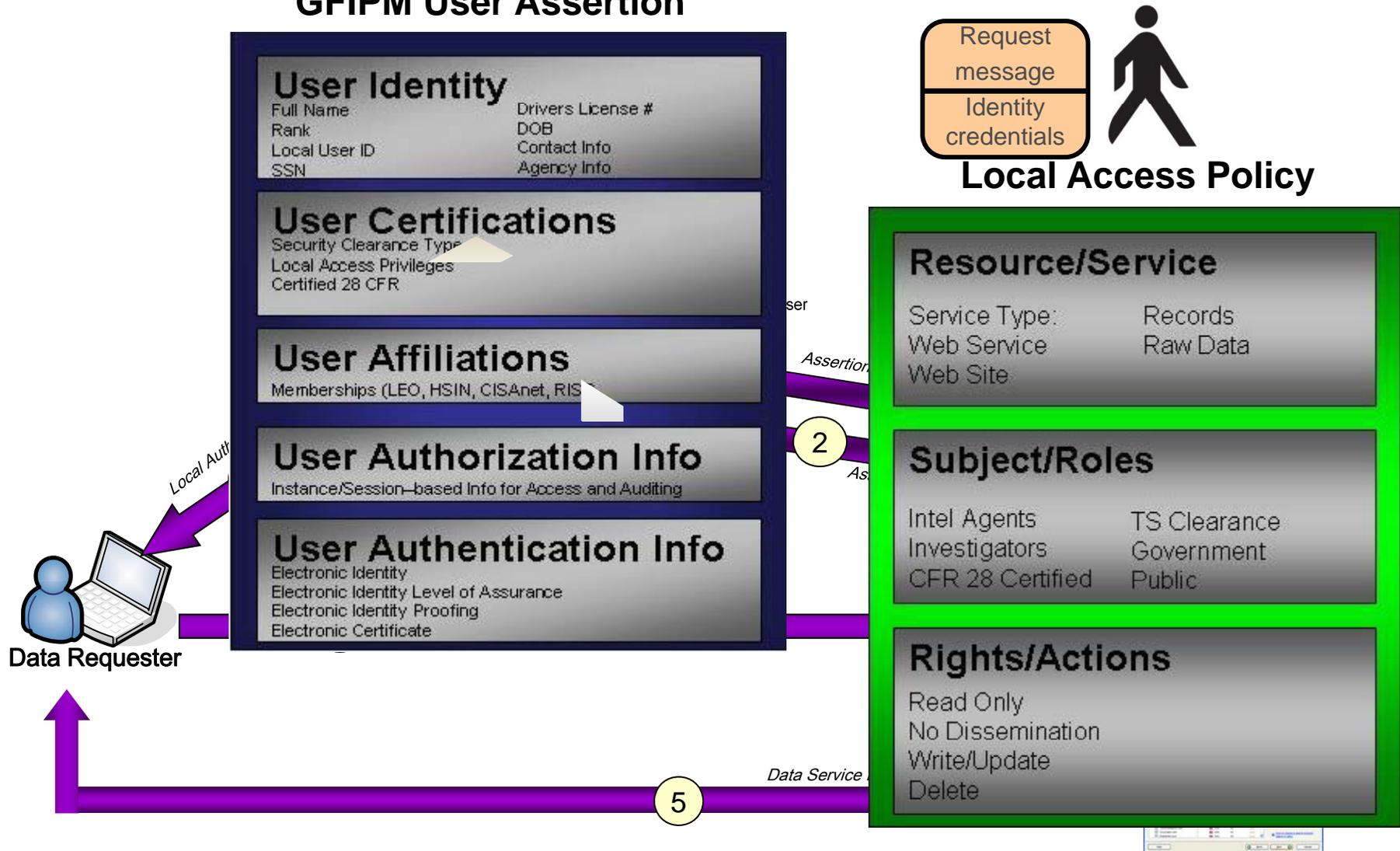
Federated

- IDP manages users
- SP systems do not manage users.
- Single sign-on (SSO).



