Introducing ArisID
“An open source, declarative identity API for developers”

OpenLiberty Webcast
Dec 11, 2008
Phil Hunt, Oracle
phil.hunt@oracle.com
An open community of developers formed in January 2007 to coordinate synergies among global open source initiatives and to identify and deliver the open source libraries developers need to build applications that take advantage of the features in Liberty Alliance standards, including: the Liberty Identity Governance Framework (IGF), Liberty Advanced Client, Liberty Federation (SAML 2.0), and Liberty Identity Web Services (ID-WSF2.0 and ID-SIS*).
A declarative identity-API, has the potential to:

- De-couple applications from specific infrastructure,
- Describe clearly the requirements and use of identity information in an application,
- Enable use of multiple modalities of identity, and
- Create a much simpler, easy-to-learn API
- Primary focus on needs of developer
- Key support for infrastructure managers, privacy & compliance officers, business managers
Project Principles

- An open community project
- Apache 2.0 License
- Encourage wide re-use
  - IDE Integration
  - Application Servers
- Don’t re-invent
  - Re-use existing open source and commercial products
  - Collaborate with other projects
Why do developers of applications choose to roll their own identity management?

Because:

- Schema can be controlled & unique
- Identity management can be controlled
- Environment can be controlled
- User-experience can be controlled
- No new systems and protocols to learn and invest in
  - I’m not sure XXXX is will last
Current Issues

- Developers unfamiliar with identity protocols and associated programming libraries
  - Interoperability issues
  - Protocol mistakes and errors
- Developers don’t care about privacy requirements
  - Minimal data usage and retention
  - Consent handling
  - Data assurance/quality
  - Legislative requirements
- Is the application generating personal information?
  - Even with minimal data, the application may generate new information about individuals
Many Identity Sources

- Healthcare & Benefits
- Travel & Other Services
- Telecom
- Professional
- Employees, Contractors
- CRM / Sales
- E-Mail
- HR Systems
- Financial & Purchasing Systems
Trends

- Increasing Information Sources:
  - How to determine best or appropriate source
  - What quality or assurance level is a source?
  - Multiple sources may need to be consulted

- Increasing Entropy:
  - Number of applications, repositories, protocols

- More Structure:
  - Changing distribution, federation, aggregation requirements
Modes of Identity

Front-channel

User Offline
Application
User Online

Back-channel

Workflow
Message-based

Atomic
Dynamic
Modes of Identity

Front-channel

Browser-centric

Atomic

Dynamic

User Offline → Application → User Online

ID-WSF

SPML/DSML

LDAP

Workflow

Message-based

Back-channel

SQL

User Online

Application

User Offline

Browser-centric

Atomic

Dynamic
Modes of Identity

Front-channel

Atomic
Dynamic

Application

User Offline

Workflow
Message-based

Back-channel

User Online

ArisID
“Solving a problem by adding a level of abstraction is a very common technique in computer science, and the examples of spectacular successes abound.”

- Vittorio Bertocci et al, “Understanding Windows Cardspace”
Current Approach

- Application View Logic
- Application Control Logic
- Application Data Model / Beans
- Cfg Mgmt
- Cxn Mgmt
- DATA PROTOCOL
- TCP/IP
Inflexible Applications

Application View Logic

Application Control Logic

Data Model / Beans

Cfg Mgmt

Cxn Mgmt

DATA PROTOCOL

TCP/IP

Fixed
* Schemas
* Protocols
* Cfg Options
Re-think Identity APIs

Application View Logic

Application Control Logic

Data Model / Beans

Cfg Mgmt  Cxn Mgmt

Requirements?
* Schemas
* Operations
* Constraints

DATA PROTOCOL

TCP/IP
Re-think Identity APIs

ArisID Provider

Application View/Control Logic
ArisID Beans / Data Model
ArisID API

Authorization / Audit
Mapping
Routing & Discovery
Protocol Adap
Protocol Adap

DATA PROTOCOLS
TCP/IP

CARML Requirements
* Schemas
* Operations
* Constraints
OVD Provider for ArisID
How does IGF work in practice?
| Assurance       | What quality is the data being transferred?  
|                | What NIST Level?                  |
| Liberty IAF    |                               |
| PCI            |                               |
| Audit Standards? |                             |

| Governance     | Why should information be transferred, collected, or updated?  
|                | Who gets to do what?  
|                | Where will the be used or held?                  |
| Liberty IGF (CARML) |                       |
| XACML (AAPML) |                                               |
| WS-Policy |                                               |
| Privacy Legislation |                             |

| Protocol       | How should information be exchanged?  
|                | Which security mechanisms?  
|                | What transactions?                  |
| LDAP           |                               |
| SAML2, ID-WSF  |                               |
| WS-Trust / WS-Policy |                         |
Demonstration
Basic Authentication (or Form or SAML or Cardspace)
JSP Execution

