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

OpenLiberty Webcast

Dec 11, 2008

Phil Hunt, Oracle

phil.hunt@oracle.com

OpenLiberty.org

- 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*).

Project Objectives

- 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

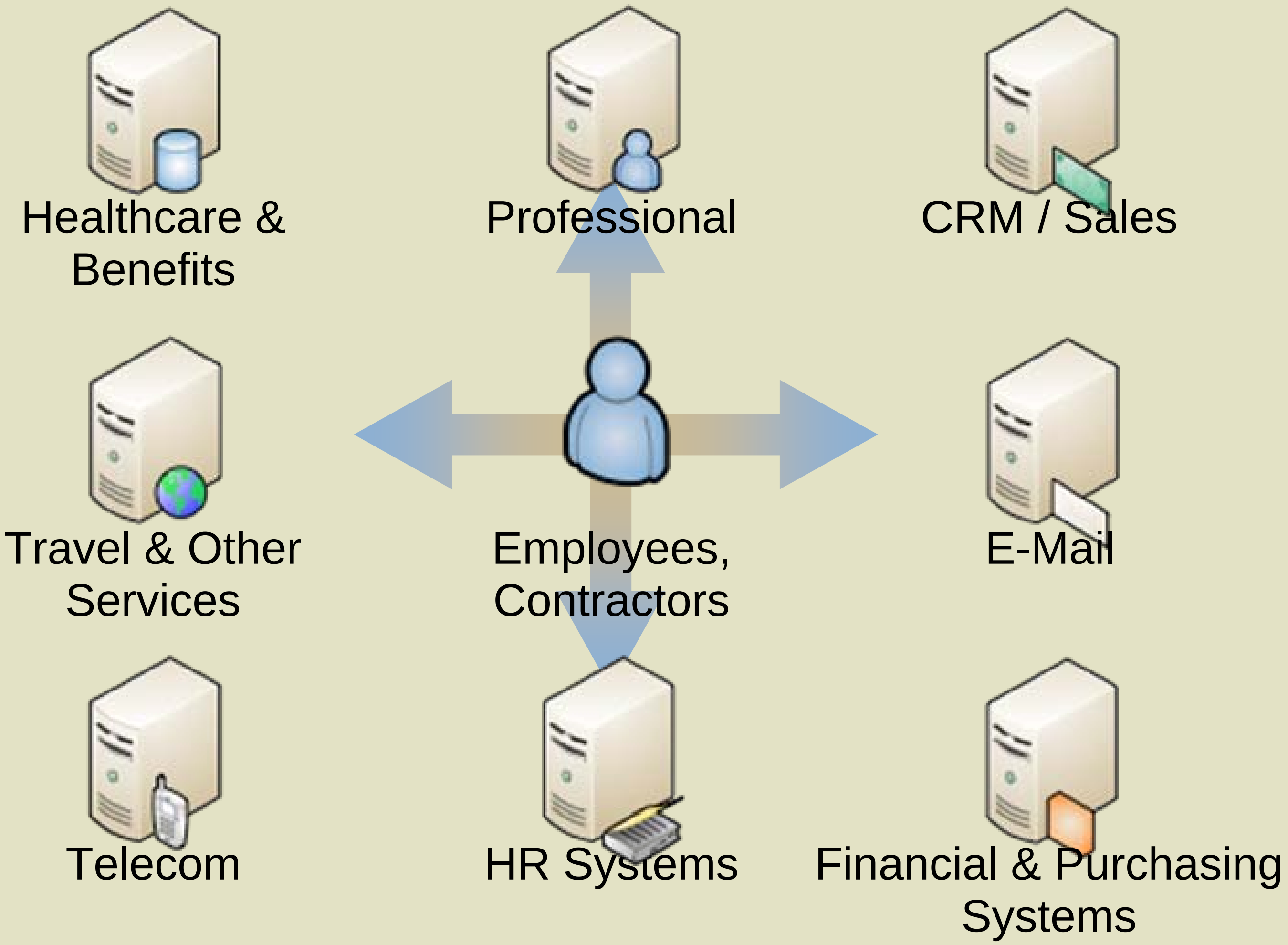
Current Practice

- 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

