LIBERTY ALLIANCE PROJECT

Identity Governance Framework Market Requirements & openLiberty Project

Prateek Mishra, Director Security Standards - Oracle
Phil Hunt, Principal, Identity Standards, IGF Lead - Oracle

Overview & Status

Agenda

- Background
- Introduction to Identity Governance
- Use Cases
- Standardization Path
- Q&A

LIBERTY ALLIANCE PROJECT

Agenda

- Background
- Introduction to Identity Governance
- Use Cases
- Standardization Path
- Q&A

LIBERTY ALLIANCE PROJECT

Business Drivers

- Legal: New Requirements for Identity Privacy
  - Requirements for accountability & ability to audit
  - Documentation, Audit, & Verification
  - Assessing Quality
  - Minimal use and minimal lifetime
  - Strong Role of Privacy Commissioners
- Reality: Most Identity In Application Silos
  - Most identity information lives inside application silos
  - Copy, Sync, & Aggregate is Standard Bad Practice
  - Applications are slow to change
  - Both technology and legal are driving change

Technical Drivers

- Historical: Developers Are Not Identity Experts
  - High deployment variability
  - Poor IDE tools
  - No IDE integrated testing & debug
  - Standalone identity is best for success
- Market: Federated Identity
  - New protocols support browser-centric identity & federation SAML, ID-FF,WSF, WS-*, OpenId,…
  - Movement to support user privacy and confidentiality
  - Rise of the identity meta-system

Motivators

- How can we include developers in the Identity Metasystem?
  - How do we make it easy to use identity services
  - How do we make it easy…
    - To understand application identity-data requirements?
    - To support multi-protocol, multi-vendor environments?
    - To support multi-organization, multi-system, multi-authority business environments?
    - For developers to adopt?
- How to understand (& audit) what identity information applications consume & what they do with it?
- When identity data is shared, how do we ensure it is accurate, useful, and above-all appropriate?

Agenda

- Background
- Introduction to Identity Governance
- Use Cases
- Standardization Path
- Q&A

LIBERTY ALLIANCE PROJECT

What is the Oracle IGF Strawman?

- Original Spec Drafted by Oracle - November 2006
  - Two specifications – CARML, AAPML
  - A set of declarative documents between suppliers and consumers of identity-related information.
- Plan to Explore Possible Open Source Implementations
  - Developer APIs
  - IDE Tools
  - Policy services
- Focus
  - Policy-driven framework to support management and governance
  - Establish policies for use of identity-related information
    - Domain and inter-domain capable
  - Multi-protocol support - policy independent of protocol
  - Standards will support better developer adoption and ability to audit privacy compliance of user-centric systems

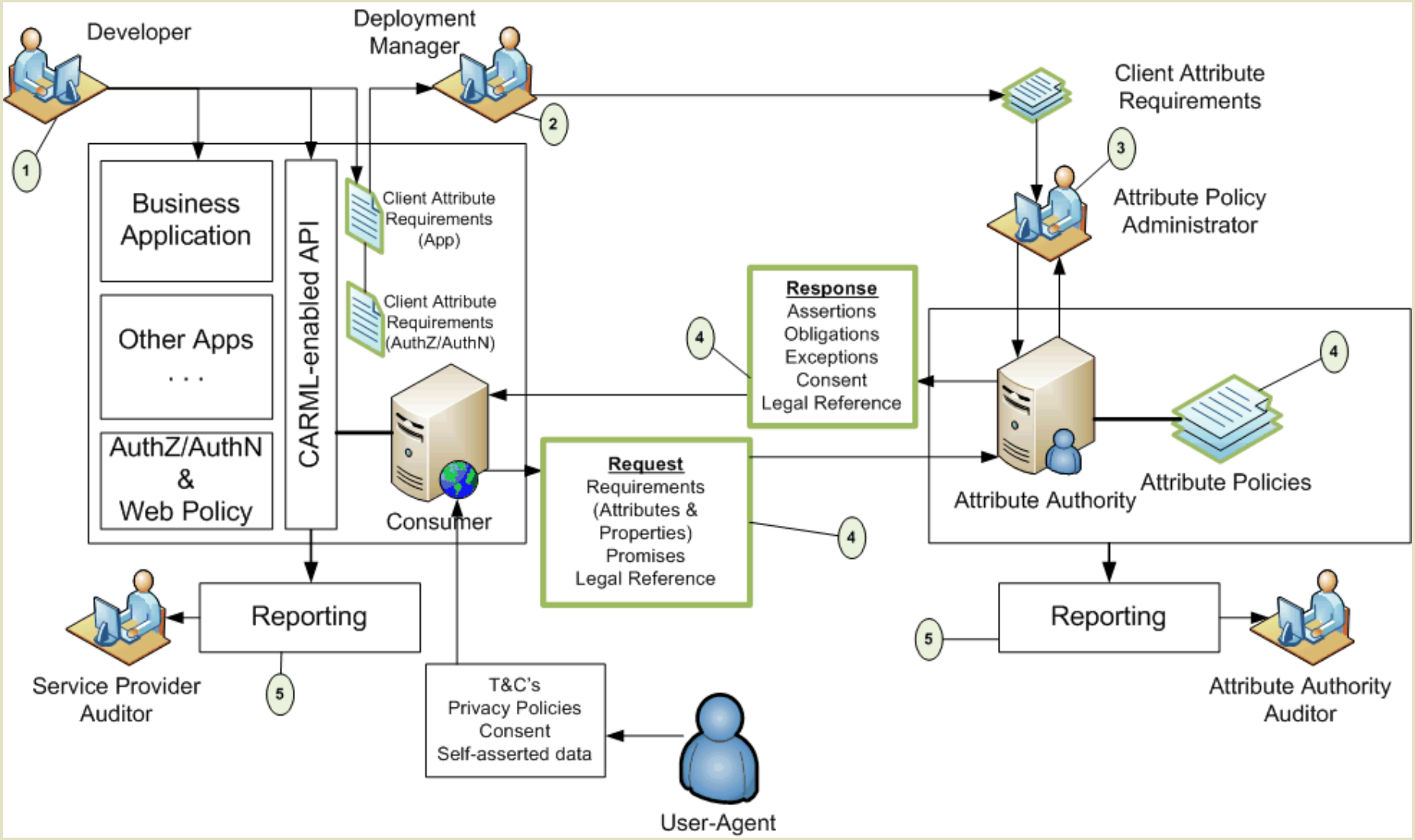
Principles

- Data collectors/requestors (e.g. enterprises, service partners, etc.) should state the purposes for collecting data
- Identity-related data is distributed & web based
- Must have a defined reason for using data
- User consent must be supported and enforced
- Data should be used and disclosed consistently
- Data should be deleted/disposed as agreed/when it is not required any longer

Why Standardize Policy?

