



IIW - IGF Policy Introduction & Update

Phil Hunt, Oracle
Internet Identity Workshop, 2007

Agenda

- Background
- Introduction
- Update
- Q&A

Background

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: User-Centric 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

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
 - Applications are slow to change
 - Both technology and legal are driving change

Why Standardize Policy?

- Need to adapt existing applications as well as new ones to the Identity Meta-system
- Complex and varied jurisdictional requirements will hamper adoption of user-centric protocols
 - Inter-play between provider, user, and relying parties
- Need audit & policy support layer regardless of protocol
 - Because at the moment, it appears deployers may 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

Introduction to Identity Governance

Motivators

- How can we include developers in the Identity Metasystem?
 - How do we make it easy to use services
 - How do we make it easy to understand application requirements
- 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?

Oracle Announces IGF: Nov 2006

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: IGF Submitted To Liberty

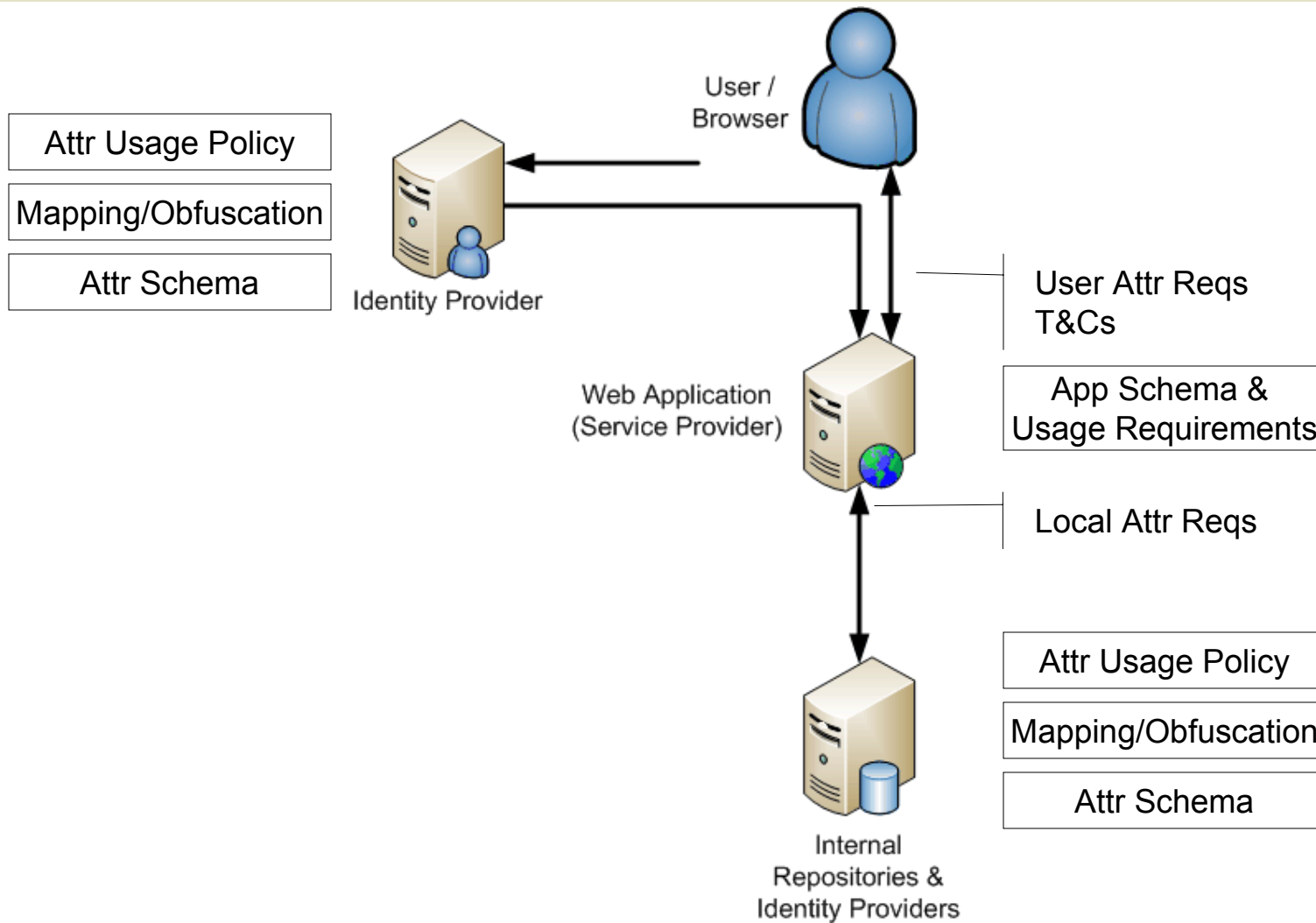
- Start of broader open review
- Work begins on gathering expanded use-cases and market requirements
- Oracle makes IGF “straw-man” specifications available royalty-free
- Prateek Mishra is chairing the IGF “MRD” committee

What is the IGF strawman?