JSP Retrieves and Displays Authenticated User Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principal Id</td>
<td>cn=Phil Hunt,dc=YourCompany,dc=com</td>
</tr>
<tr>
<td>mail</td>
<td><a href="mailto:phil.hunt@oracle.com">phil.hunt@oracle.com</a></td>
</tr>
<tr>
<td>description</td>
<td>This is a description</td>
</tr>
<tr>
<td>givenname</td>
<td>Phil</td>
</tr>
<tr>
<td>surname</td>
<td>Hunt</td>
</tr>
</tbody>
</table>
What is going on?
Two Active ArisID Clients

1. Container security authentication
   - Authenticates user according to policy
   - Container security uses ArisID

2. JSP
   - Uses session credential as key
   - Looks up application related attributes
   - Pretty prints found data
Protected Servlets, JSPs, and static content

JAAS Realm

ArisIDLoginModule

CARML.xml

ArisID API
JAAS ArisIDLogin Module is an IGF Client.

Below: OVD server virtualizes it’s data to support JAAS

```
1@IGF Ovd Stack Mapper Config for: IGF.JAAS.AttributeServiceImplModule Wed Jun 04 12:33:09 PDT 2008
2#Wed Jun 04 12:33:09 PDT 2008
3carml.role.mapattribute-description
4search.base=dc\YourCompany,dc=com
5carml.attribute.mail-mail.com.octetstring.vde.syntax.IA5String!org.openliberty.igf.stack.ovid.mapper.SimpleAttributeMapper
6carml.interaction.qc.Authenticate/inetorgperson
7carml.app.passwordAttributes=pwd
8default.rdn=sn
10```

LIBERTY ALLIANCE PROJECT
JSP Execution

ArisID API

showInfoAttrSvc.jsp

CARML.xml
JSP Script To Show User Information

JSP initializes using external CARML document.
    <DataDefs>
        <Attributes>
            <Attribute Name="mail" Cardinality="single" DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name" Description="The email address of the user">
            </Attribute>
            <Attribute Name="userpassword" Cardinality="single" DataType="http://www.w3.org/2001/XMLSchema#string" Description="Password used for login">
            </Attribute>
            <Attribute Name="description" Cardinality="single" DataType="http://www.w3.org/2001/XMLSchema#string" Description="Any descriptive text about the user">
            </Attribute>
            <Attribute Name="givenname" Cardinality="single" DataType="http://www.w3.org/2001/XMLSchema#string" Description="Given name and any middle names">
            </Attribute>
            <Attribute Name="surname" Cardinality="single" DataType="http://www.w3.org/2001/XMLSchema#string" Description="Surname or Family name">
            </Attribute>
        </Attributes>
        <Predicates/>
        <Roles/>
        <Policies/>
    </DataDefs>
    <ReadInteraction Description="Retrieve user profile for demo" Name="getUserProfile">
        <AttributeRef Optional="false" Ref="mail"/>
        <AttributeRef Optional="false" Ref="description"/>
        <AttributeRef Optional="false" Ref="givenname"/>
        <AttributeRef Optional="false" Ref="surname"/>
    </ReadInteraction>
</ClientAttrReq>
OVD Mapping of CARML Declaration

IGF Ovd Stack Mapper Config For: Tomcat.IGF.Demo/1.0 Thu May 15 19:21:38 PDT 2008

3
carml.attribute.mail=mail.com.oclctstring.vde.syntax.IA5String|org.openliberty.igf.stack.ovd.mapper.SimpleAttributeMapper
4
carml.app.passwordAttributes=
5
carml.interaction.ac.getProfileUserProfile/inetorgperson
6
search.base=dc=YourCompany,dc=com
7
carml.role.mapattribute=description
8
9
10
11
default.rdn-cn
13
Look-up authenticated user information

User Context / Session Info

Definition of getUser

```html
<ReadInteraction Description="Retrieve user profile for demo" Name="getUserProfile">
  <AttributeRef Optional="false" Ref="mail"/>
  <AttributeRef Optional="false" Ref="description"/>
  <AttributeRef Optional="false" Ref="givenName"/>
  <AttributeRef Optional="false" Ref="surname"/>
</ReadInteraction>
```
<table>
<thead>
<tr>
<th>Principal Id</th>
<th>%userid%</th>
</tr>
</thead>
</table>

```java
while (iter.hasNext()) {
    AttributeValue val = iter.next();
    String name = val.getNameIdRef();
    
    String value = null;
    if (val.isError())
        value = "<undefined or unavailable>";
    else
        value = val.get(0);

    %name%
    %value%
} 
```
ArisID Summary

- Standards
  - CARML - Data and transaction definitions
  - WS-Policy - Privacy assertions
  - AAPML - Attribute Authority Policy
  - Protocol Profiles - How IGF is Applied to Protocols
- Future
  - Work on federation protocols
  - Development of open source provider
  - IDE Tooling
Web


ArisID Providers:


Inquiries to

- phil.hunt@oracle.com
- prateek.mishra@oracle.com

Blogs:

- [http://independentid.com](http://independentid.com) - Phil
- [http://blogs.oracle.com/identityprivacy](http://blogs.oracle.com/identityprivacy) - Prateek