LIBERTY ALLIANCE PROJECT

Identity Governance Framework openLiberty Project

January 2008

History

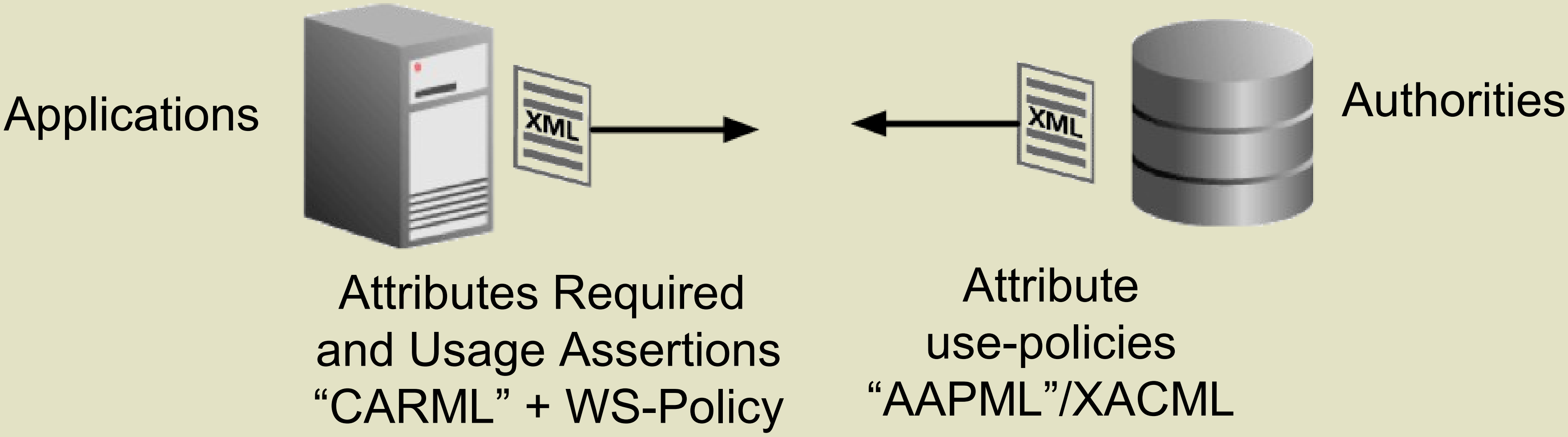
- Initial announcement in November 2006
  - Led by Oracle, support from CA, Layer 7, HP, Novell, Ping Identity, Securent, Sun Microsystems
  - Released key draft specifications for review
    - CARML and AAPML draft specifications
    - Sample CARML API
- Work begins in Liberty Alliance in Feb 2007
  - Creation of MRD - Use-cases, Scenarios, End-to-End Examples
    - Computer Associates, France Telecom/Orange, Fugen, HP, Intel, NEC, New Zealand, NTT, Oracle
    - MRD document released July 2007
  - TEG Work started fall 2007

Current Status

- Two Track Approach
  - Development of open source components at www.openliberty.org
    - Core components based upon Apache 2.0 license
      - Broadly embeddable developer API and tools, IDEs
    - Start with Java and expansion to other languages (future)
    - Aligned with open source ecosystem (Higgins)
      - Re-use existing components wherever possible
    - Simultaneous with creation of Liberty final specification drafts
  - Technical work – specifications and profiles – ongoing at Liberty Alliance TEG
    - Builds on IGF Market Requirements Document and CARML, AAPML draft specifications

IGF Focus

- A set of declarative contracts that document and govern exchange of identity-related data between consumers and providers.