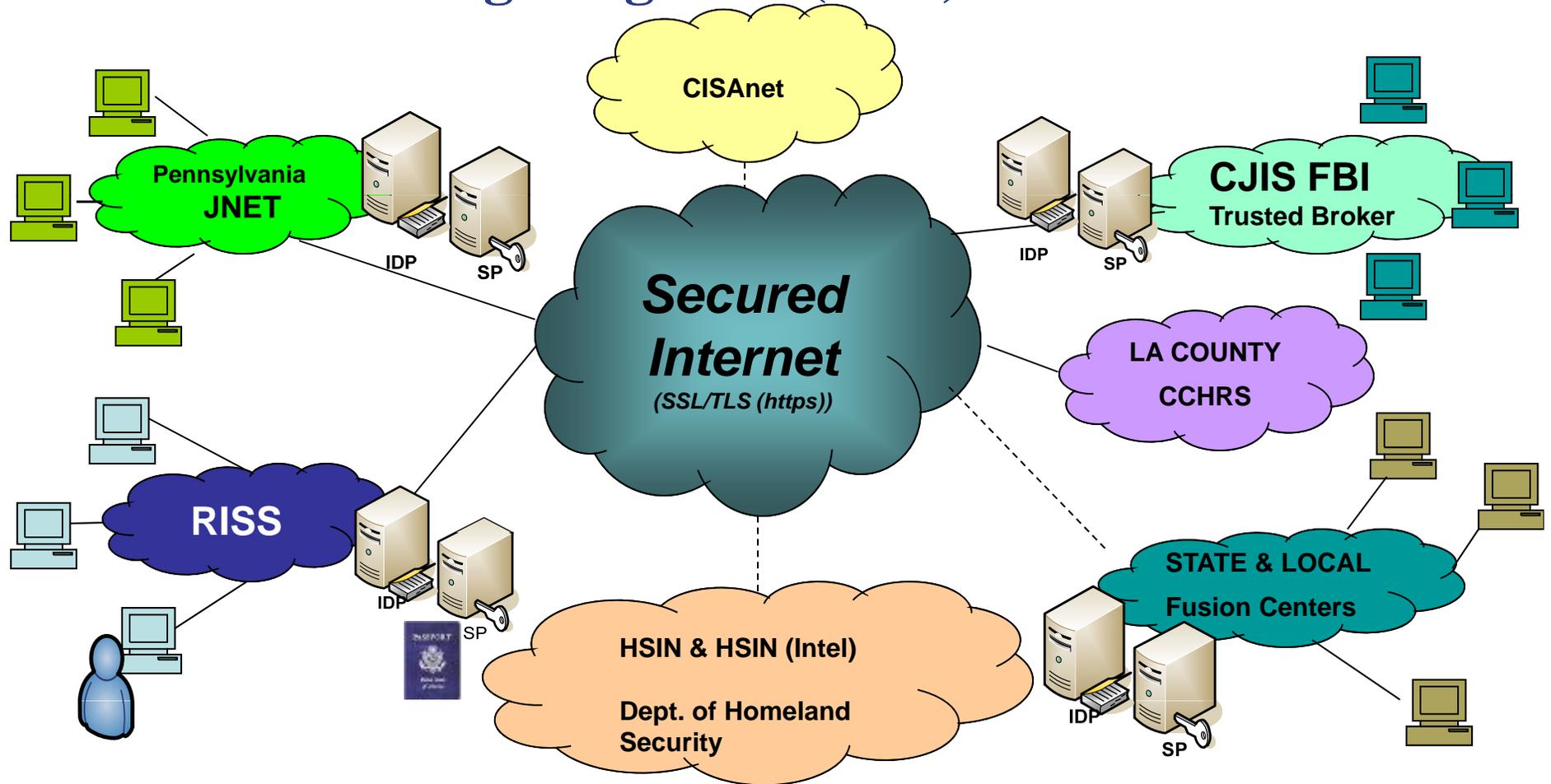
Single Sign-on using Federated Identity Credentials

GFIPM User Assertion



NIEF/GFIPM Federation

Single Sign-On (SSO) Solution

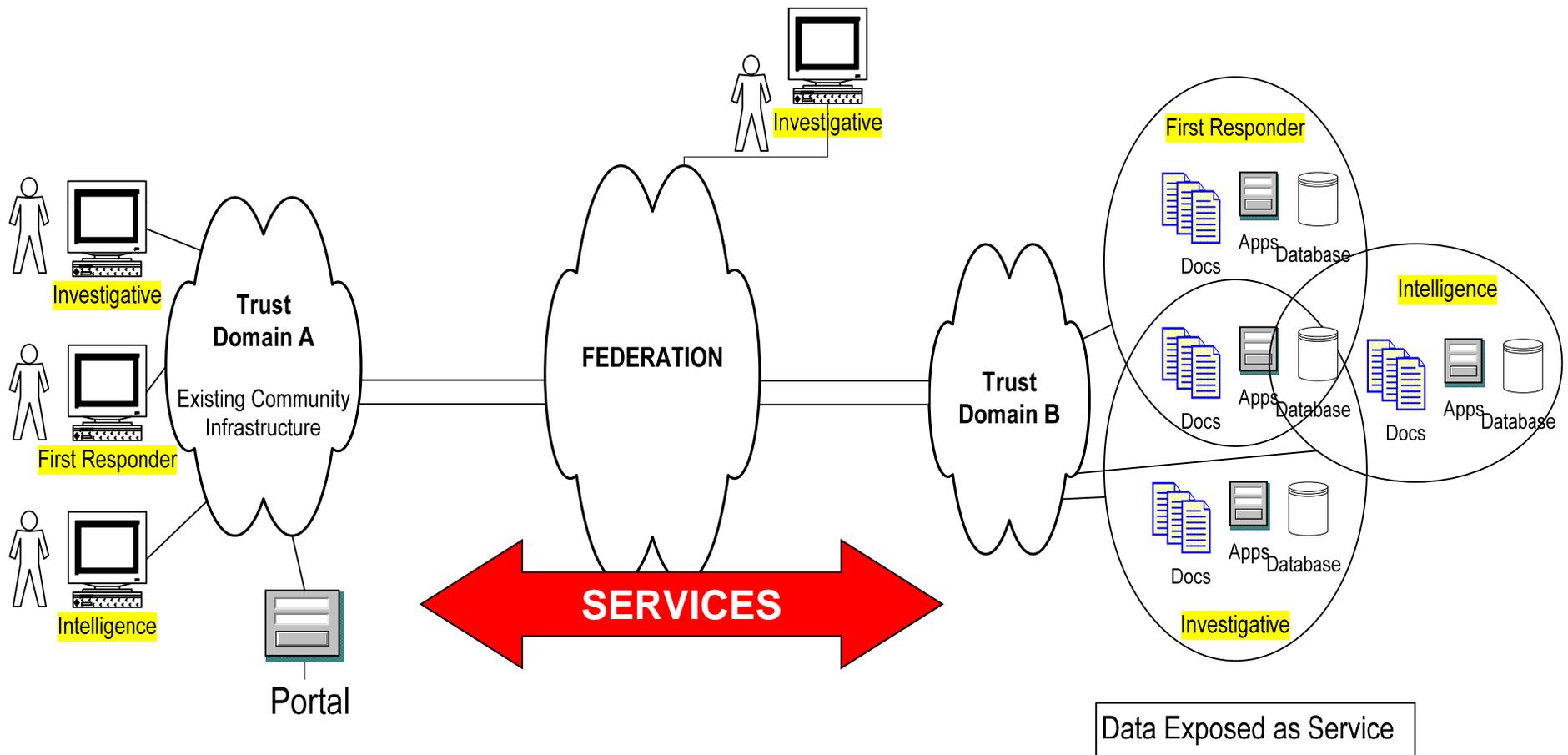


GFIPM Federation Technology Standards

- SSL/TLS Network Transport Protocol (https)
- XML Digital Signature
- XML Encryption
- Security Assertion Markup Language (SAML 2.0)
- SAML 2.0 Web Browser Single Sign-on Profile
- NIEM
- GFIPM Metadata 2.0
- X.509 Certificates (PKI for IDP/SP) and Federation Trust File