- Connecting existing & new applications to the Identity Meta-system
- Complex and varied jurisdictional requirements will hamper adoption of federated protocols
  - Inter-play between provider, user, and relying parties
- Need audit & policy support layer regardless of protocol
  - Application deployers need multi-protocol support for some time
  - Exchange of identity data requires some policy data exchange (e.g. consent, restricted use obligations)
  - Common reporting & auditing
  - Policy crosses boundaries and products
- Lessons learned from the past
  - Policy languages are difficult to convert once written (e.g. LDAP)

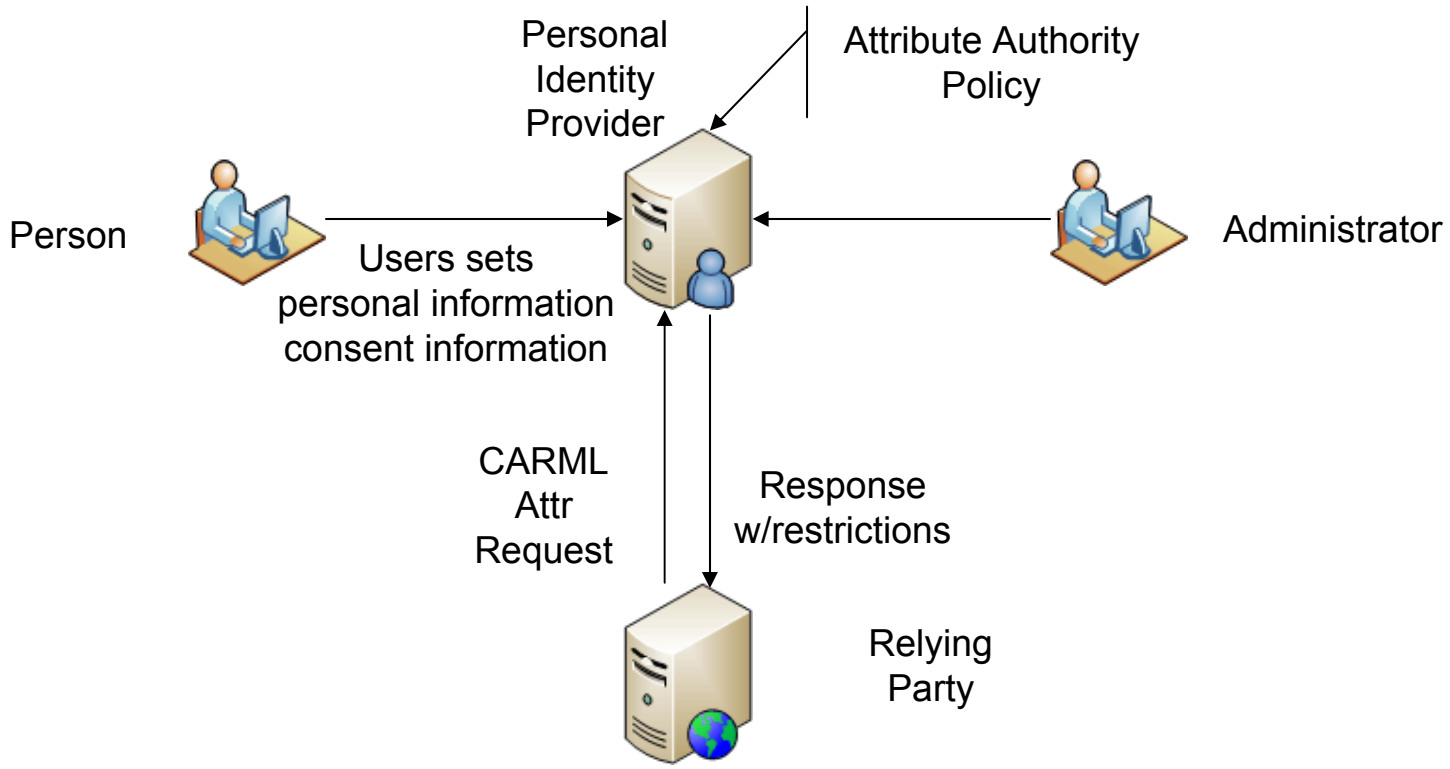
IGF Lifecycle



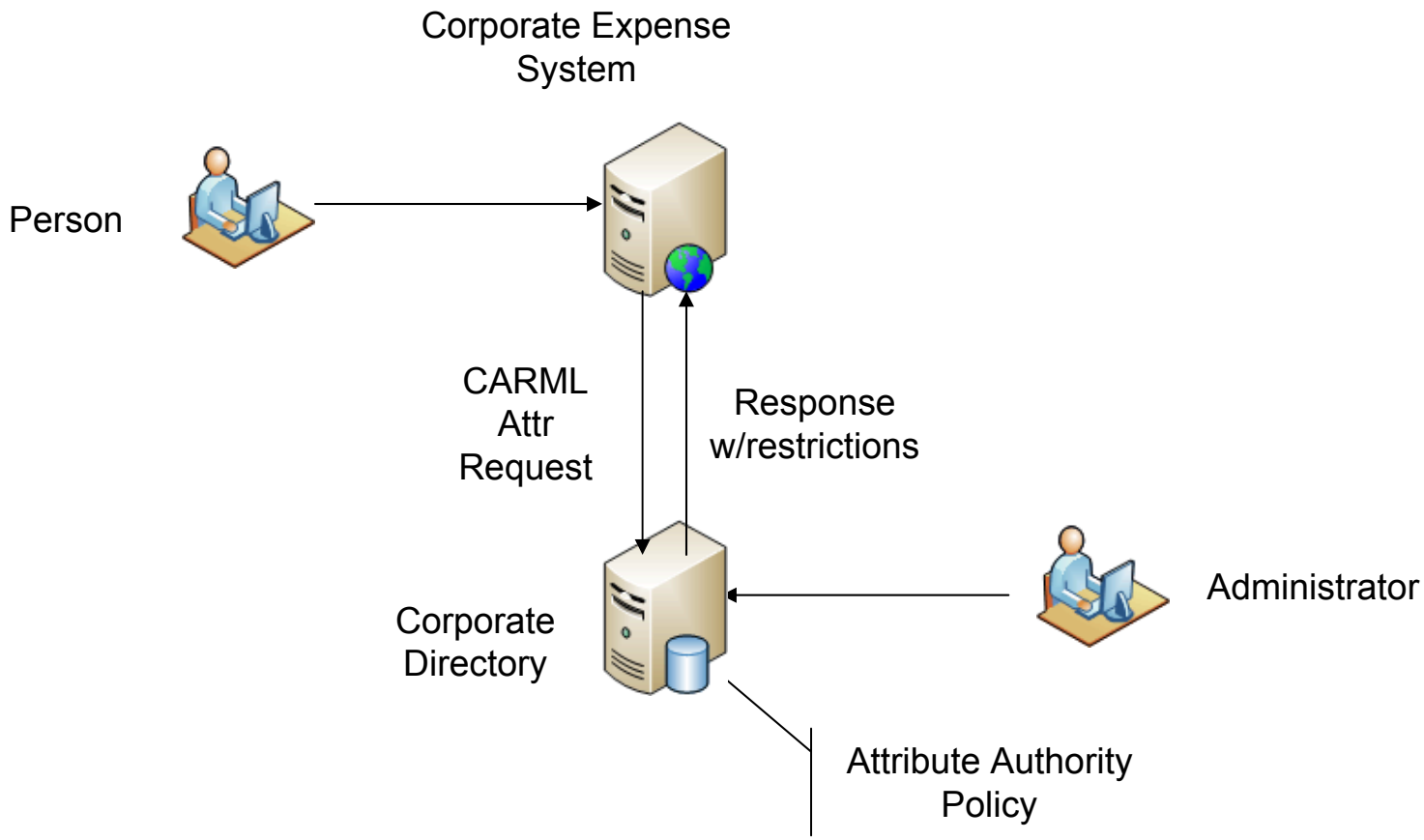
Agenda

- Background
- Introduction to Identity Governance
- Use Cases
- Standardization Path
- Q&A