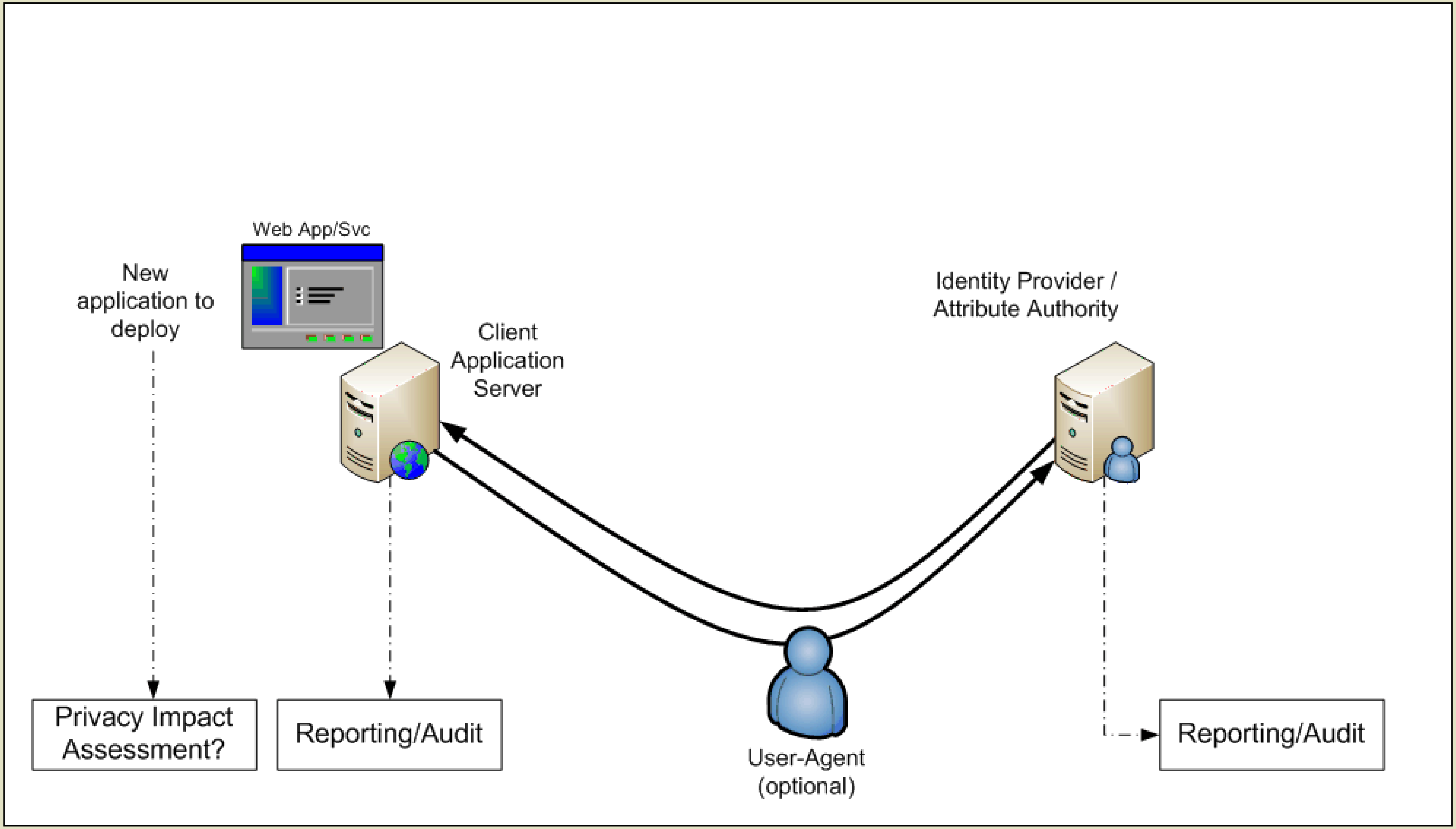
Perspectives

- Application developers =/= identity experts
  - High-level expression of identity requirements
  - Ability to use silo’d and standardized schemas
  - Tools and frameworks for developers are key
    - Otherwise, identity data will be copied and duplicated…
- Deployers
  - Ability to understand schema and transactions in advance
    - Support for Privacy Impact Assessment
  - Ability to map client requirements to identified authorities (sources)
  - Ability to apply deployment declarations and requirements
- Users
  - Capture what agreements the user accepted
  - Reflect consent and purpose of data use
  - But IGF does **not** directly address interactions with users
- Attribute Authorities
  - Increasing drive to publish identity data outside the “silo”
  - User consent must be supported and enforced
  - Enable custodians of identity data to express use constraints