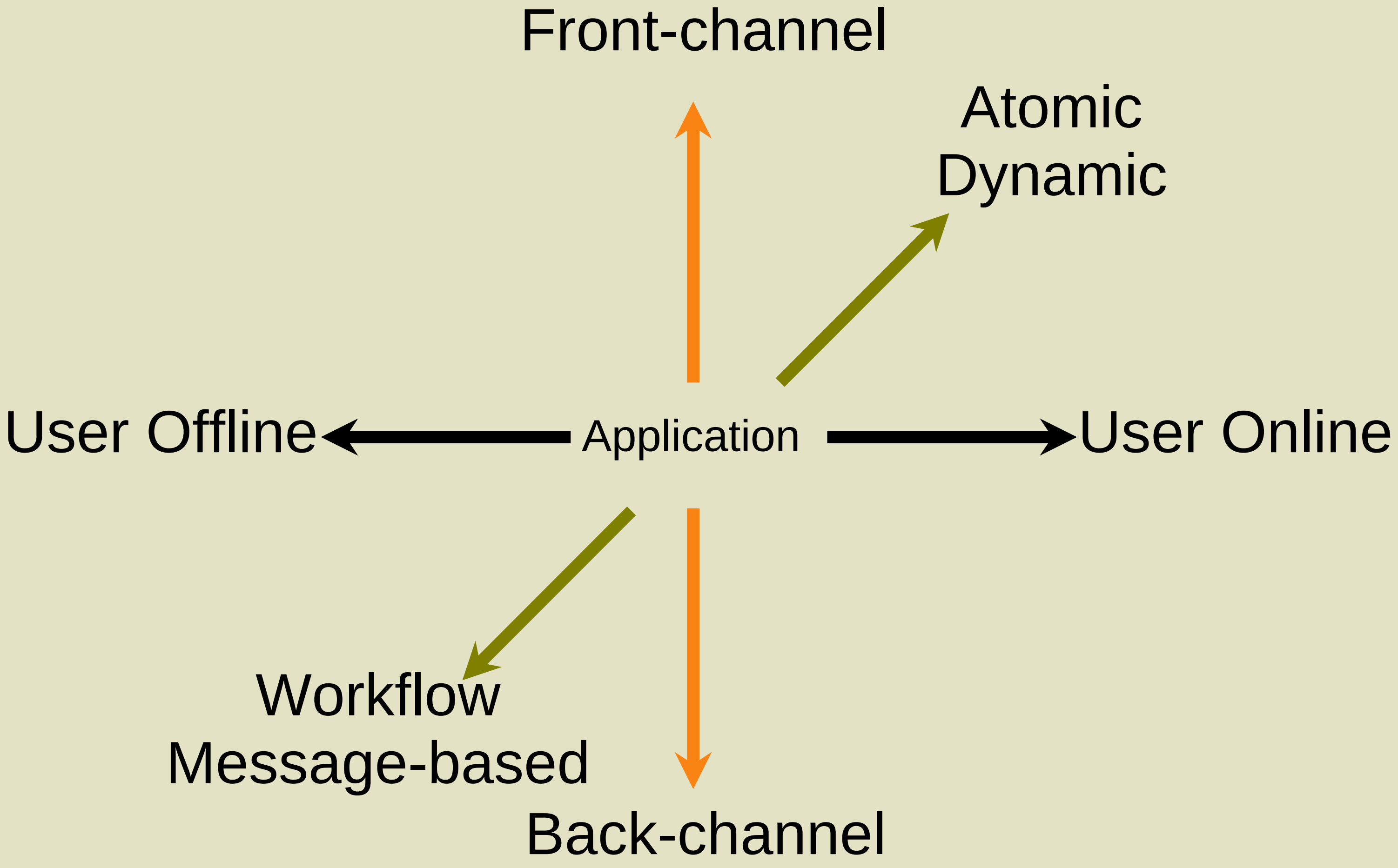
Many Identity Sources



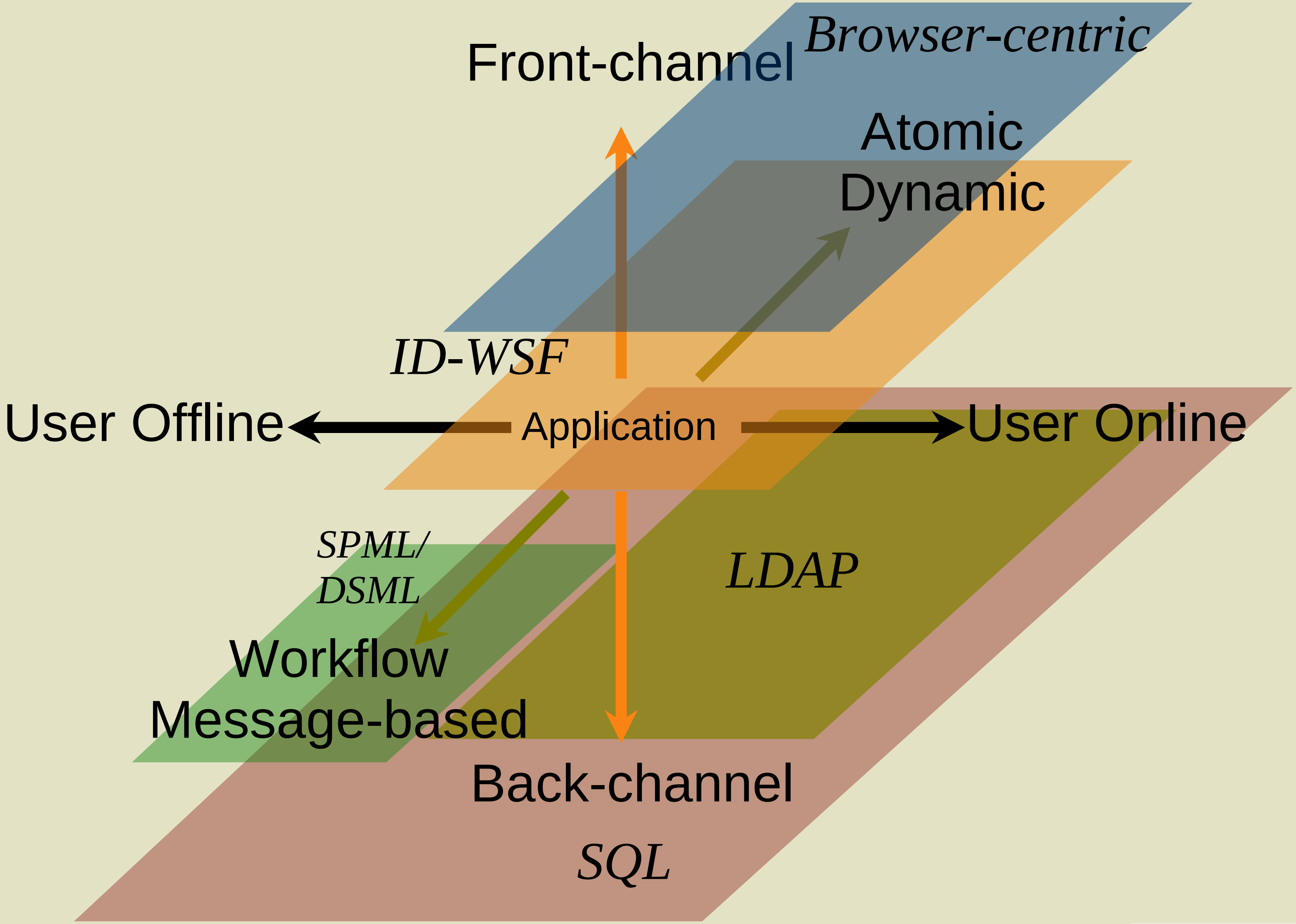
Trends

- 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

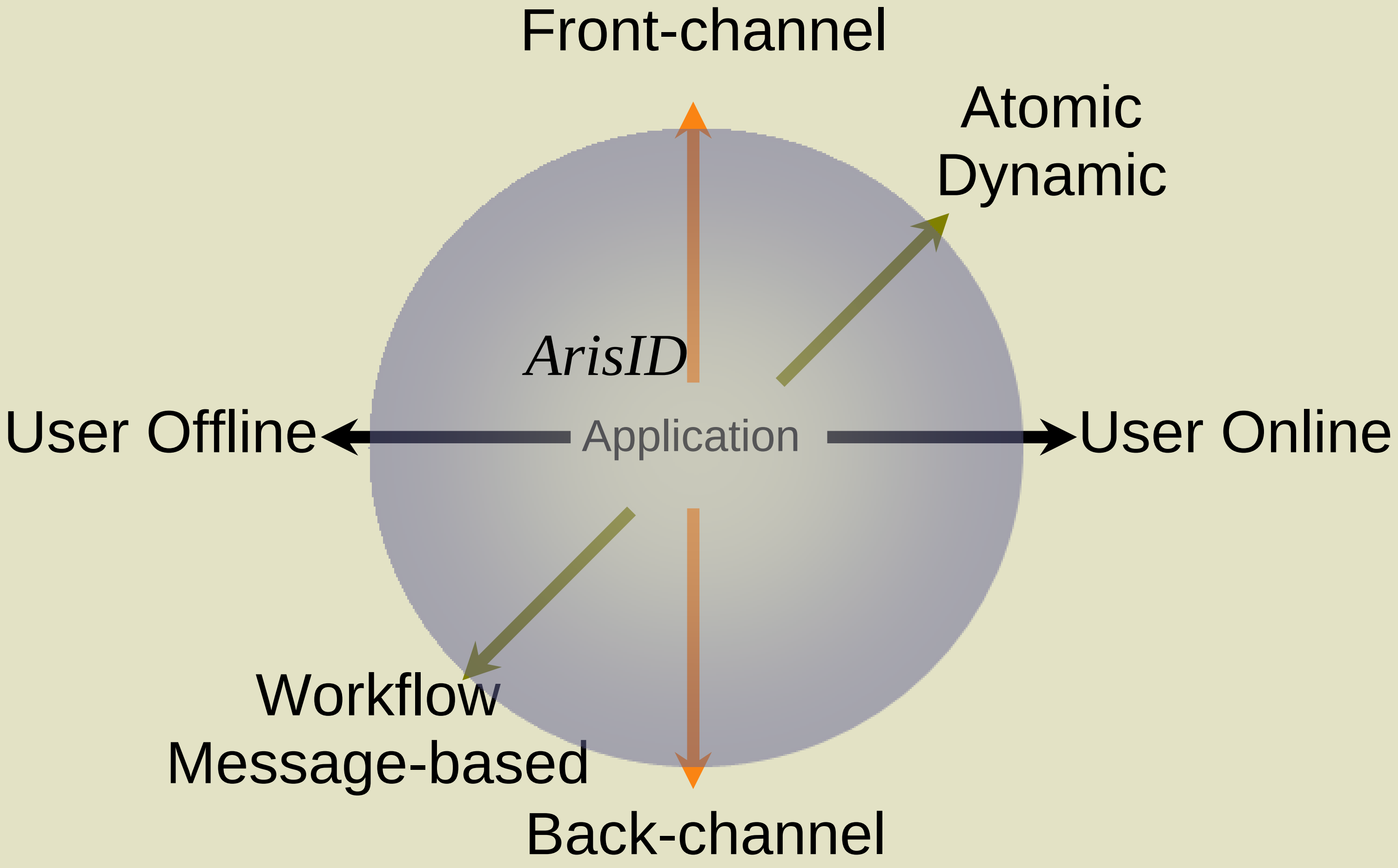
Modes of Identity



