The Identity Governance Framework
Liberty Alliance’s Privacy Initiative

John Aisien
Vice President, Product Management
Fusion Middleware, EMEA
john.aisien@oracle.com
Agenda

- Introduction
- Use Cases
- Standardization Path
- Q&A
Observations about Identity Data

- Identity is essential to enterprises and web sites providing services to customers
  - Many different sources of information (attribute authorities)
    - Enterprise: HR, CRM, Partners, IT Directory, Departmental Systems,
    - Internet: Portals, users, banks, employers, governments, retail, identity processors (background and credit checks)

- Increasing legal and regulatory focus
  - Privacy & Compliance:
    - EU Data Protection Directive
    - US: HIPAA, SB 1386, SOX, GLB
    - Many others
  - Industry vertical regulations: credit bureaus, credit card processors (PCI standard)

- Identity data is a significant source of enterprise risk!
Myths about identity data

- Myth #1: Users/Citizens have complete control over their personal identity information
  - NOT!
  - Enormous amount of information available from public sources
  - Business contracts govern identity data held by employers, banks, schools, portals, associations
  - Autonomous identity sources are flourishing
    - Background check, credit bureau, crime registries, Google?

- Myth #2: It’s hopeless – Scott McNealy was right!
  - "You have no privacy. Get over it."
  - But collectors and users of identity data are targets of regulation and lawsuits.
    - Requirements for accountability & audit
GOAL: Reduce risk for all applicable organizations
- Creation, maintenance & use of identity data
- Who has access to my social insurance number or account numbers? Under what conditions? For what purpose?

Declarative statements (i.e. policies) published by consumers (i.e. applications, services) and sources of identity data (attribute authorities)
- Enterprises can audit and implement governance against these policies
Observations on Key Parties

- Users
  - Capture what agreements the user accepted
  - Reflect consent and purpose of data use
  - But IGF does not directly address interactions with users

- Applications Developers
  - Developers are not identity experts
  - How can they express application identity requirements at development time?
  - Tools and frameworks for developers are a key focus for IGF
Observations on Key Parties

- **Application Deployers**
  - Have to deploy applications in open environments
  - Often restricted by developer assumptions
  - Need to understand the identity requirements of an application
  - Need to decide who the acceptable authorities of information are

- **Attribute Authorities**
  - Identity-related data is distributed & web based
  - User consent must be supported and enforced
  - Enable owners of identity data to express use constraints
  - Need to be able to define policy on use

- **Auditors**
  - Need to understand where information is stored and consumed
  - Need to be able to assure that correct policies and procedures are followed
  - Need to provide GRC compliance
IGF Components

- **CARML** – Defines application identity requirements
  - What identity information an application needs and how the application will use it

- **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

- **IGF Enabled Protocols** – Links applications to identity data

- **Developer APIs/Tools** – Developers can express identity requirements at a business level at development time
  - Key to IGF adoption & use
Agenda

- Introduction
- Use Cases
- Standardization Path
- Q&A
IGF Part 1: Foundations

1. Multi-protocol (LDAP, WS-Trust, SAML, ID-WSF, ..)
2. Focus on producers and consumers of identity data
Many distributed authorities, each capable of expressing constraints on use of identity data
Applications publish requirements for identity data.
IGF Part 4: App Developer and Enterprise Administrators

- **Application Developer**
  - Identity needs of business applications expressed at a high-level
    - Application developers lack identity middleware expertise
  - Declarative model is preferred
  - Ability to express identity requirements at a business-level without regard to sources

- **Enterprise Administrators**
  - Support for deployment-time binding to specific identity architectures which vary over time and between enterprises
  - Declarative approach simplifies compliance and configuration
Agenda

- Introduction
- Use Cases
- Standardization Path
- Q&A
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
   - Sample CARML API
   - Announced intention to submit to a standards org
3. Key vendors supported initiative
   - CA, Layer 7, HP, Novell, Ping Identity, Securent, Sun Microsystems
• Start of broader review 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
• IGF Market Requirements Document Released July 2007
  • Use-cases, Scenarios, End-to-End Examples
  • www.projectliberty.org/index.php/liberty стратегic_инициативы/identity_governance
Next Steps (2007-2008)

- Two parts -
  - 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, NEC, NTT, Novell, SUN and other partners
Open Source

- 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 стратегических инициатив/идентификация/гovernance
    - 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:
    - Oracle: phil.hunt@oracle.com & prateek.mishra@oracle.com
    - Liberty: britta@projectliberty.org & brett@projectliberty.org
  - Blog: blogs.oracle.com/identityprivacy