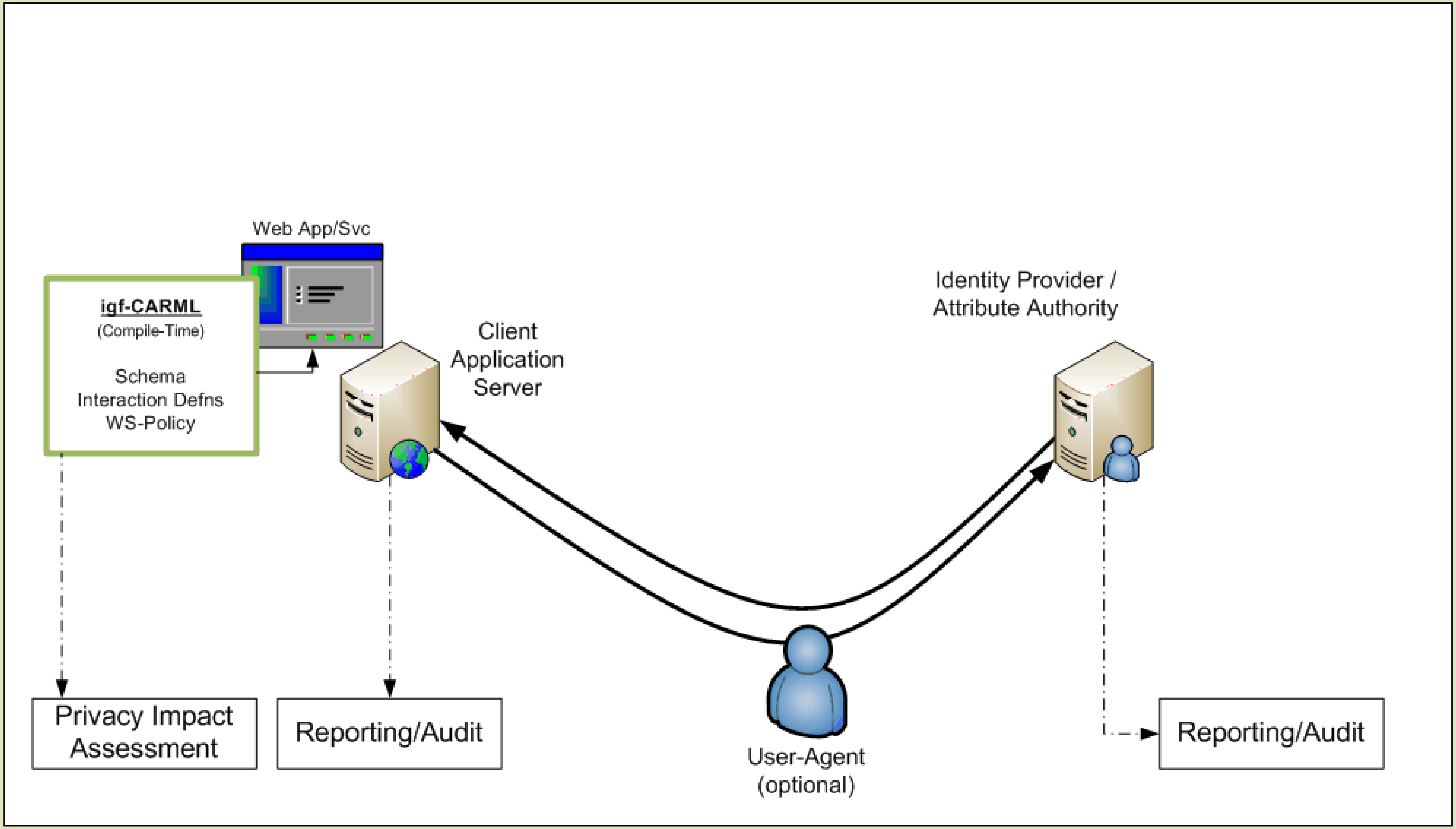
Proposed Standards Components

- **CARML** – Defines application identity requirements
  - what identity information an application needs and how the application will use it.
- **WS-Policy** Support
  - igf-AppIdPolicy - Compile time assertions & declarations
  - igf-DeployIdPolicy - Deployment time assertions & declarations
- **AAPML** – Defines identity use policies (XACML)
  - Constraints on user and application access to personal data
  - obligations and conditions under which data is to be released
- **Attribute Service** – Profiles of existing protocols
  - Support for browser-centric and backend approaches
  - Mapping & translation
  - Policy aware
  - igf-TransactionMetadata - full information context & exceptions

IGF Walk-thru


Web App/Svc
New application to deploy
Client Application Server
Identity Provider / Attribute Authority
Privacy Impact Assessment?
Reporting/Audit
User-Agent (optional)
Reporting/Audit