Modes of Identity



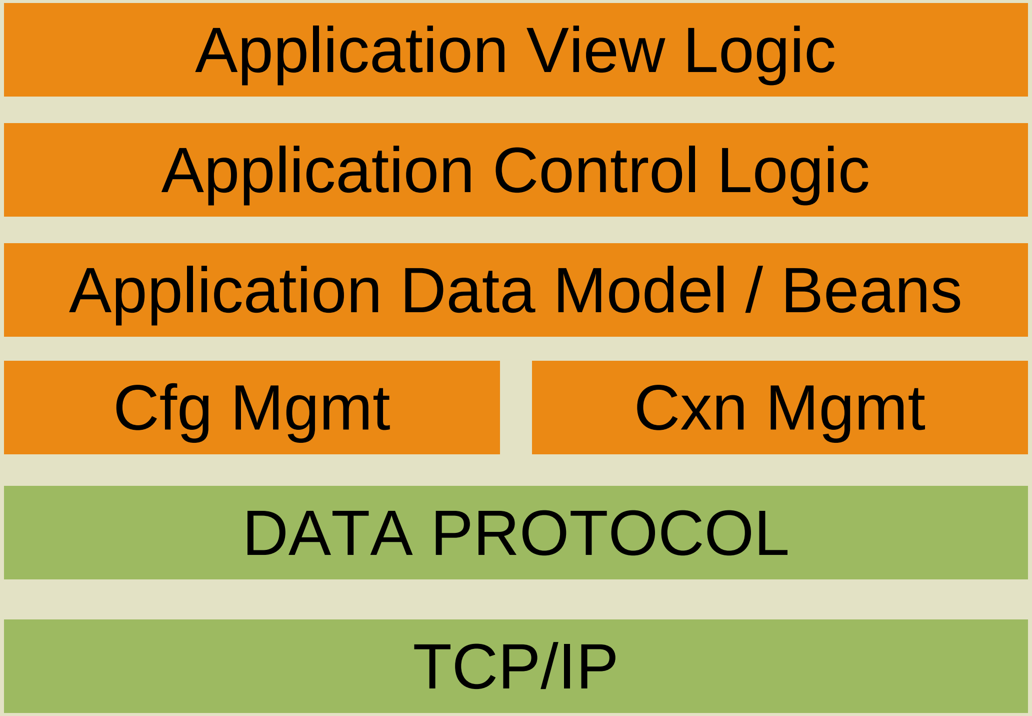
Modes of Identity



What is De-coupling

- “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

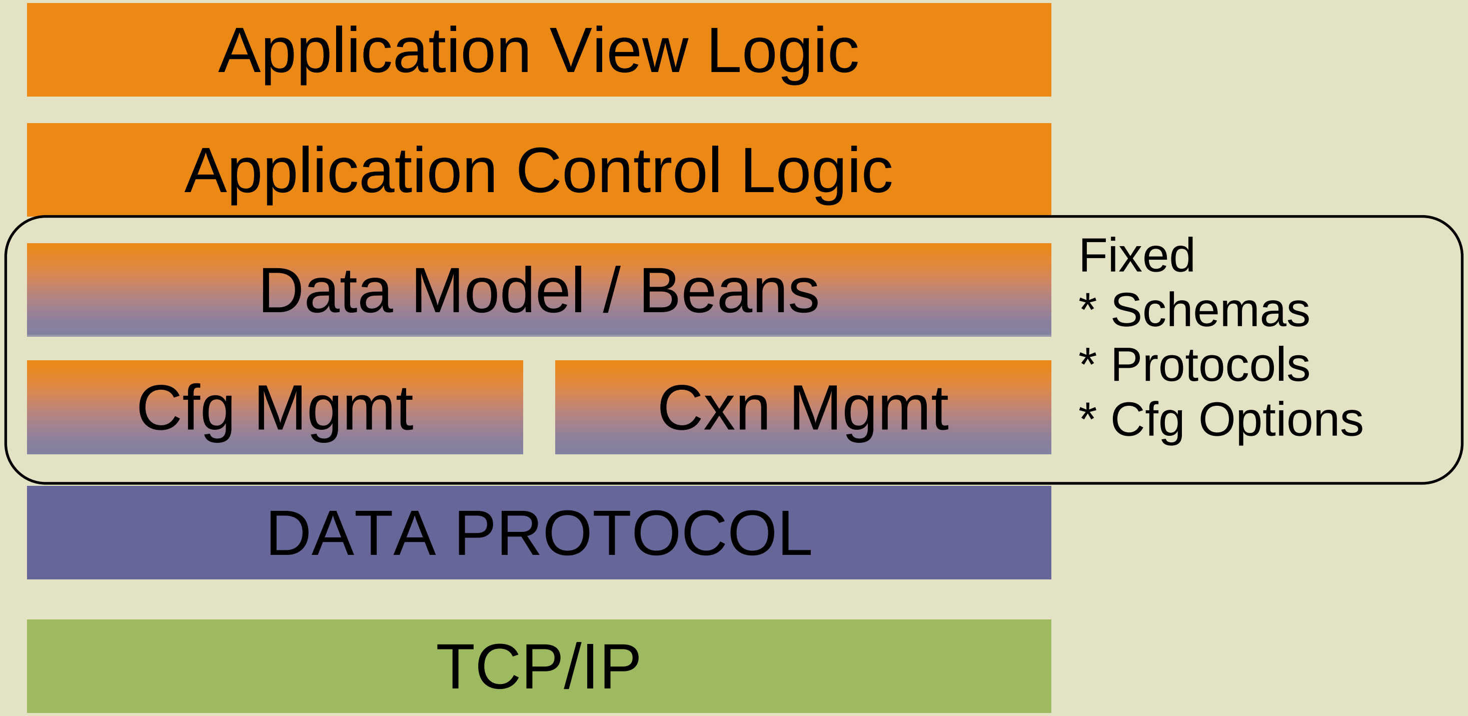
