Identity Governance Framework openLiberty Project

Policy Governance Meets Identity

Liberty Alliance Workshop

March 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
- Liberty Alliance work began in February 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

Thesis

Current use of information highly unstructured, unmonitored, and in many cases, poorly governed.

Legislation, liability suits, and press exposure are highlighting the need for proper governance and management of personal information.

With proper governance,
the sharing of personal information can reduce information collection, improve privacy, reduce liability, and improve business accuracy, workflow, and profitability.

LIBERTY ALLIANCE PROJECT

Information Silos

- Silo Definition
  - Personal information typically held/controlled/used for a single application
- Traits
  - Independent Architecture
    - Protocols, databases, schemas
  - Stand on their own - not impacted by external dependencies
  - Obtain, manage, use their own data
  - Fewer dependencies means less complexity
- Examples
  - Enterprise: Payroll, CRM
  - Consumer: Banking, Credit, Retail
  - Government: Taxes, Licenses, Services
  - Social Networking: Facebook, LinkedIn, MySpace

LIBERTY ALLIANCE PROJECT

Silo Challenges

- Verification & Validation
  - Requires more private information for validation
  - Self-asserted information does not often lead to privacy
- Sharing Siloed Information
  - Re-use or re-purposing information
  - Extremes in policy
    - Data kept isolated, or data shared too often
    - E.g. HR as source of truth often used to trigger IT provisioning systems
  - Web 2.0 & Software As A Service
    - DataPortability.org - sharing social information
  - Change in Corporate/Government Business Entities & Structures
    - E.g. Airline Frequent Flier Programs Often Independent Corps
    - Banks offering unified customer experience across many corporations (banking, investments, insurance).
  - Audit - Increased Audit Requirements
    - SOX, GLB, European Data Protection Directive, Can PIPEDA
    - U.K. Gov't - Loss of disks during transfer between agencies via traditional transfer using postal service - audit itself can cause problems!

Observations

- Dynamic access better than bulk transfers.
- Information silos do not assure privacy!
- Sharing information is good for privacy!
  - Identity Oracle
- Verified information has more value than self-asserted.

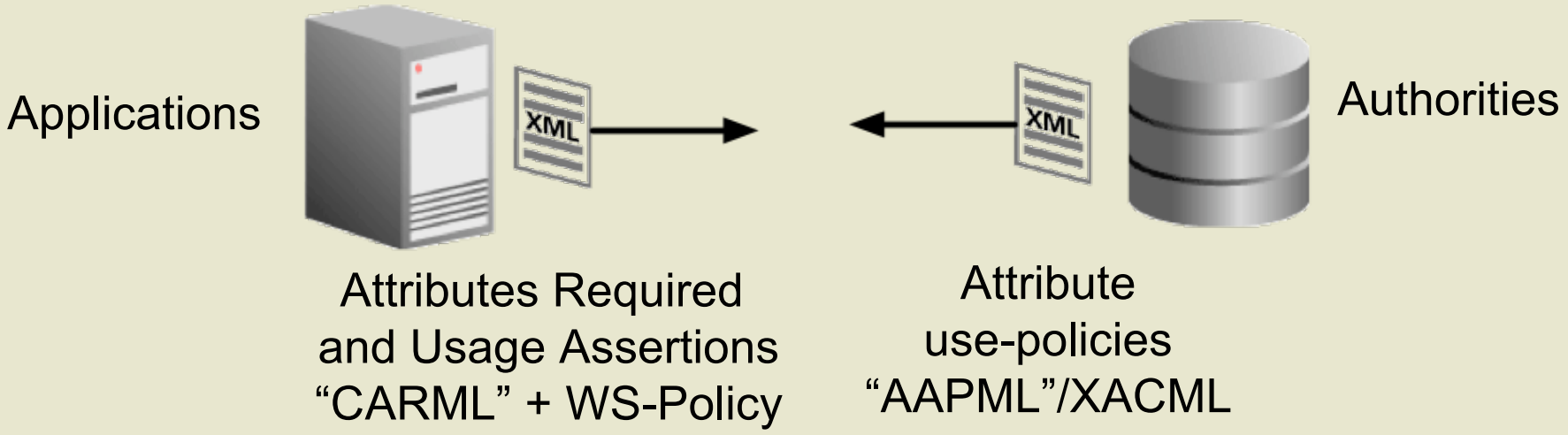
Business Requirements Are Changing!