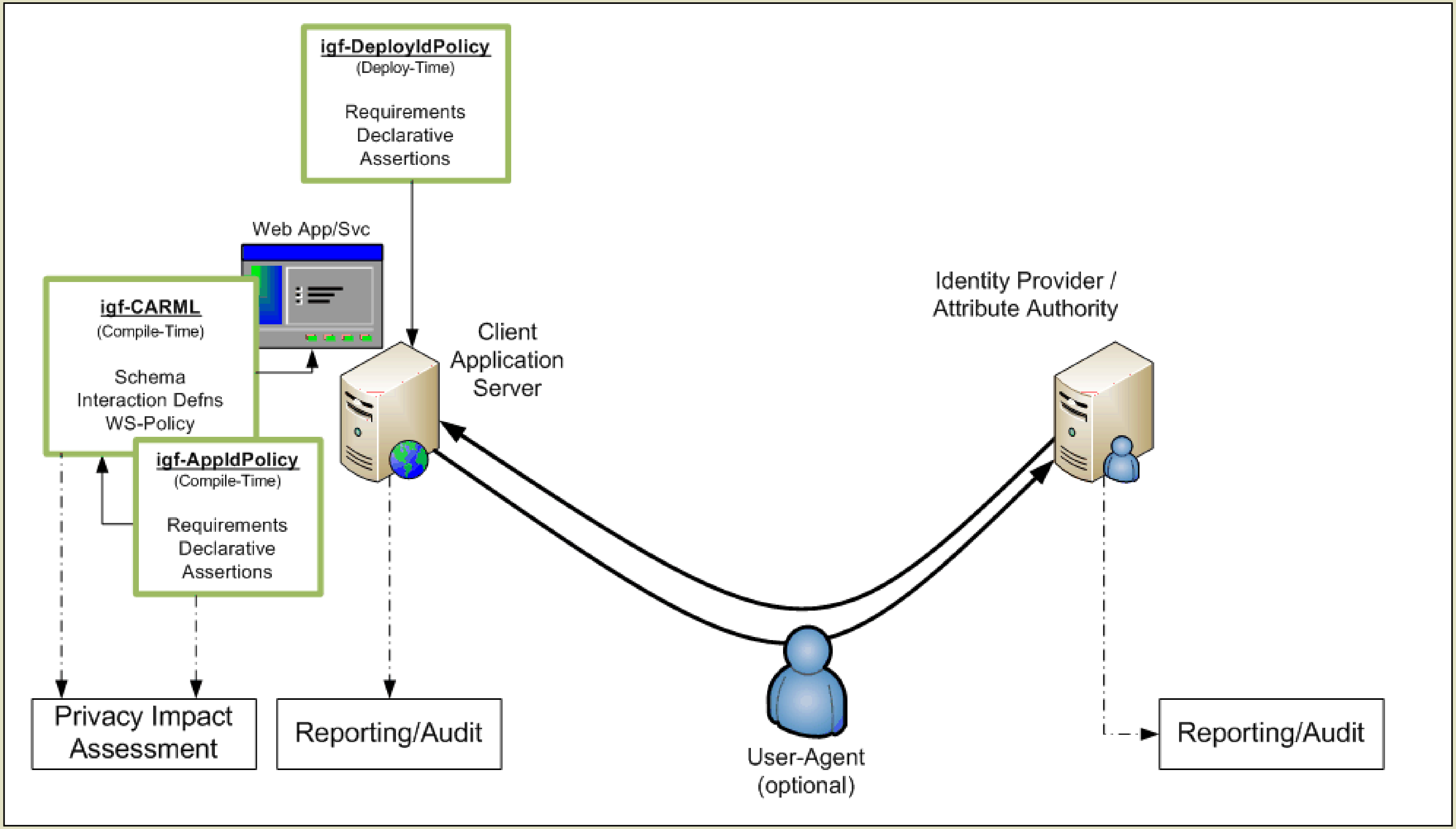
IGF Walk-thru



CARML

- Schema
  - Attributes
  - Predicates
  - Roles
  - Filters
- Interactions
  - Type: Authenticate, Search, Read, Add, Modify, Delete
- WS-Policy * (new)
  - Can be associated with schema and/or interactions
- “Anything that can and should be defined at compile time that minimizes or avoids binding”