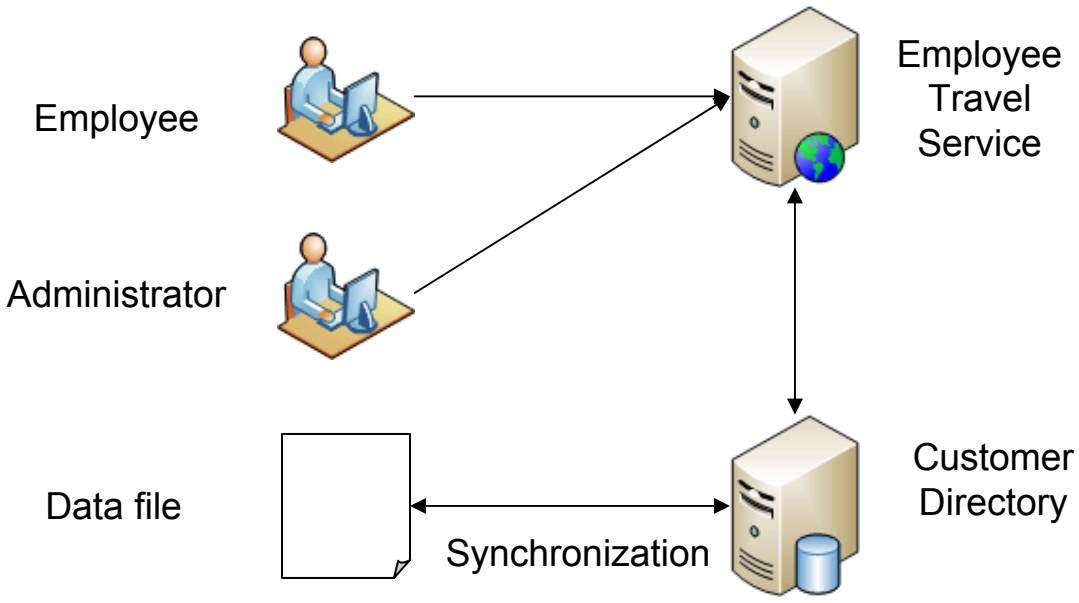
Personal Identity Provider



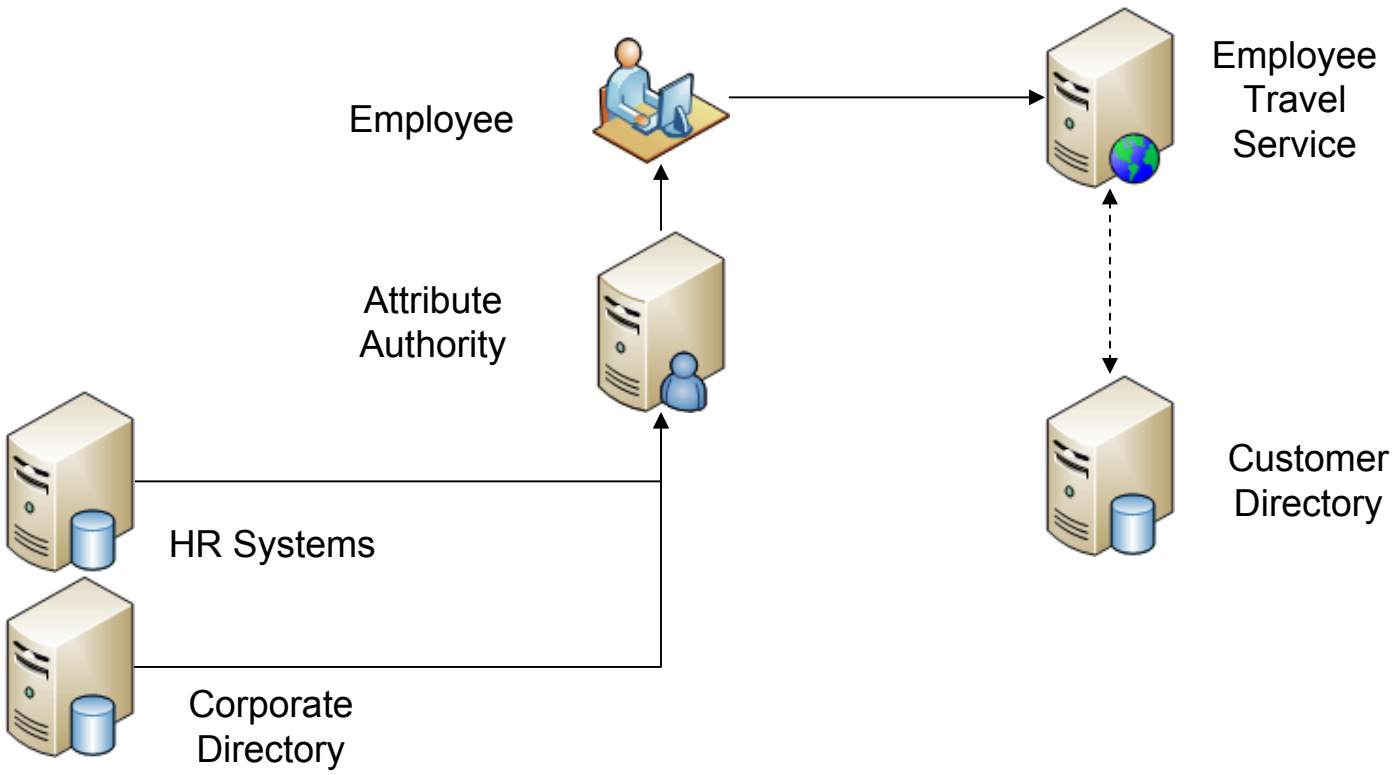
Corporate Application



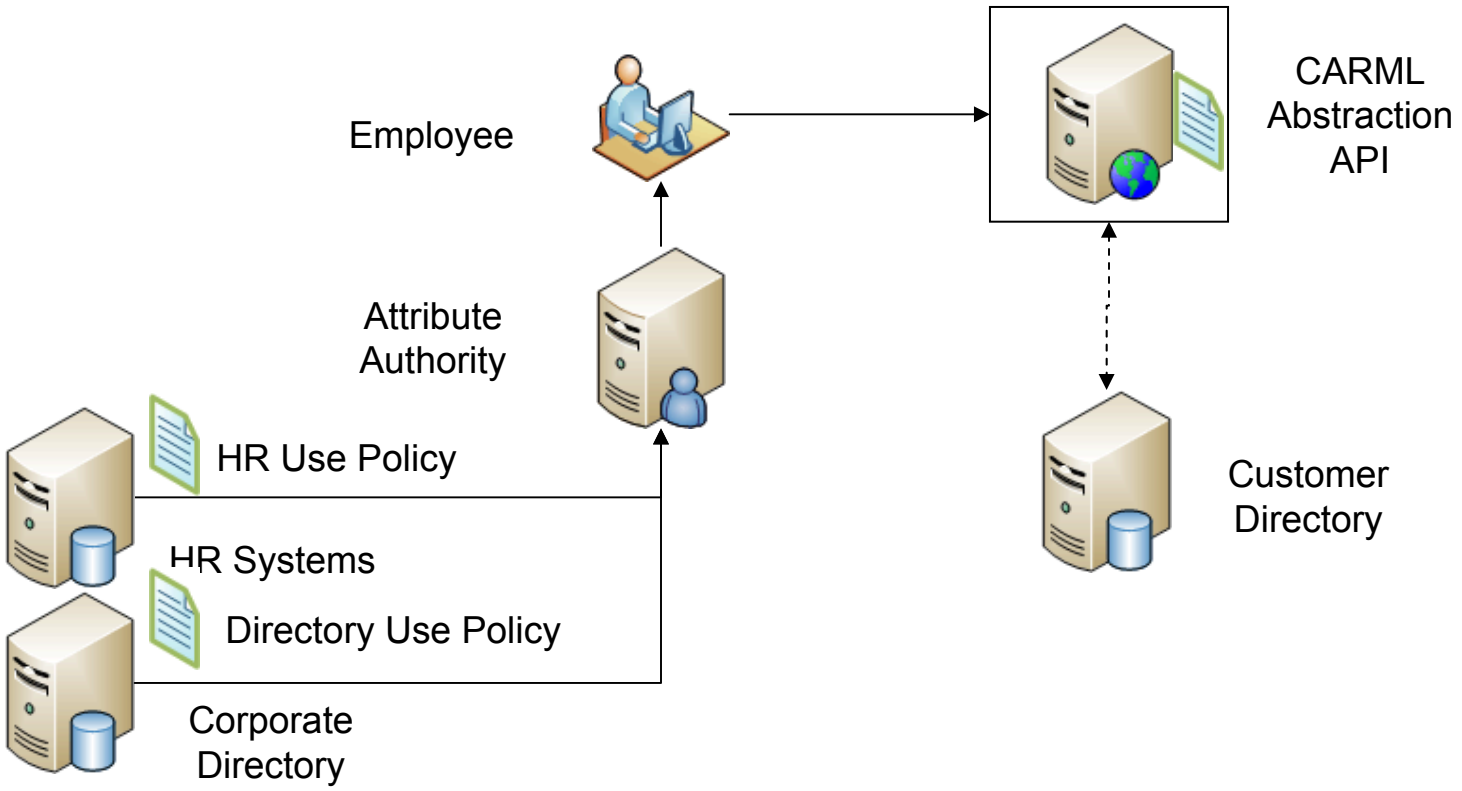
Travel Service



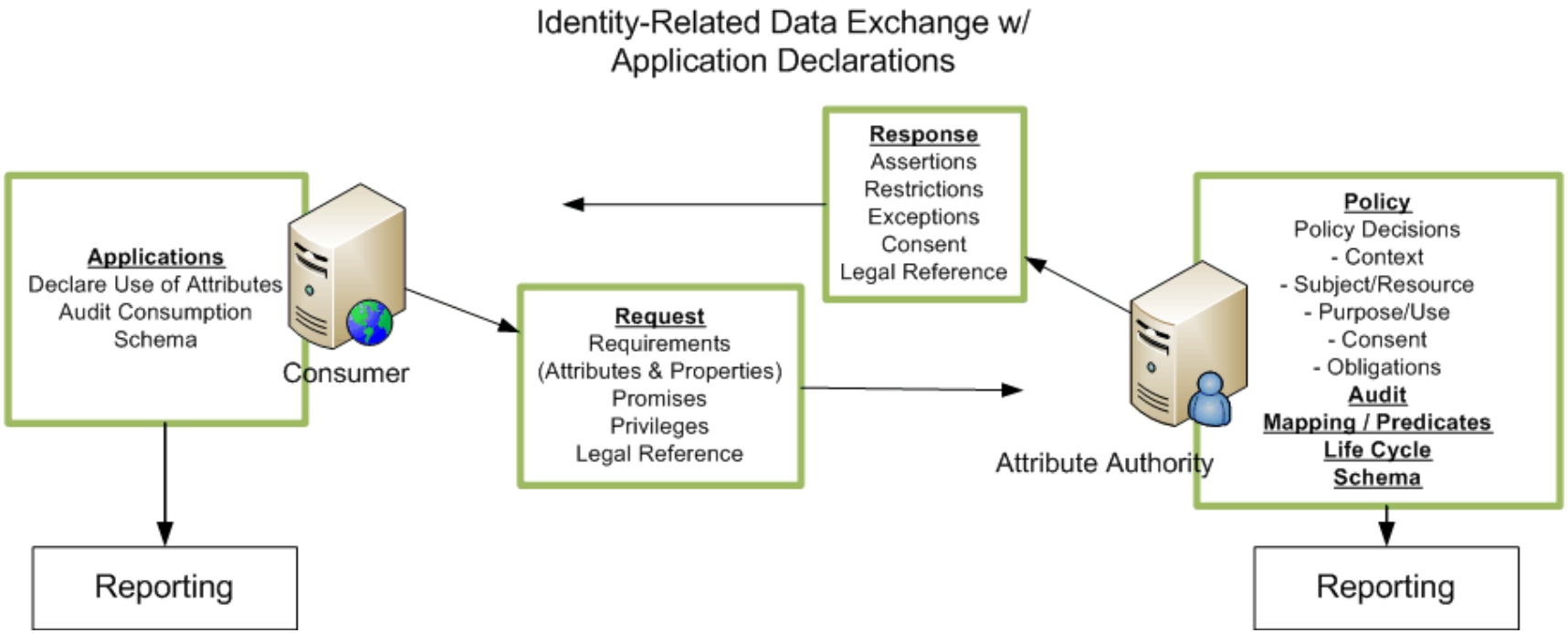
Travel Service



Travel Service



Declarative Exchange



Agenda

- Background
- Introduction to Identity Governance
- Use Case
- Standardization Path
- Q&A

LIBERTY ALLIANCE PROJECT

Nov 2006: Oracle Announces IGF

1. Open-vendor initiative to address handling of identity related information within enterprise lead by Oracle
2. Released key draft specifications
   - CARML and AAPML
   - Announced intention to submit to a standards org
3. Key vendors supported initiative