System-to-System Use Case

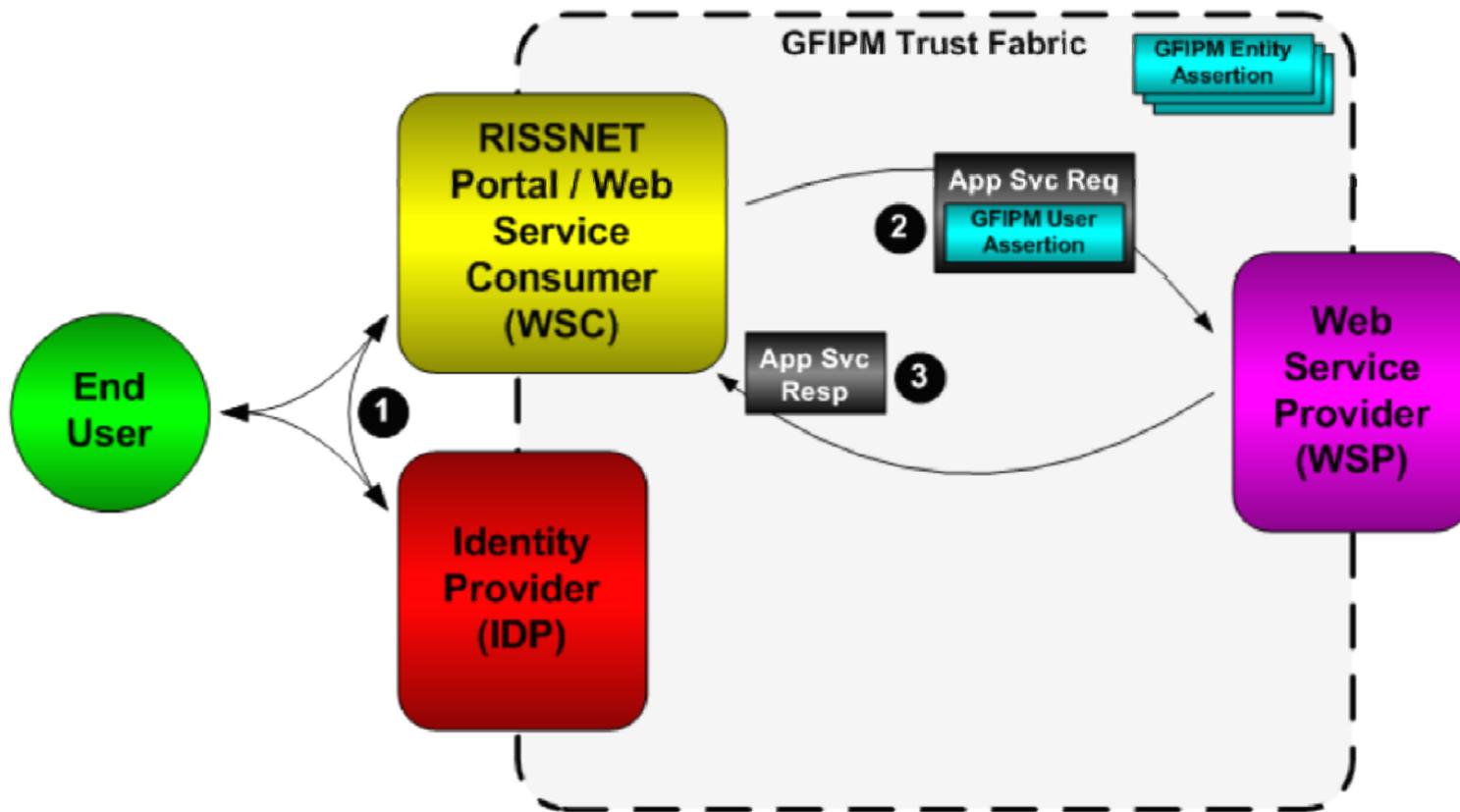
**GFIPM Services are GRA Conformant



System-to-System Use Case

Example 1

RISS Use Case #1: Federated Search From RISSNET Portal to a Single WSP



Implementation Challenges

- Federated ID and Attribute Based Access Control Awareness
- Organizational change – Who is responsible for the IDP
- Where are the attributes and which system/organization is the authoritative source
- Working across Enterprise Boundaries
- Readiness to participate
- Federation Governance Agreements