- *Many old ways of doing business are proving unsafe and unacceptable!*
- Requirements
  - Secure backups
  - Secure publication and distribution
  - Limit scope of information - need to know only
    - By individuals disclosed
    - And the amount of information disclosed by each
  - Privacy Impact Assessments
    - Applications reviewed and approved before deployment
    - Review of information use and distribution
  - Audit
    - Be able to review each use of information
    - Periodic policy review and testing
    - Forensics
  - *Policy to govern shared of personal information*

LIBERTY ALLIANCE PROJECT

Identity Governance

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



LIBERTY ALLIANCE PROJECT

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

LIBERTY ALLIANCE PROJECT

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

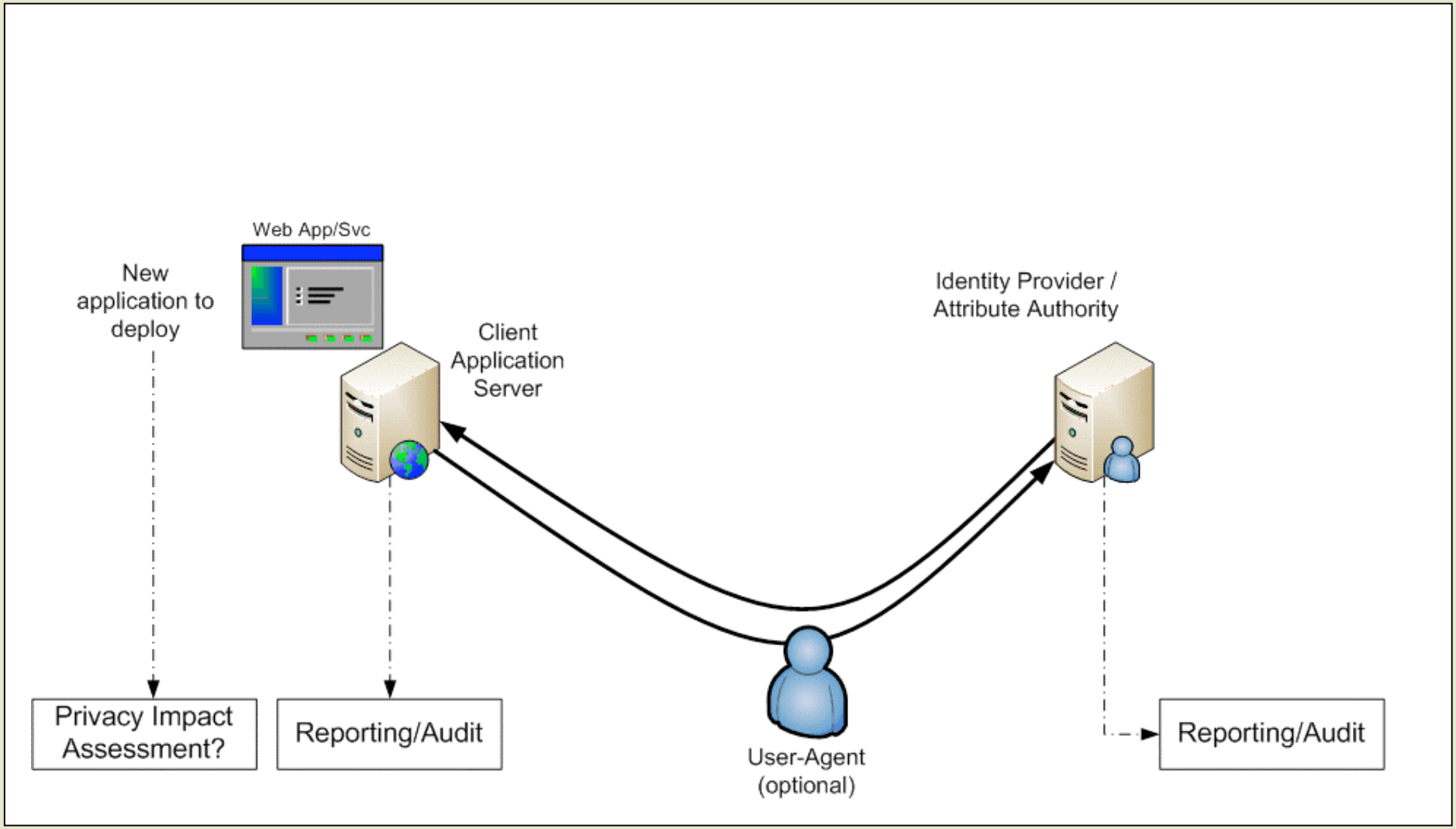
LIBERTY ALLIANCE PROJECT

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

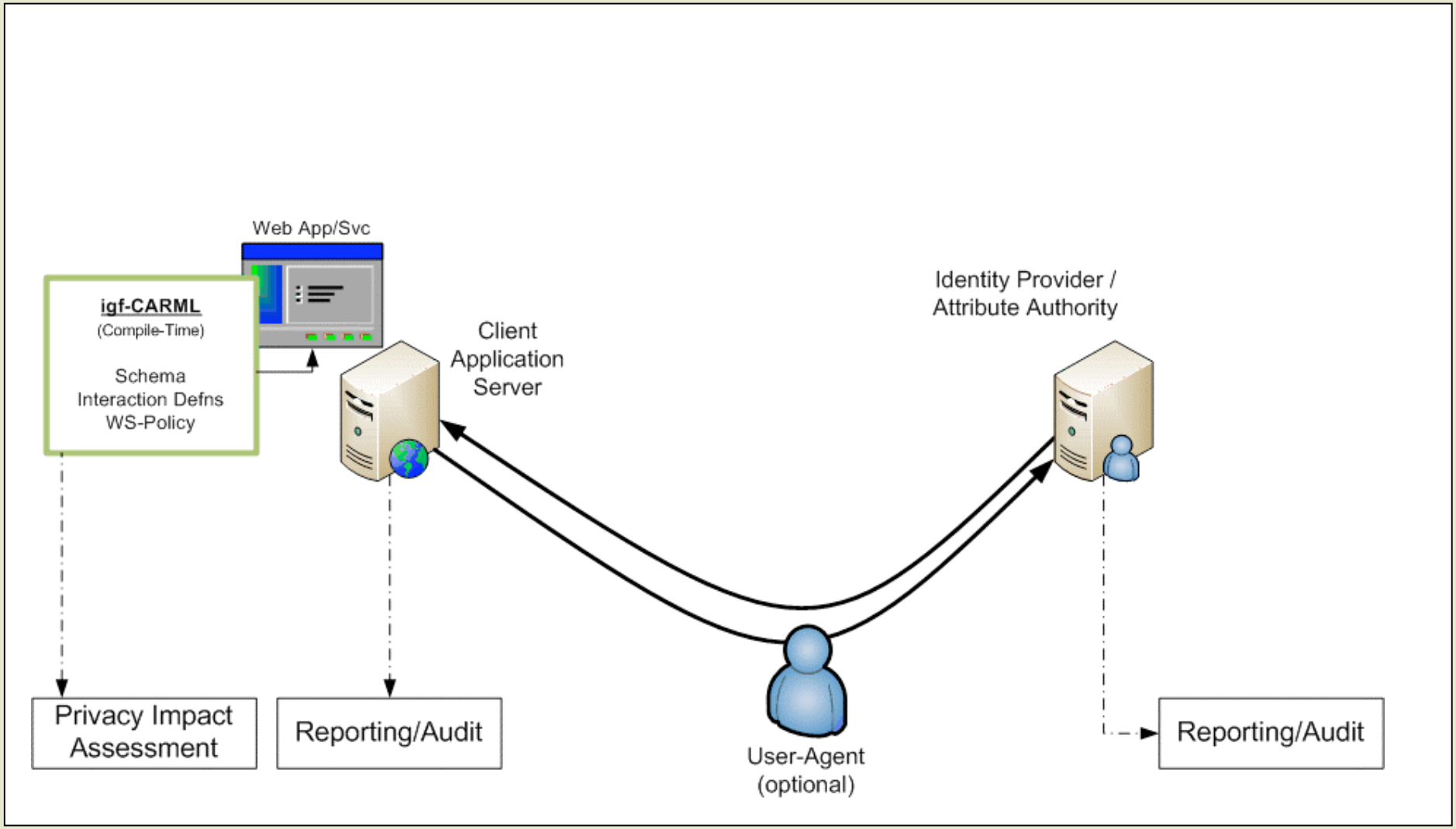
LIBERTY ALLIANCE PROJECT

IGF Walk-thru



LIBERTY ALLIANCE PROJECT

IGF Walk-thru



LIBERTY ALLIANCE PROJECT

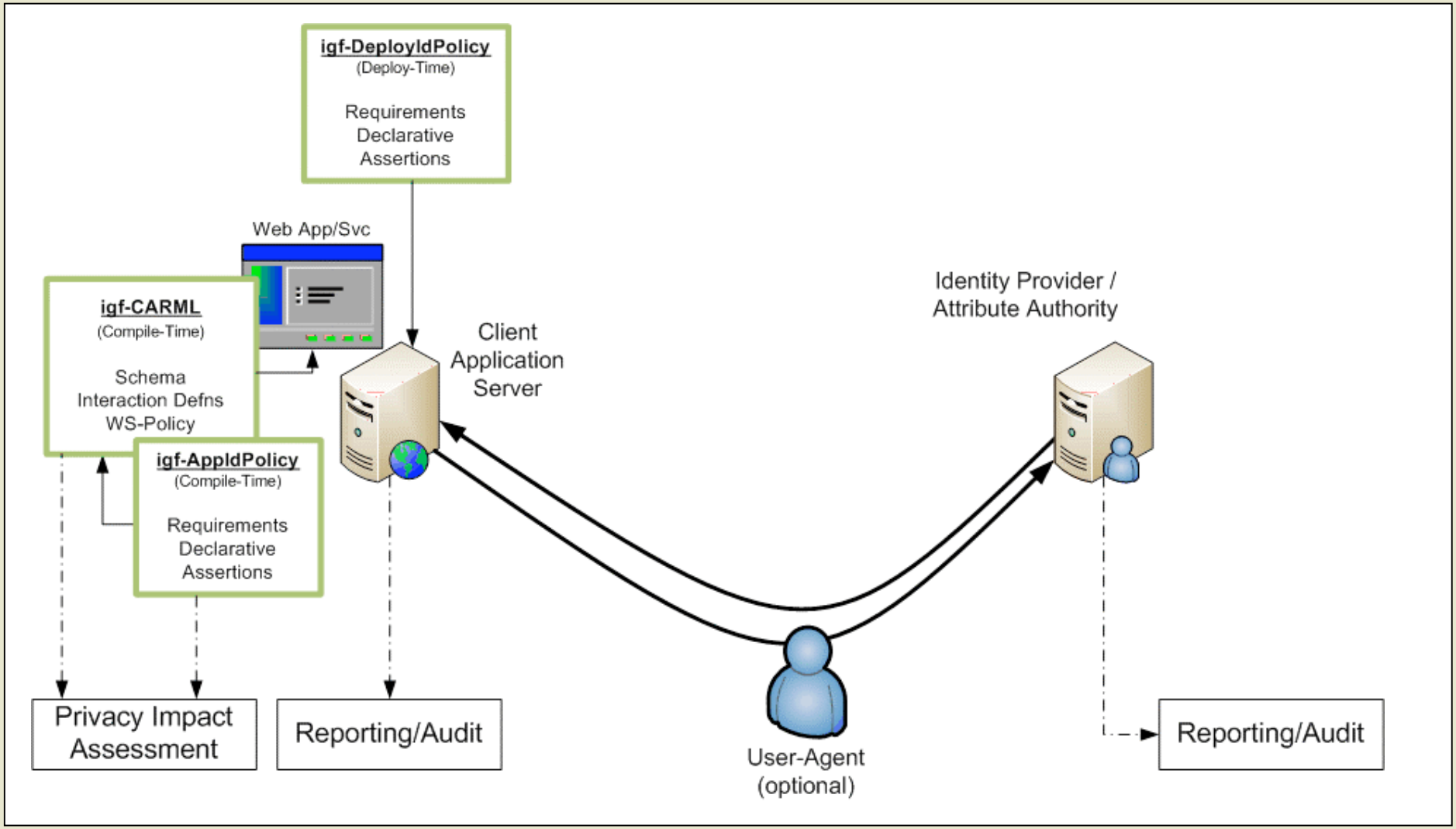
CARML

- 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”