IGF Walk-thru



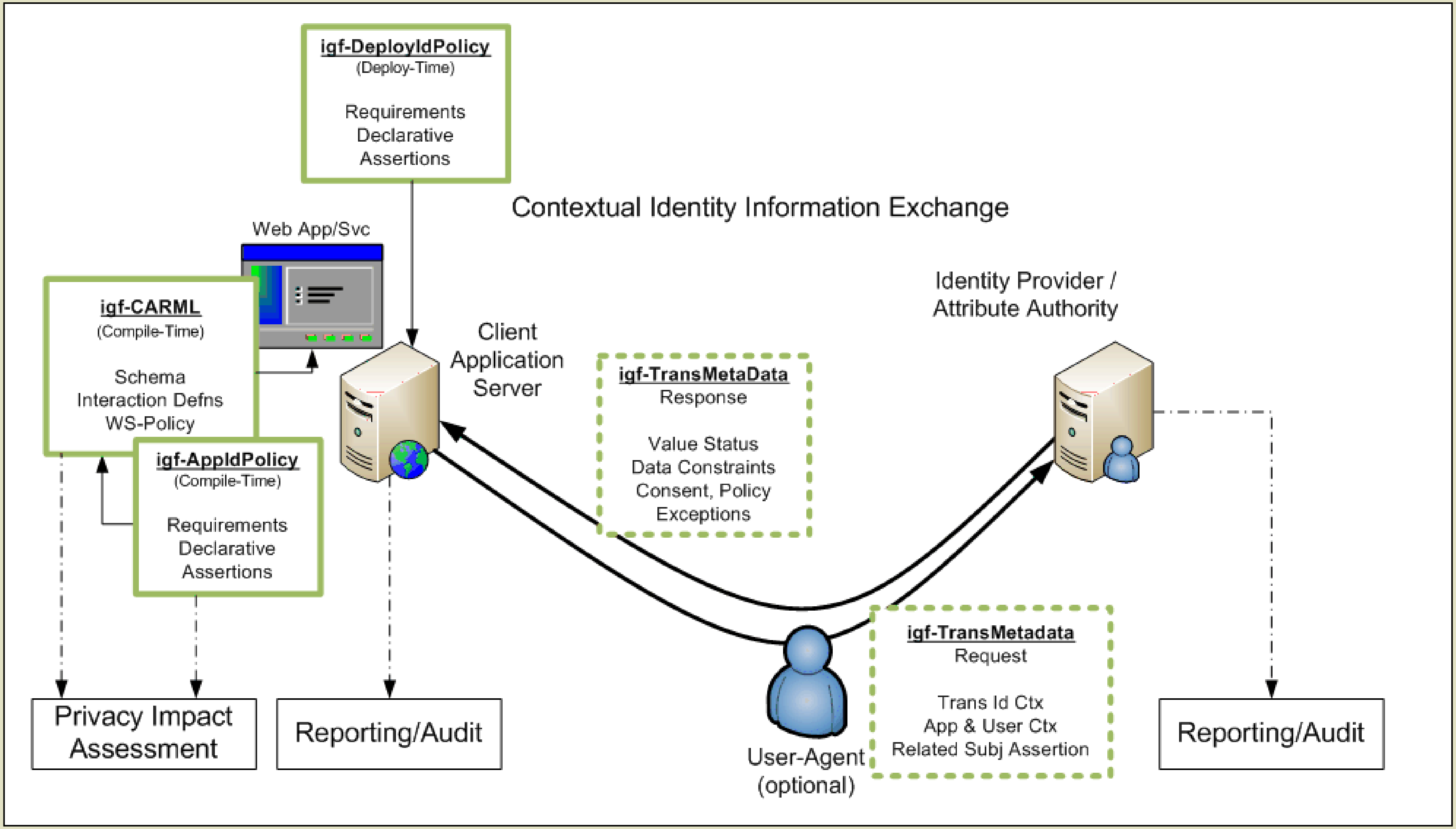
WS-Policy Assertions

- igf-AppIdPolicy
    - *Compile-Time Assertions by Developer*
  - Assertions
    - Purpose
    - Retention
      - Duration & Archive Policy
    - Memory Cache
    - Processing (transient, encrypted, etc)
    - DataDisplayMask
    - ValueMask
    - PropagationServiceDefn

WS-Policy Assertions

- igf-DeployIdPolicy
    - Deployment time assertions
- Assertions
    - DeployedPurpose
    - PropagateEndpoint
    - DataLossOrBreach
    - ContractOrContext
    - AssuranceRequest