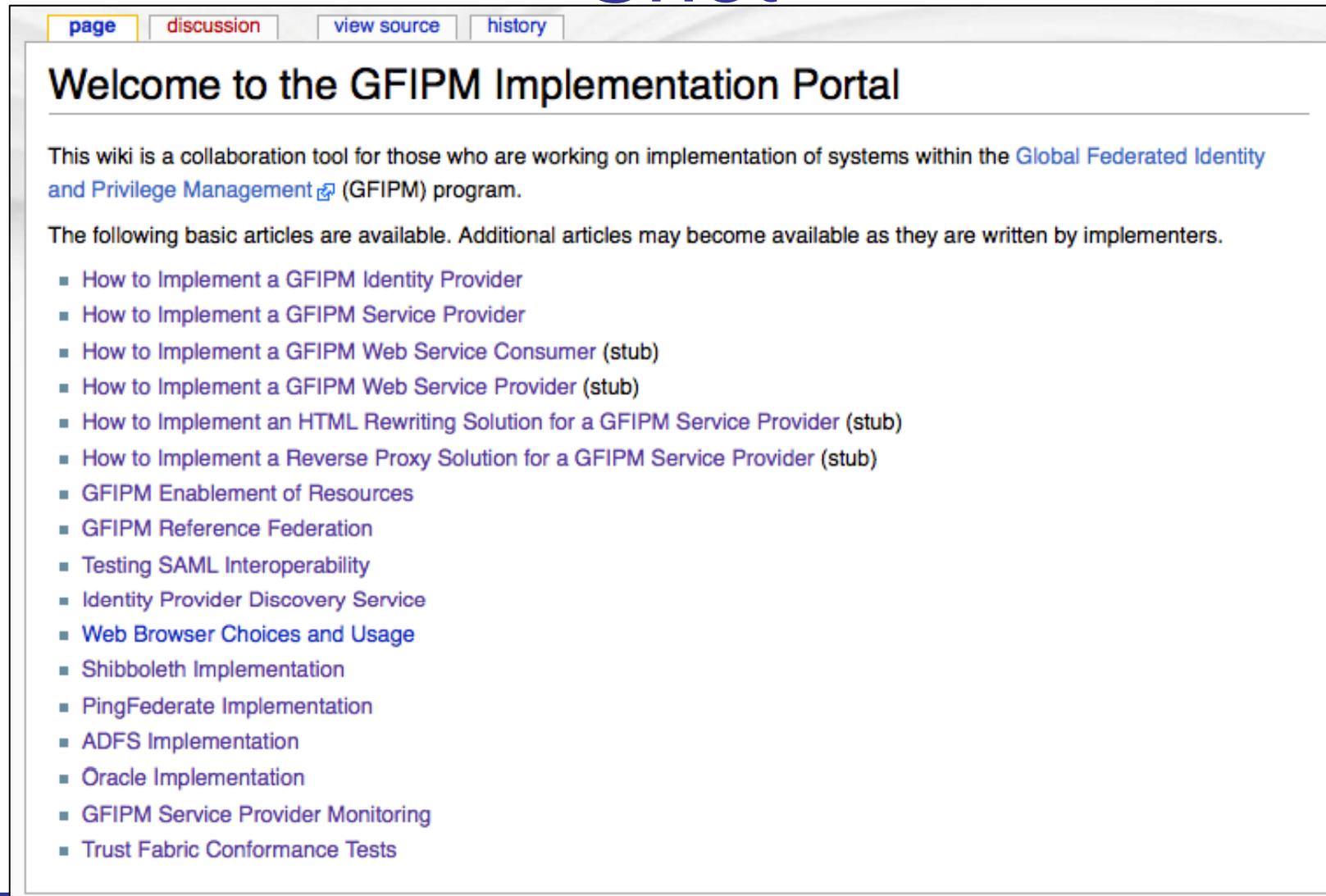
Implementation Challenges

- Incorporation of Security Token Services into the IT infrastructure(IDP's, SP's, Directory Services, Attribute stores)
- Integrating Browser Applications and Web Services to be SAML aware
- Common vocabulary needed for attributes and message payloads (GFIPM metadata, NIEM)
- Testing Platform for interoperability among multi-vendor IDP's/SP's

GFIPM Governance Model

- Representative federation governance
 - Scope of governance is limited to ID and privilege mgmt issues and underlying inter-agency trust
 - Governance of federation services is outside scope
- Formal application and onboarding processes
- Formal interoperability testing process
 - Tests are done in a non-live “reference” federation
- “Federation Manager” agency provides support for the governance process

Implementation Portal Screen Shot



The screenshot shows a web browser window displaying a wiki page. At the top, there are navigation tabs for 'page', 'discussion', 'view source', and 'history'. The main heading is 'Welcome to the GFIPM Implementation Portal'. Below the heading, there is a paragraph of introductory text and a list of article titles.

[page](#) [discussion](#) [view source](#) [history](#)

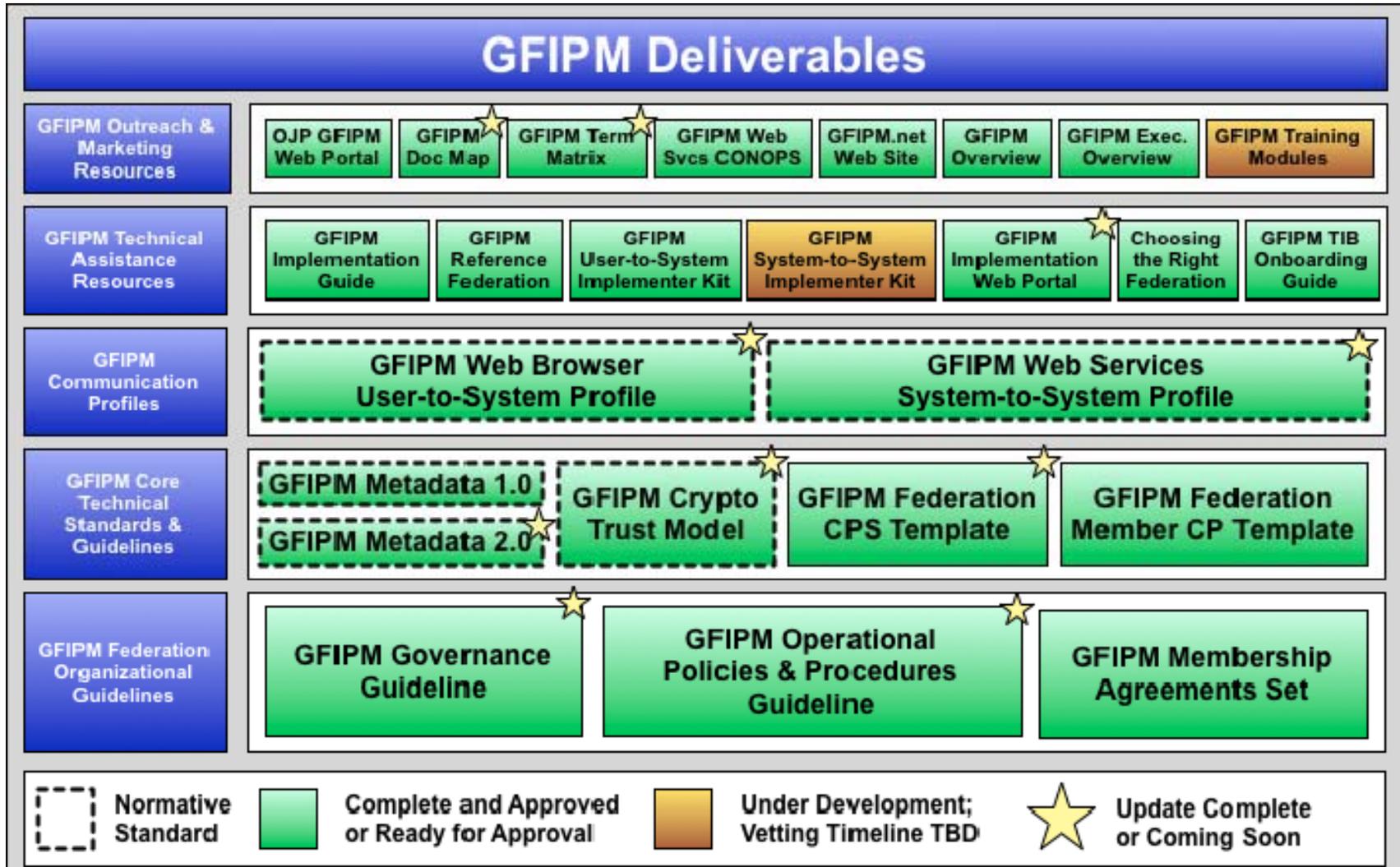
Welcome to the GFIPM Implementation Portal

