

# Interoperable, Federated Identity Management Frameworks Across Enterprise Architectures.

We can do this.

**Scott McGrath**

**COO**

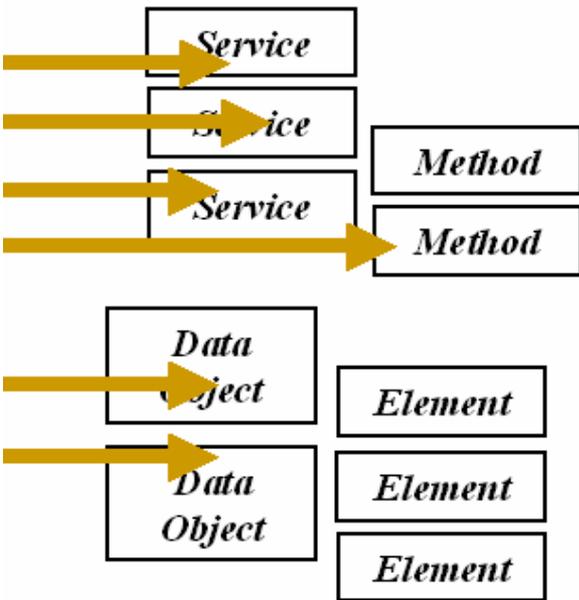
**Organization for the Advancement of  
Structured Information Standards**

**A diverse federated system, constantly adding new nodes, will use multiple data structures and methods.**

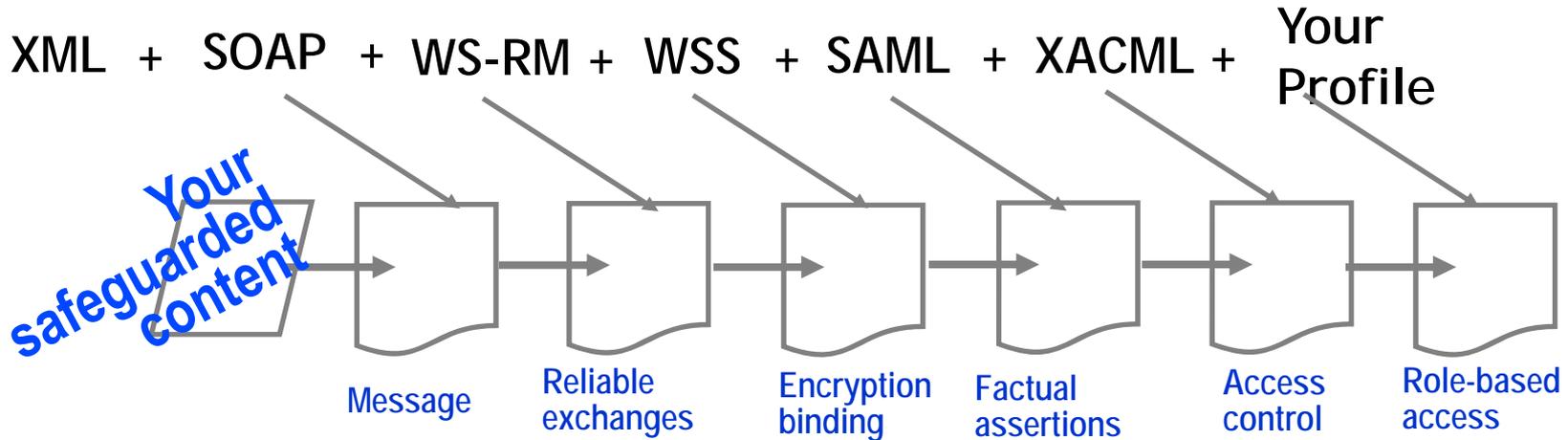
**They all must interoperate.**

**Participating systems need common representations, or shared useable crosswalks, of their capabilities, services & data.**