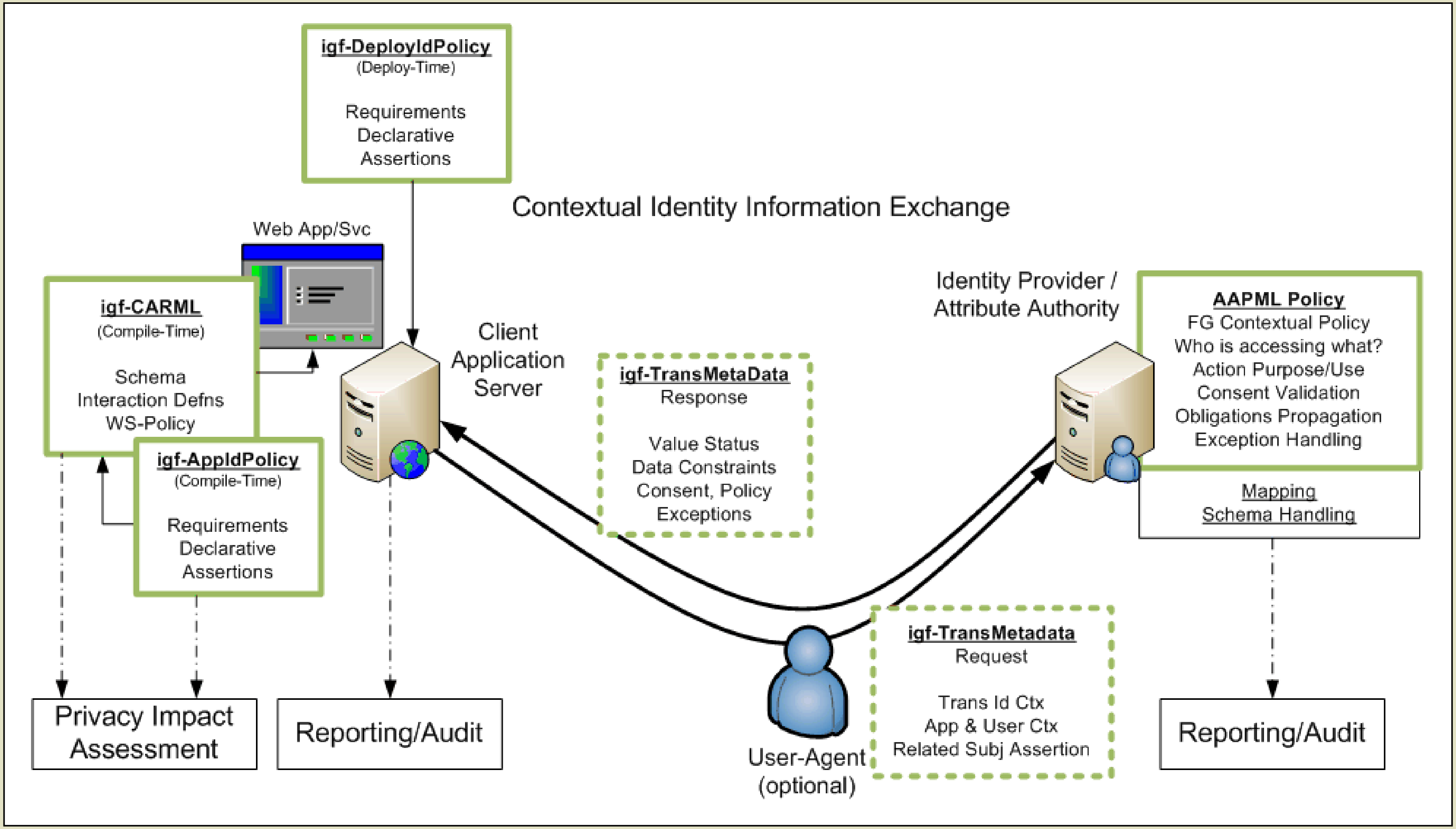
IGF Walk-thru



Transaction Metadata

- WS-Policy like assertions
  - Not protocol specific
  - Request Assertions
    - AppId
    - ActiveUser
    - RelatedSubject
    - InteractionId
  - Response Assertions
    - ValueNotDefined
    - ValueDefaults
    - ValueDerived
    - ValueAssurance
    - DataConstraint
    - UndefinedException
    - ConsentExcetioin
    - PolicyException