   - CA, Layer 7, HP, Novell, Ping Identity, Securent, Sun Microsystems

February 7, 2007: Transfer To Liberty

- Start of broader open review under BMEG
- Work begins on gathering expanded use-cases and market requirements
- Oracle makes IGF “straw-man” specifications available royalty-free
- Participation from:
  - Computer Associates, France Telecom/Orange, Fugen, HP, Intel, NEC, New Zealand, NTT, Oracle

July 2007: IGF MRD & Open Source

- IGF MRD Released July 2007 www.projectliberty.org/index.php/liberty/strategic_initiatives/identity_governance
- Plan two step completion of Id Governance Framework
  - Development of open source components at www.openliberty.org
  - Technical work – specifications and profiles – to continue at Liberty Alliance and complete in 2H-2008
    - Follows successful completion and publication of IGF Market Requirements Document within Liberty Alliance
  - Supported by HP, CA, Cisco, Novell, SUN and other partners

July 2007: Standards Plan

- Publication of Id Governance Marketing Requirements Document
  - Available from http://www.projectliberty.org/MRD
  - Explains use-cases and requirements met by the effort
  - Active participation of CA, HP, Intel, NTT, NEC, NZ Govt SSA
  - Concludes initial phase of IGF work begun in January 2007
- Next Steps: development of profiles/specifications/recommendations based on requirements within Liberty Alliance
  - Anticipate key drafts to be ready in 2H-2008.