LIBERTY ALLIANCE PROJECT

IGF Walk-thru



LIBERTY ALLIANCE PROJECT

WS-Policy Assertions

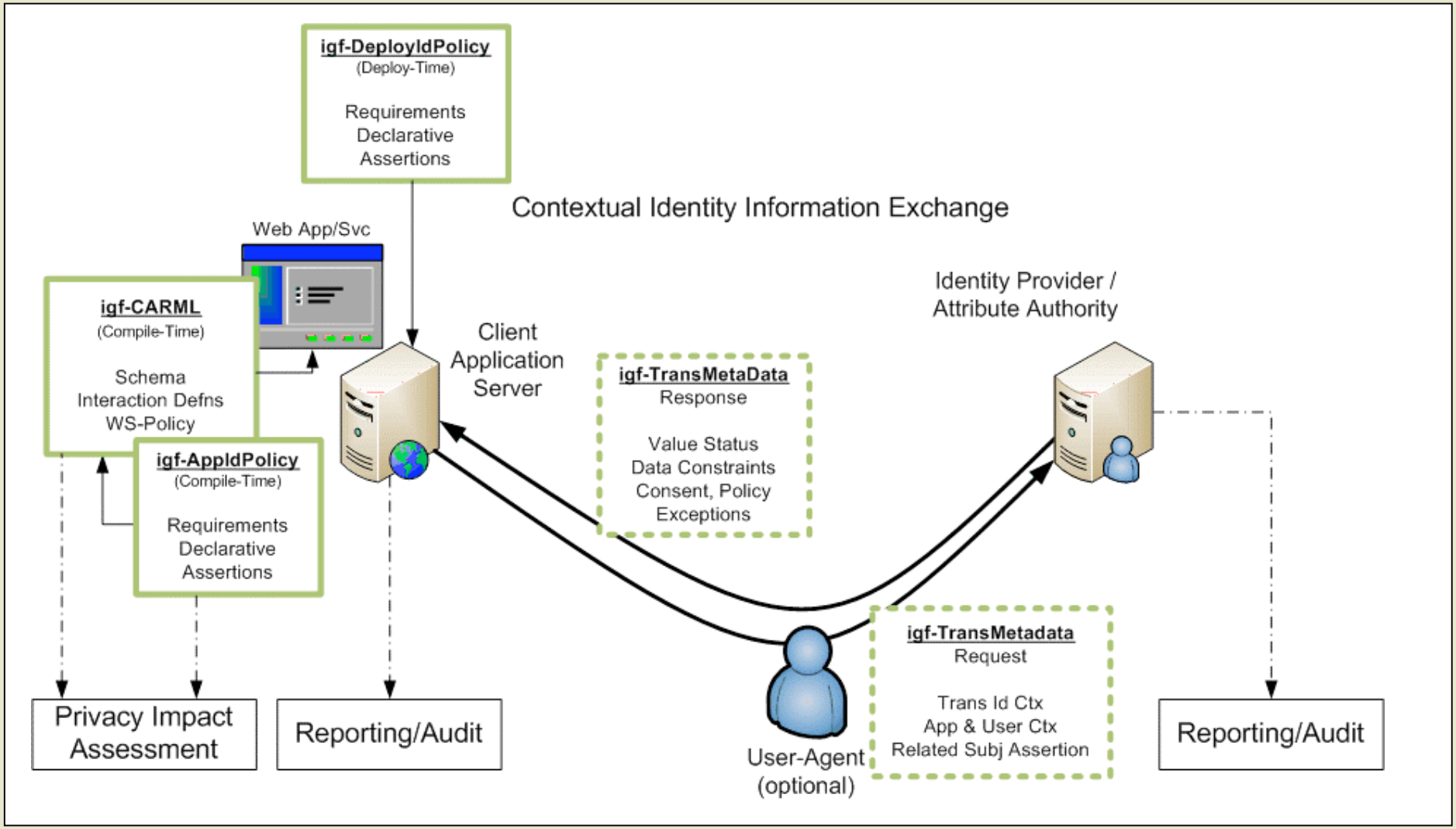
- igf-AppIdPolicy
  - *Compile-Time Assertions by Developer*
  - Assertions
    - Purpose
    - Retention
      - Duration & Archive Policy
    - Memory Cache
    - Processing (transient, encrypted, etc)
    - DataDisplayMask
    - ValueMask
    - PropagationServiceDefn