This wiki is a collaboration tool for those who are working on implementation of systems within the [Global Federated Identity and Privilege Management](#) (GFIPM) program.

The following basic articles are available. Additional articles may become available as they are written by implementers.

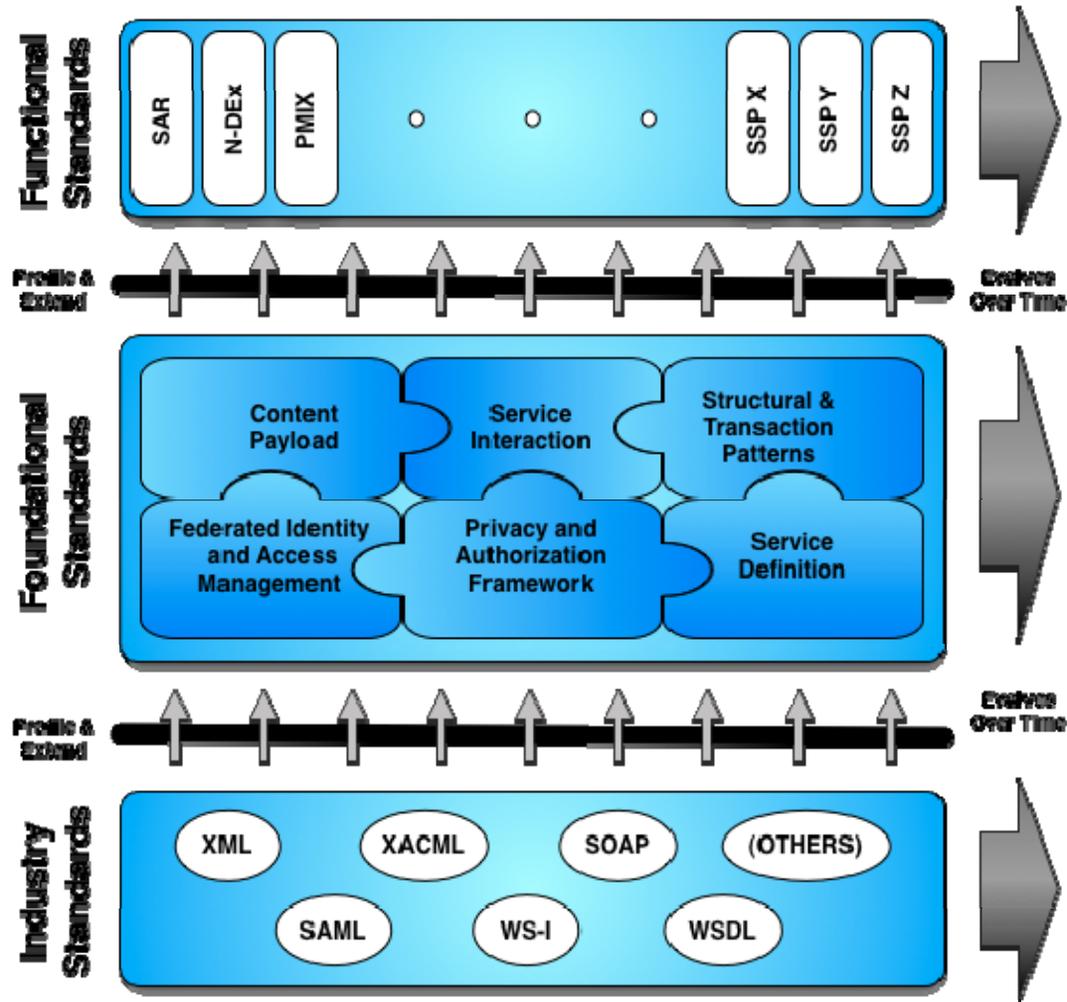
- [How to Implement a GFIPM Identity Provider](#)
- [How to Implement a GFIPM Service Provider](#)
- [How to Implement a GFIPM Web Service Consumer \(stub\)](#)
- [How to Implement a GFIPM Web Service Provider \(stub\)](#)
- [How to Implement an HTML Rewriting Solution for a GFIPM Service Provider \(stub\)](#)
- [How to Implement a Reverse Proxy Solution for a GFIPM Service Provider \(stub\)](#)
- [GFIPM Enablement of Resources](#)
- [GFIPM Reference Federation](#)
- [Testing SAML Interoperability](#)
- [Identity Provider Discovery Service](#)
- [Web Browser Choices and Usage](#)
- [Shibboleth Implementation](#)
- [PingFederate Implementation](#)
- [ADFS Implementation](#)
- [Oracle Implementation](#)
- [GFIPM Service Provider Monitoring](#)
- [Trust Fabric Conformance Tests](#)