Open Source Plans

- Hosted at www.openLiberty.com
  - Based upon Apache 2.0 license
  - Create software libraries aimed at developers
  - Aligned with open source ecosystem (Higgins, Bandit)
    - Re-use existing components wherever possible
  - Simultaneous with creation of Liberty final specification drafts
    - Based on Liberty IGF MRD and original Oracle IGF technical materials
      - www.oracle.com/goto/igf
      - www.projectliberty.org/index.php/liberty/strategic_initiatives/identity_governance
      - Update to final Liberty drafts when available

Summary

- Identity Governance Framework
  - Open initiative for identity governance across enterprise systems
- Key draft specifications provide initial policy components
  - CARML, AAPML
  - Intent to ratify as full standards at an existing standards body
- Under Liberty Alliance Leadership
  - Broad input and support in an open standards process
  - Legal community review
  - IP clearances - open standards for everyone to use

Learn More

- www.projectliberty.org/index.php/liberty/strategic_initiatives/identity_governance
  - IGF Overview Whitepaper
  - FAQ
  - Use Cases (MRD)
  - Links to Oracle draft specifications:
    CARML, AAPML, Client API

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

LIBERTY ALLIANCE PROJECT

Agenda

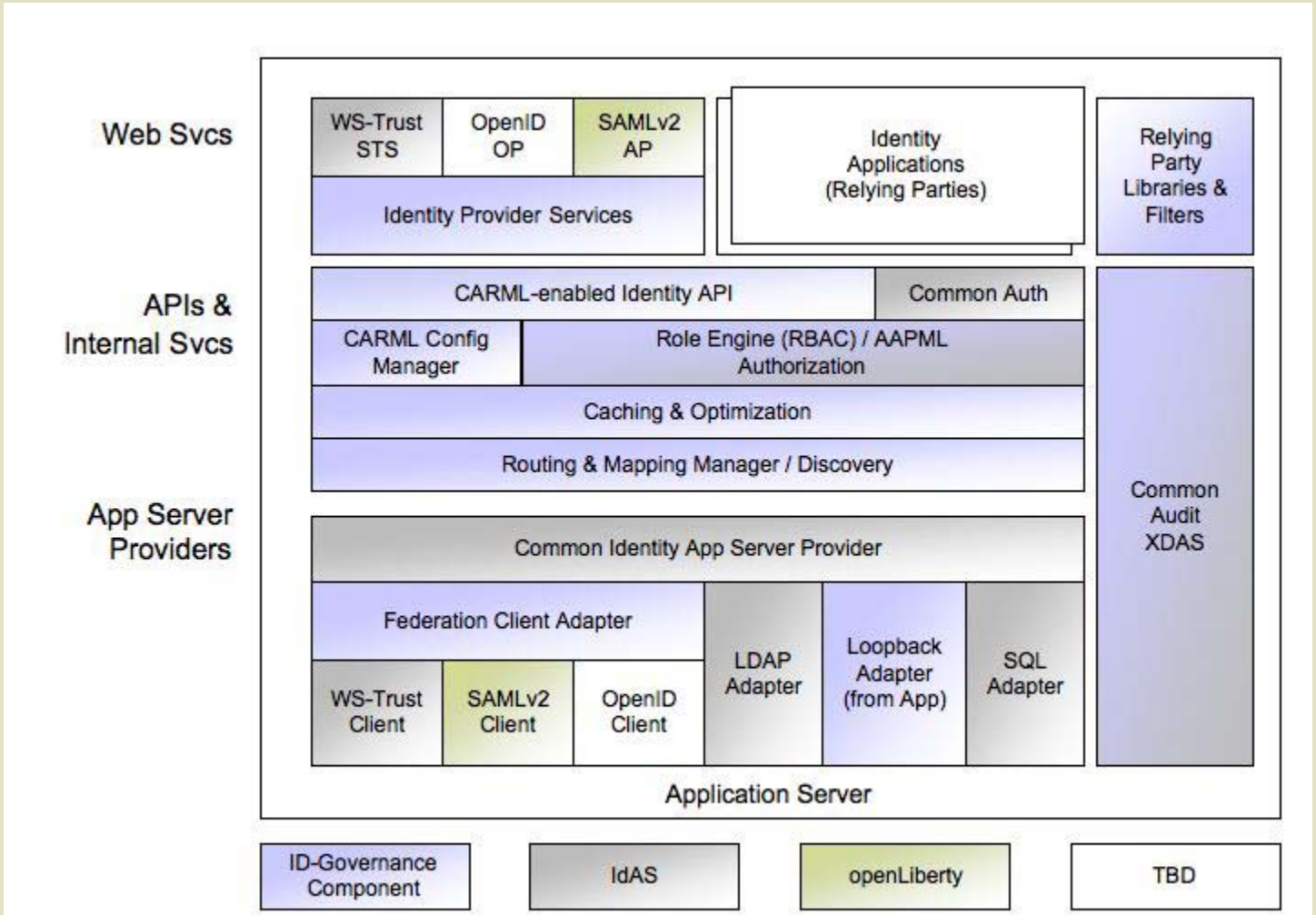
- Background
- Introduction to Identity Governance
- Use Case
- Standardization Path
- Q&A