**Open data standards supply that.**



# The Goal: Composition of standards that fit together, and work like a set of filters



**A set of interoperable standards allows for D.I.Y. invocation of multiple functions**

**Each standard permits use of the others  
... relying on vendor-neutral **availability** and **conformance****

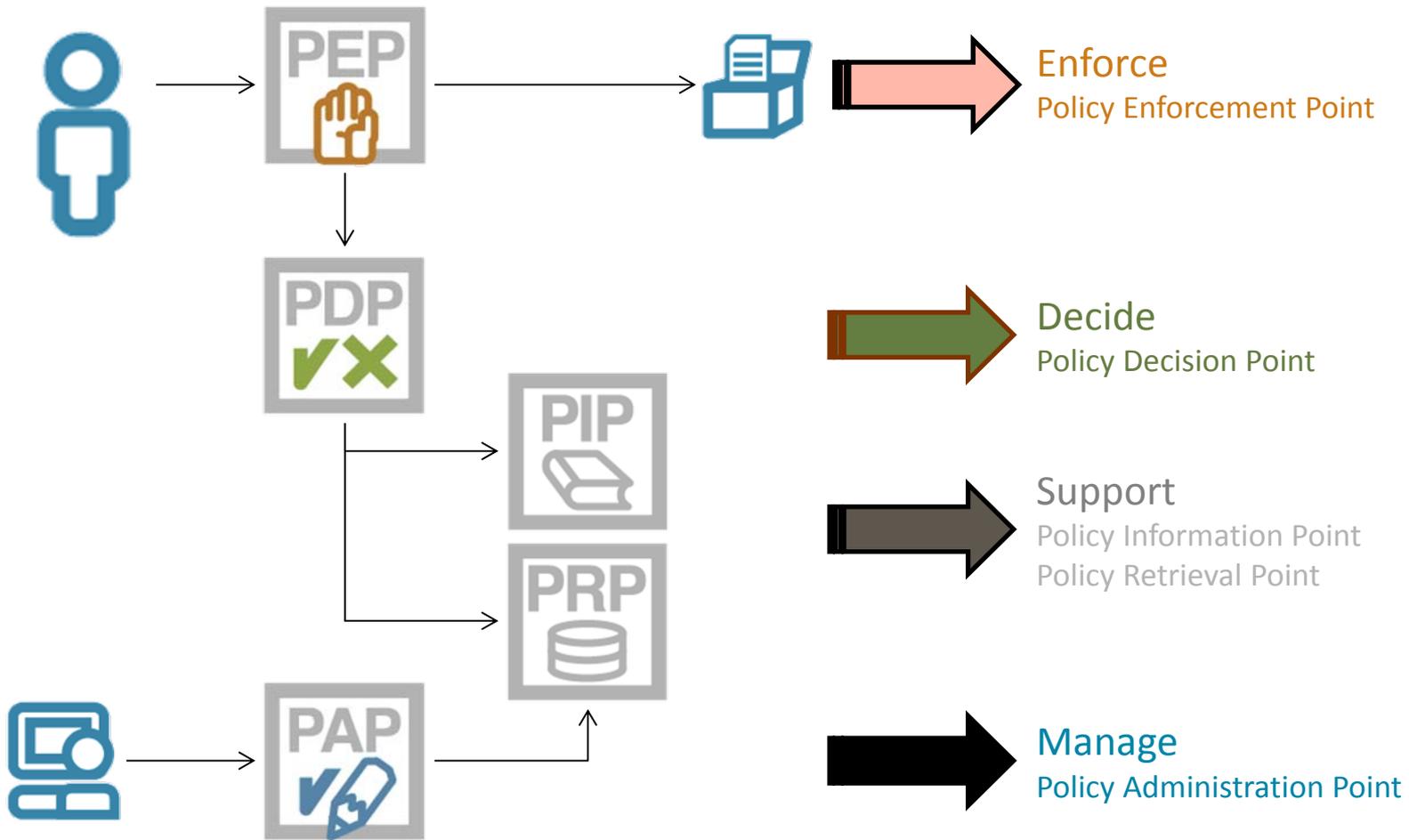
# Security Assertion Mark-up Language (SAML)

- Completely interoperable. Dominant SSO solution in the marketplace
- Used to exchange authentication and authorization data about end user between identity provider and service provider
- Federation partners choose the attributes they need to pass

# eXtensible Access Control Markup Language (XACML)

- Describes both a policy language and an access control decision request/response language
- Manages multiple policies, has structures for identifying applicable policies and reconciling decisions of all the policies invoked

# XACML Architecture



# Interoperability

- XACML policy language is the basis for interoperability
  - Within an agency
  - Across agencies
  - Between gov and commercial
- XACML architecture defines logical integration points for interoperability between vendor solutions

# XACML and Federated Identity

- XACML based authorization supports any type of authentication
  - Loosely coupled architectures create the most flexibility to choose the right authentication based on risk management decision
  - Easily implement the appropriate authentication technique to combat rapidly changing threat and vulnerability landscape

## Centralized or Distributed

- Each application or agency domain chooses how to deploy authorization
  - but retain the ability to interoperate
    - Central or distributed policy management and enforcement
    - Hybrid approaches also supported
    - Achieve consistent and proper enforcement of access control regardless of configuration or operational preferences

# The Last Piece -Your Profile Requires its Own Technical Committee

- FICAM gives a good starting basis
- Additional profiles for XACML and SAML are necessary
- Engage experts in the process—lots of them
- Create the right ecology
- Be ready to take it step-wise

# Cross-Enterprise Security and Privacy Authorization TC (XSPA)

- exchange privacy policies, consent directives, and authorizations within and between healthcare organizations.
- Driven by HITSP/TP20
- Significant TC leadership from VA Health
- Demo video at <http://www.oasis-open.org/committees/xspa/media/xspaoverview/>

# Your Profile Must Be a Real Standard

- Real Standards have real rules that meet government requirements
  - *WTO Technical Barriers to Trade Agreement, Annex 3*
  - *National criteria, like the U.S. OMB A-119*
- Real Standards have hardened, clear rules for IPR licensing
- Real Standards have conformance clauses, test of implementations and transparency

Who is Going To Do The Work?

Who Should Lead?

Who Must Participate?

- OASIS has the largest collection of experts available
- Who owns the vision?
- Who needs to ensure outcomes?
- Who can coordinate needs and incentives?

Let's continue the discussion

Scott.McGrath@oasis-open.org  
[www.oasis-open.org](http://www.oasis-open.org)