- Proposed
 - 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

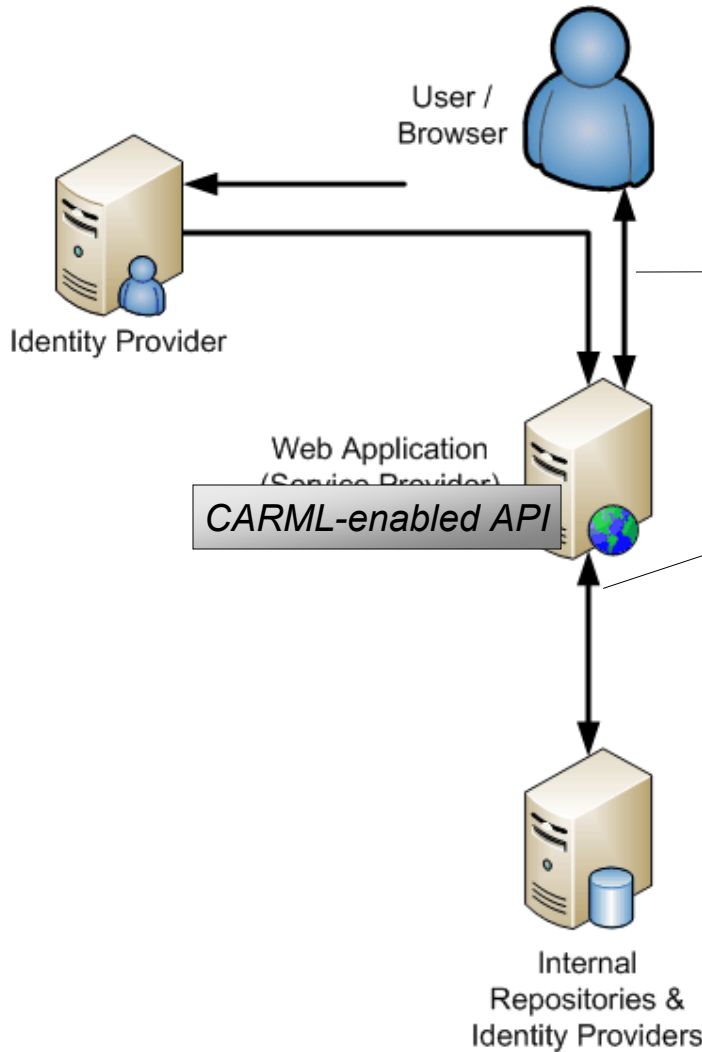
- Data collectors/requestors (e.g. enterprises, service partners, etc.) should state the purposes for collecting data
- Identity-related data is distributed & web based
- Must have a defined reason for using data
- User consent must be supported and enforced
- Data should be used and disclosed consistently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



Attr Auth Policy

Mapping/Obfuscation

Attr Schema



Multi-protocol support
(OpenID, SAML, ID-FF, WS-*)

*Client Attribute
Requirements*

Multi-protocol support
(LDAP, OpenID, SAML, WSF,
WS-*)

Attr Auth Policy

Mapping/Obfuscation

Attr Schema

Update

Liberty Work Progresses

- Broader Industry Review
- Reviewing and expanding
 - Use cases
 - Requirements
- Publication expected 3-4 weeks (pending legal)
- Next steps...
 - Review alignment with existing standards
 - Develop protocol profiles
 - Identity protocol specific policies (e.g. P3P)
 - Assignment of Expert Groups
 - Open source initiatives

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.oracle.com/goto/igf
 - IGF Overview Whitepaper
 - FAQ
 - Draft specifications of CARML, AAPML, Client API
- Inquiries to
 - Mail: phil.hunt@oracle.com
 - Blog: blogs.oracle.com/identityprivacy

Q & A