GFIPM Work Products

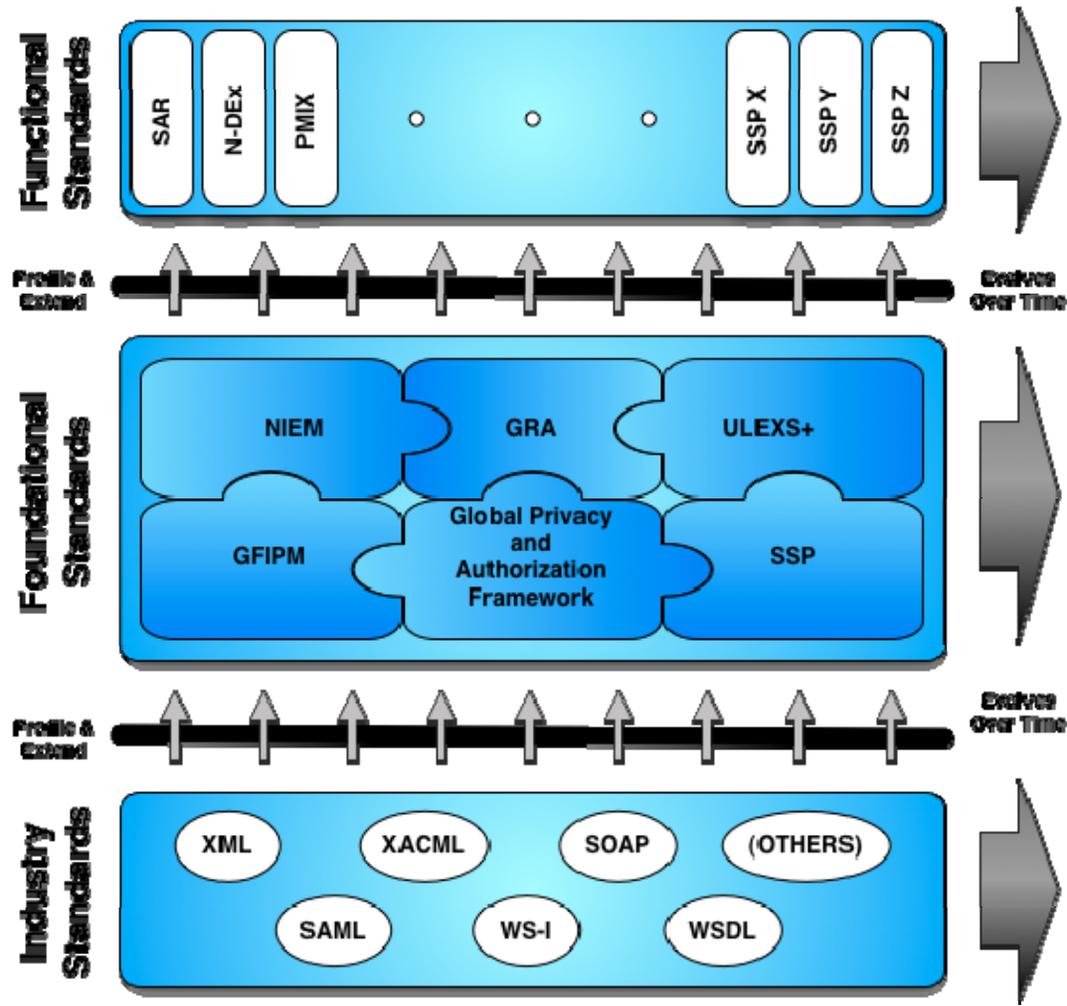


★

Interoperability Standards



Interoperability Standards



Global Privacy Technical Framework

General Privacy Policy Rule

(Permit or Deny, Requestor, Action, Resource, Purpose, Obligations)
IF (one or more Conditions are met))

Example – Request Message

Requestor = Drug Treatment Provider (gfipm attributes)

Request Action = Read

Requested Resource = Medical Record Drug History

Request Business Purpose = Drug Treatment

GFIPM Identity Provider
(IDP)