IGF Walk-thru

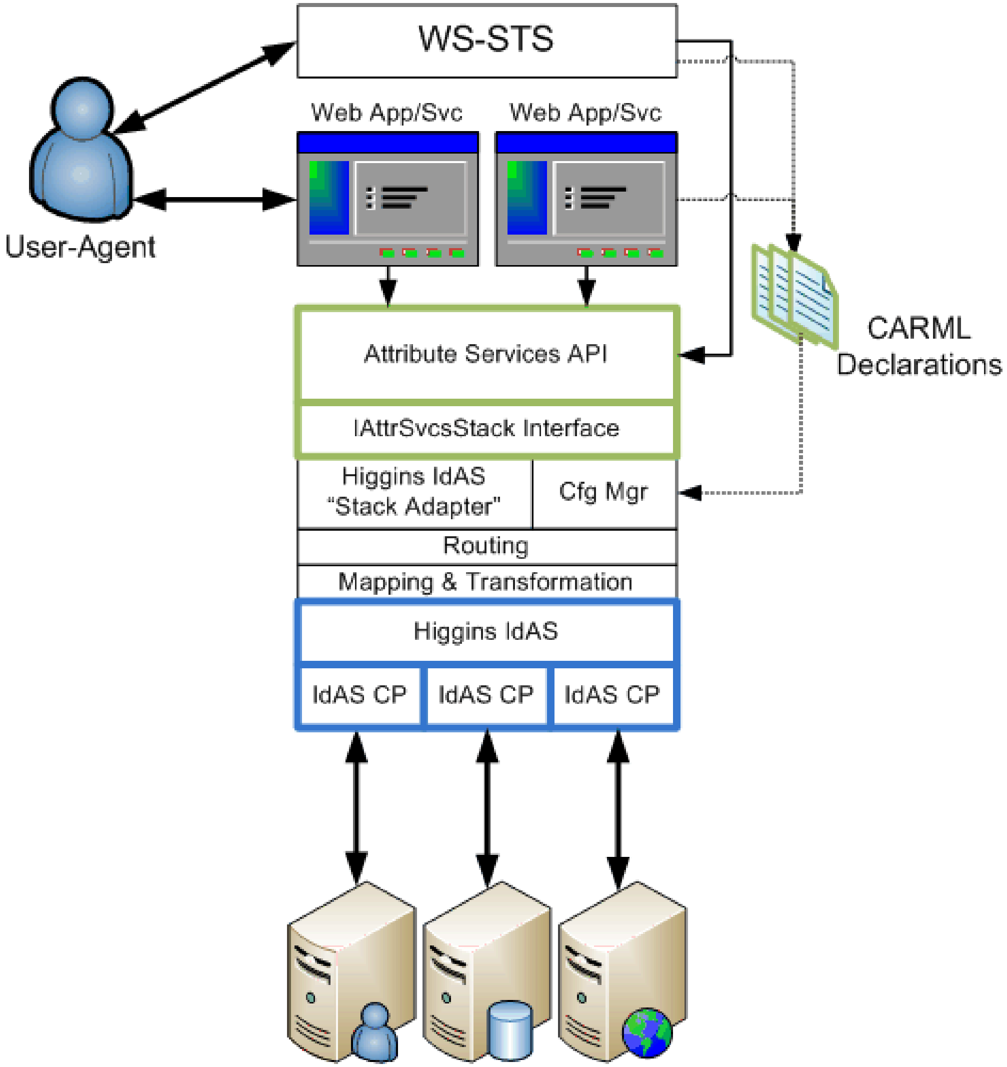


Assurance, Governance and Run-Time Protocols

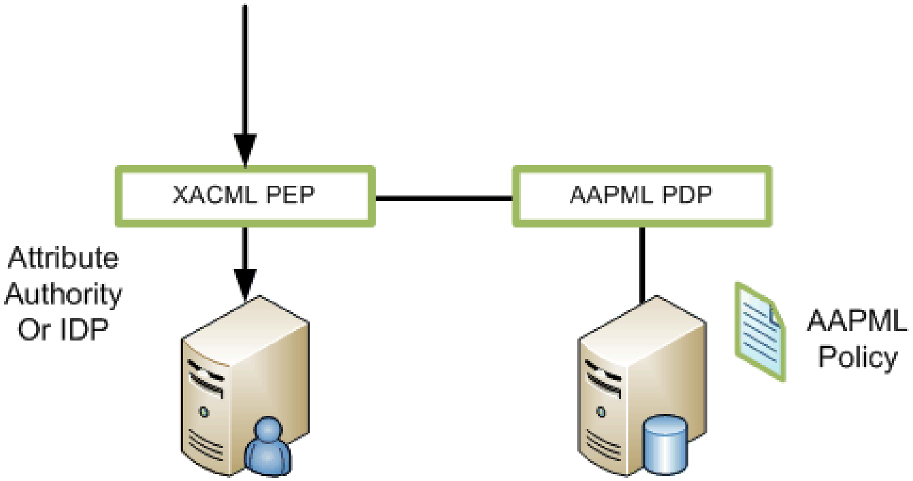
Assurance Liberty IAF, PCI, Privacy Legislation	Requirements that an enterprise or group of enterprises should meet to obtain certification. ↓ *impacts*
Governance IGF XACML WS-Policy Audit Standard?	Policy creation and update, policy enforcement, audit, decision explanation ↓ *impacts*
Run-time Protocols SAML 2.0 ID-WSF WS-*, LDAP	Run-time protocols and wire representations.

LIBERTY ALLIANCE PROJECT

Attribute Service & Higgins



Attribute Service & Higgins



Learn More

- http://www.openliberty.org
- Inquiries to
  - Mail: phil.hunt@oracle.com & prateek.mishra@oracle.com
  - Blog: blogs.oracle.com/identityprivacy