LIBERTY ALLIANCE PROJECT

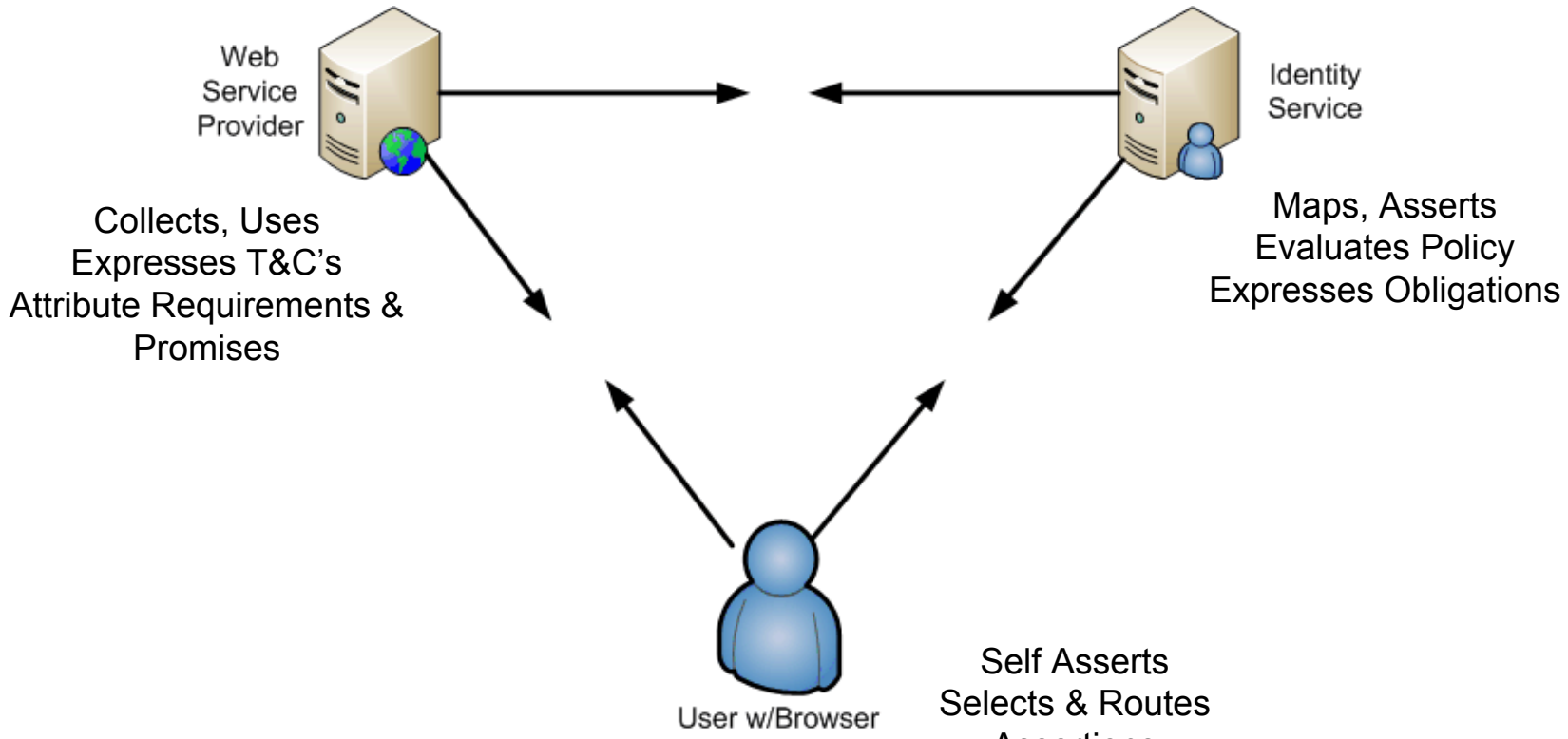
LIBERTY ALLIANCE PROJECT

Q &A

IGF Open Source Arch



Policy Players

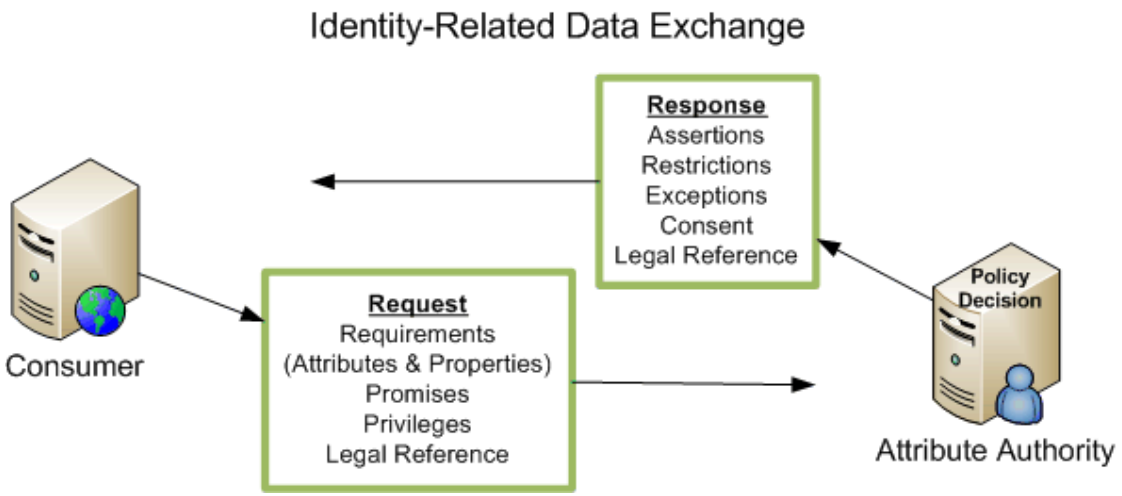


Attribute Authority Types

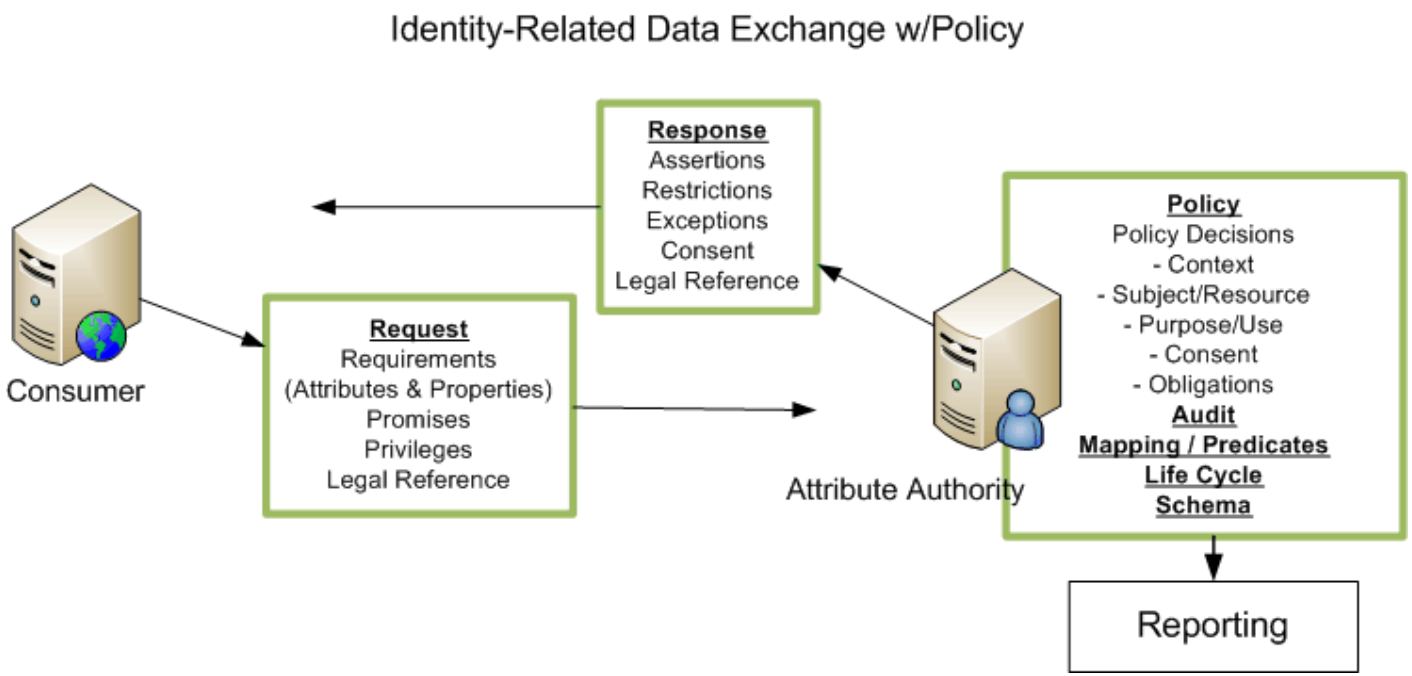
- User-Managed - direct user control
  - Profile service
  - Self-managed & asserted
- 3-rd Party - managed by some autonomous entity distinct from the user.
  - The entity controls access who may use it
  - The user may or may not assert data