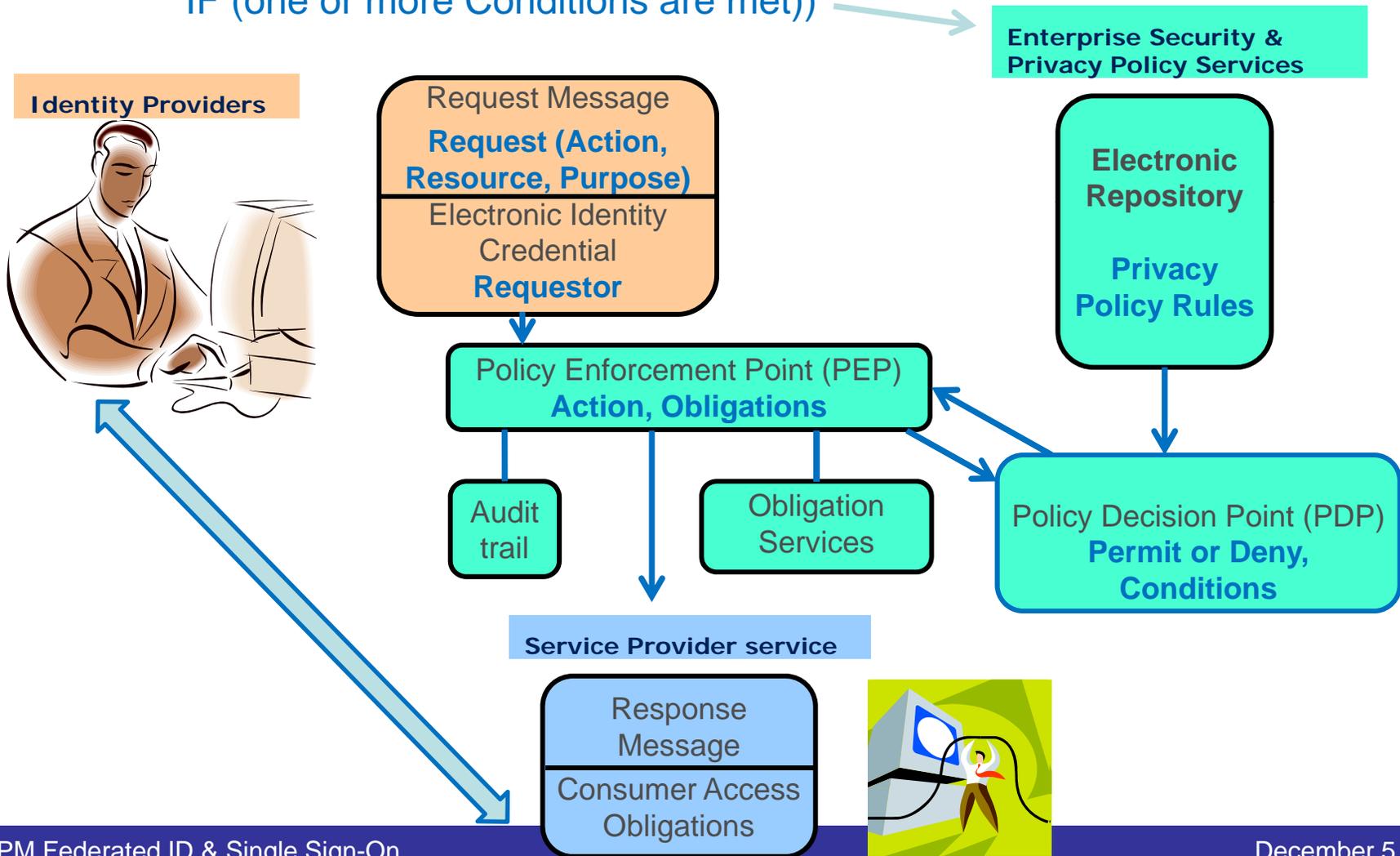


Request Message
**Request (Action,
Resource, Purpose)**
Electronic Identity
Credential
Requestor

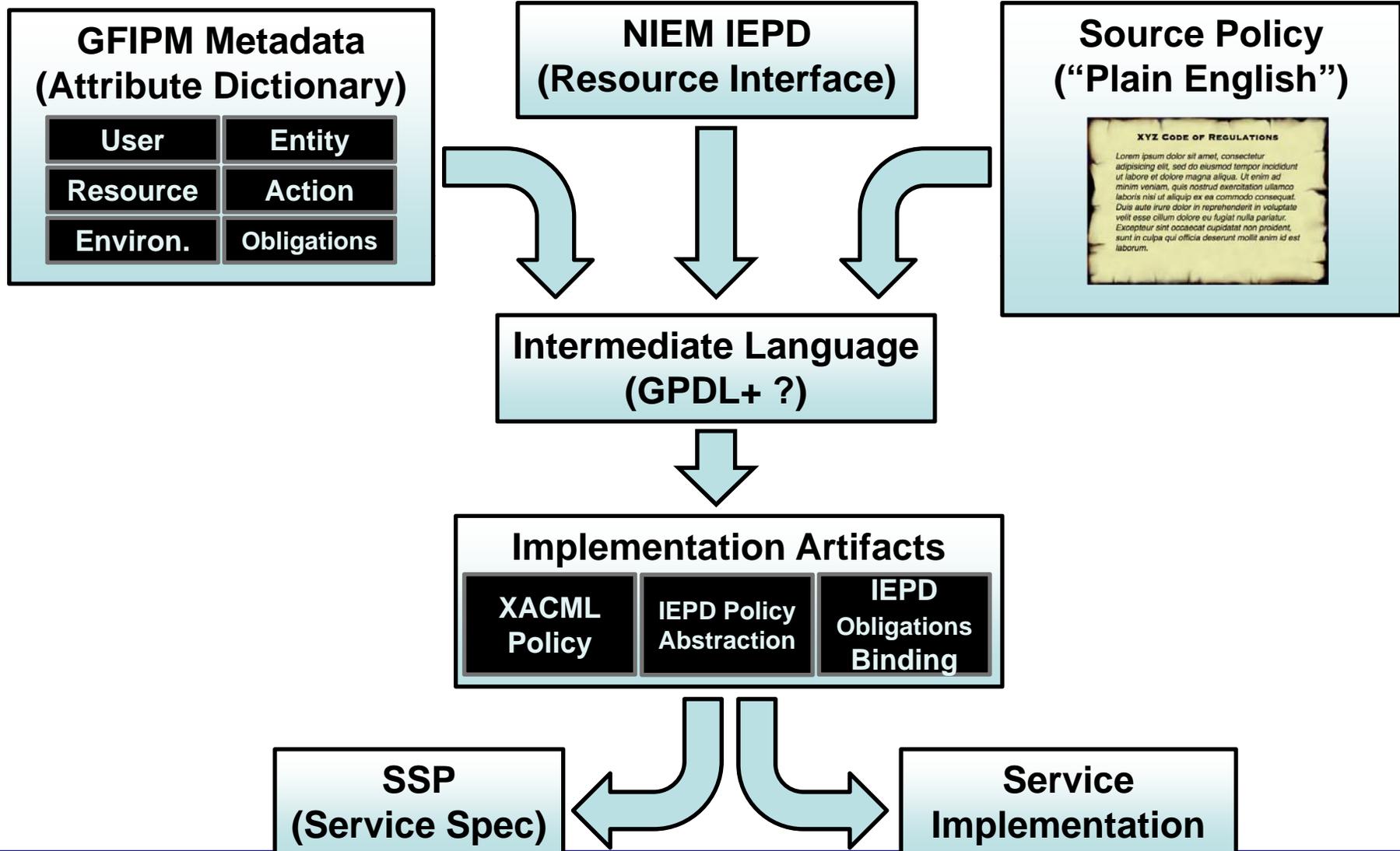
Global Privacy Technical Framework

General Privacy Policy Rule

(Permit or Deny, Requestor, Action, Resource, Purpose, Obligations)
IF (one or more Conditions are met)