WS-Policy Assertions

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

LIBERTY ALLIANCE PROJECT

IGF Walk-thru



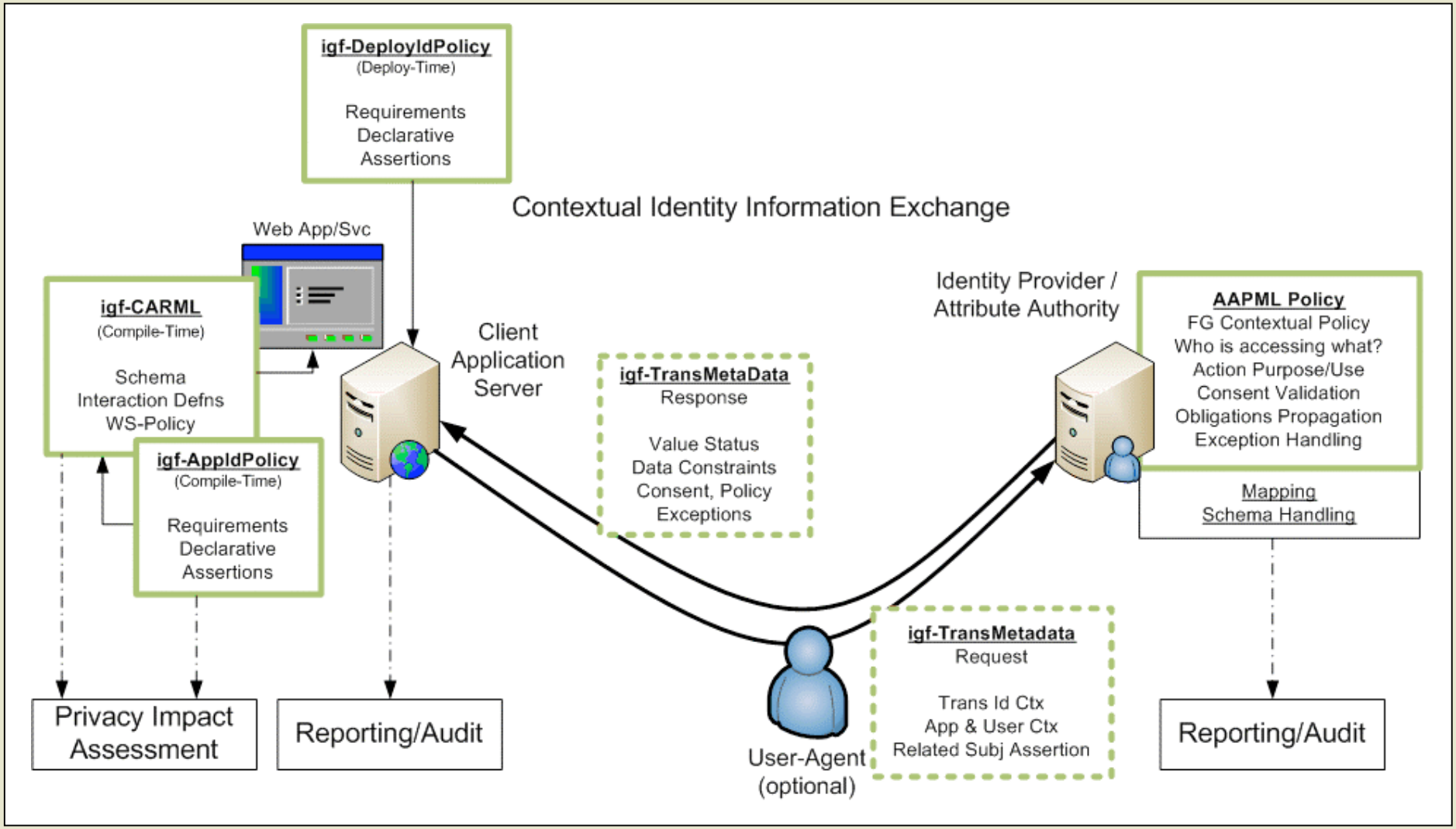
LIBERTY ALLIANCE PROJECT

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