  - Entity has some relationship with the user
- Autonomous - no direct relationship with the user
  - E.g. Credit Card Rating, Criminal History
- Enterprise - managed by an enterprise
  - E.g. an employer
  - User has influence but may not control directly in all cases

➔ Each of these cases requires policy to ensure privacy & reliability

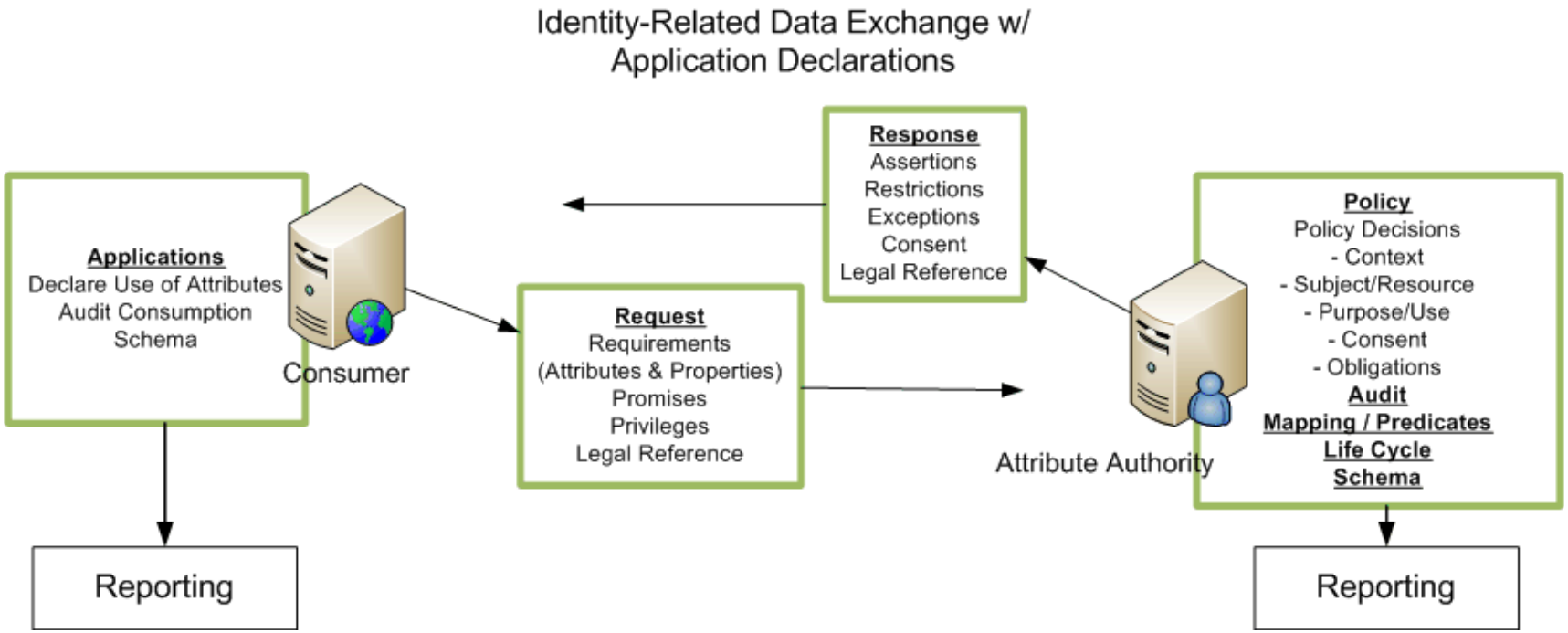
How IGF works…



AAPML Policy



CARML-Enabled Apps



LIBERTY ALLIANCE PROJECT

In Browser-Based Exchange