Privacy and Authorization Policy Implementation



GFIPM/NIEF Next Steps

- GFIPM planning on synchronizing their SAML 2.0 profile with ICAM
 - The current delta is minimal
- PM-ISE will be working with NIEF to usher them through the TFPAP process (Trust Framework Provider Adoption Process)
- Establishment of a plan for SSO going forward
 - Essential for interoperability between Trusted Broker and NIEF
 - Emphasis on usability
 - Ensure future capabilities (such as federated search and discovery) are supported by the technical approach

DOJ Global Resources

- Global Justice Reference Architecture (GRA) for Service-Oriented Architecture
 - GRA Version 1.4, Web Services Service Interaction Profile (SIP): <http://it.ojp.gov/globaljra>
- Global Federated ID & Privilege Management (GFIPM)
 - Documentation, Guidelines: <http://gfipm.net/>
 - Flyer, demonstration report, and users conference briefing: <http://it.ojp.gov/GFIPM>
- National Information Exchange Federation (NIEF)
 - Operational GFIPM Federation Documentation: <https://nief.gfipm.net/>

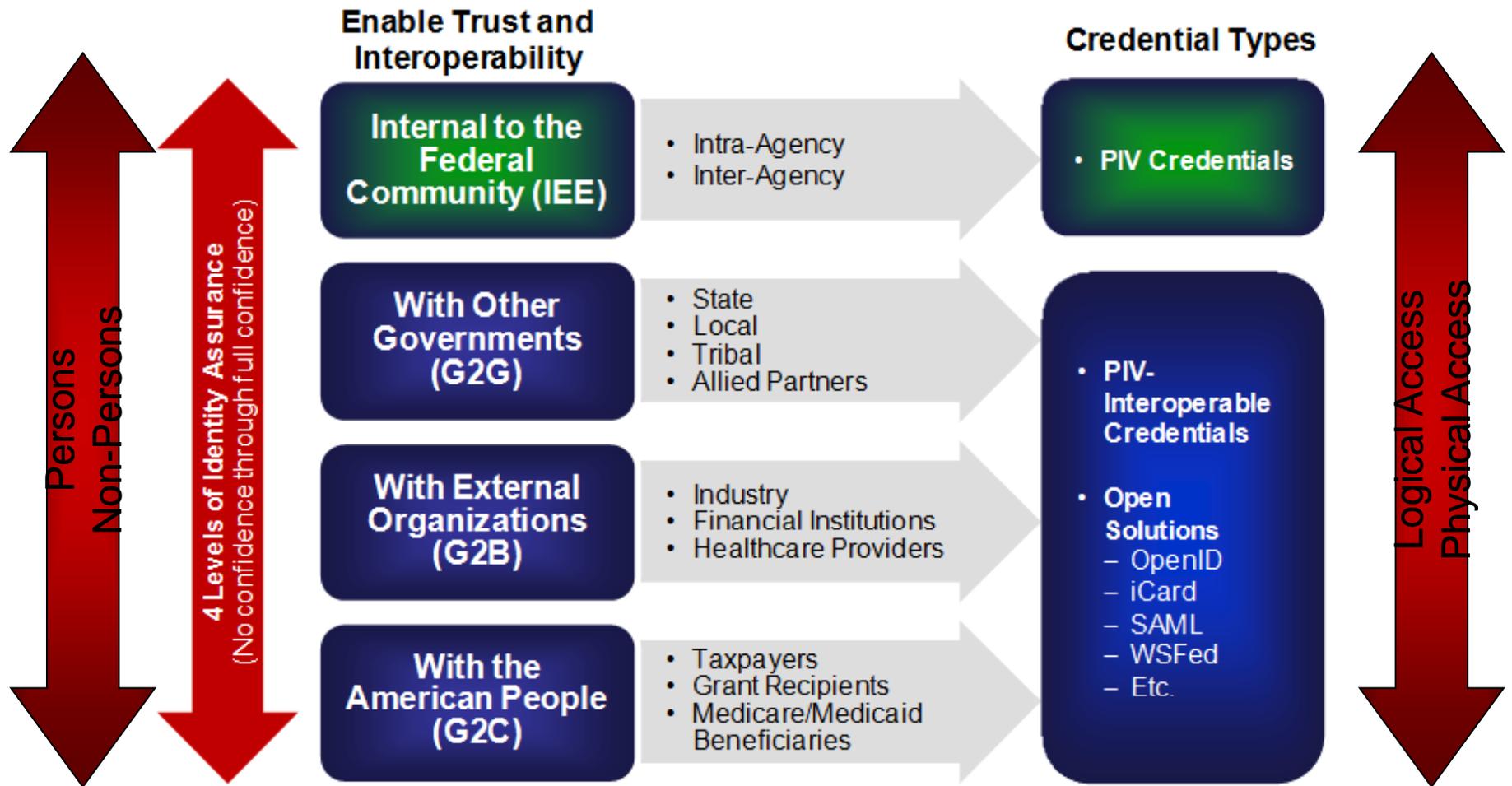
Putting it All Together



Time Permitting

- Relationship of NIEF to FICAM and PIV-I
DHS certificates

FICAM & Federated ID



NIEF/BAE Pilot Use Case