LIBERTY ALLIANCE PROJECT

IGF Walk-thru

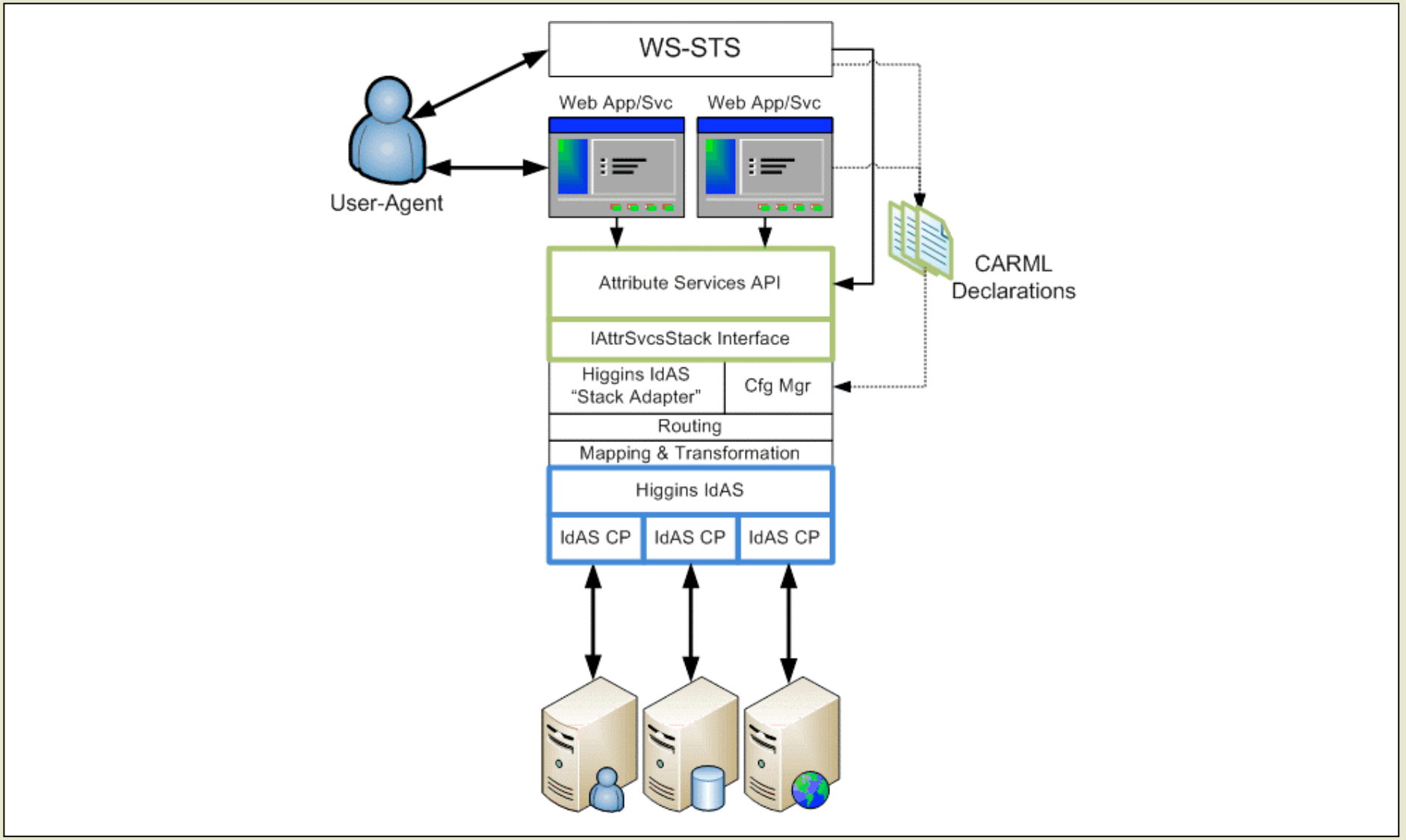


Assurance, Governance and Run-Time Protocols

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.

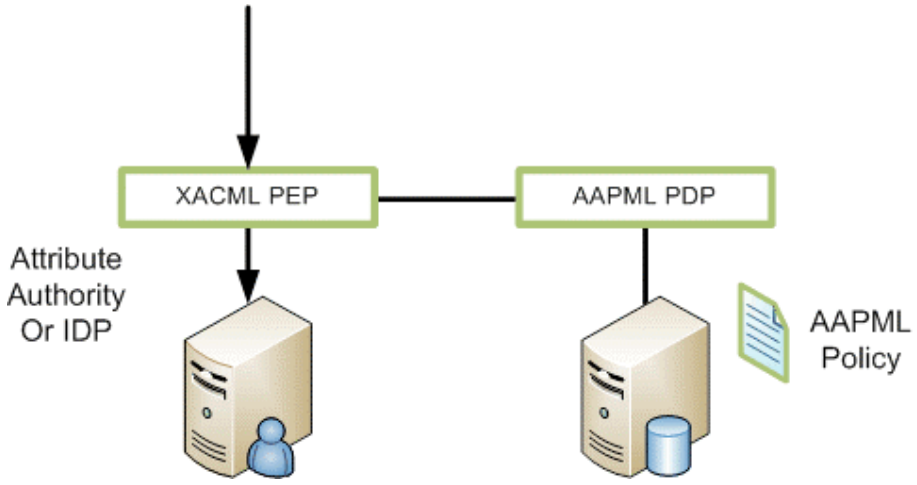
LIBERTY ALLIANCE PROJECT

Attribute Service & Higgins



LIBERTY ALLIANCE PROJECT

Attribute Service & Higgins



LIBERTY ALLIANCE PROJECT

Learn More

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

LIBERTY ALLIANCE PROJECT