Cfg Mgmt

Cxn Mgmt

DATA PROTOCOL

TCP/IP

Inflexible Applications



Application View Logic

Application Control Logic

Data Model / Beans

Cfg Mgmt

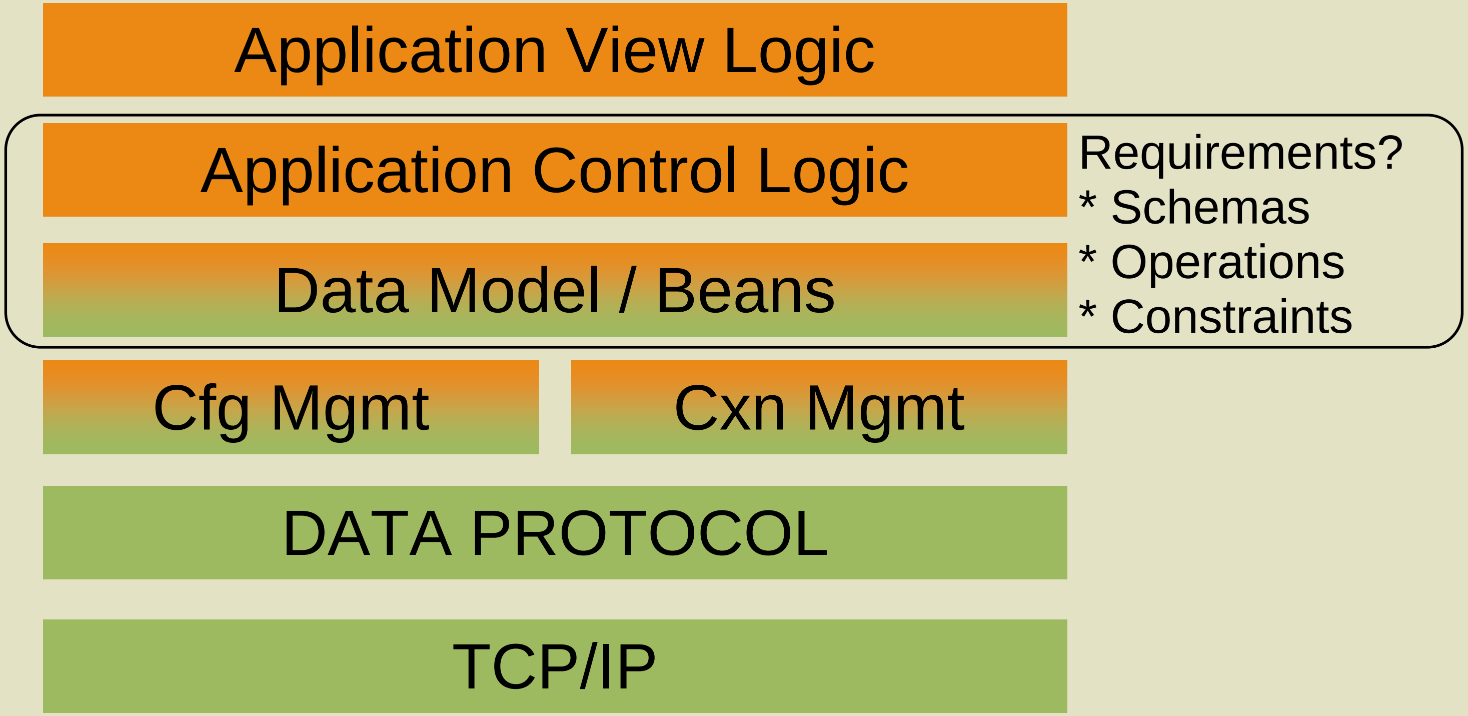
Cxn Mgmt

Fixed
* Schemas
* Protocols
* Cfg Options

DATA PROTOCOL

TCP/IP

Re-think Identity APIs



Application View Logic

Application Control Logic

Data Model / Beans

Requirements?
* Schemas
* Operations
* Constraints

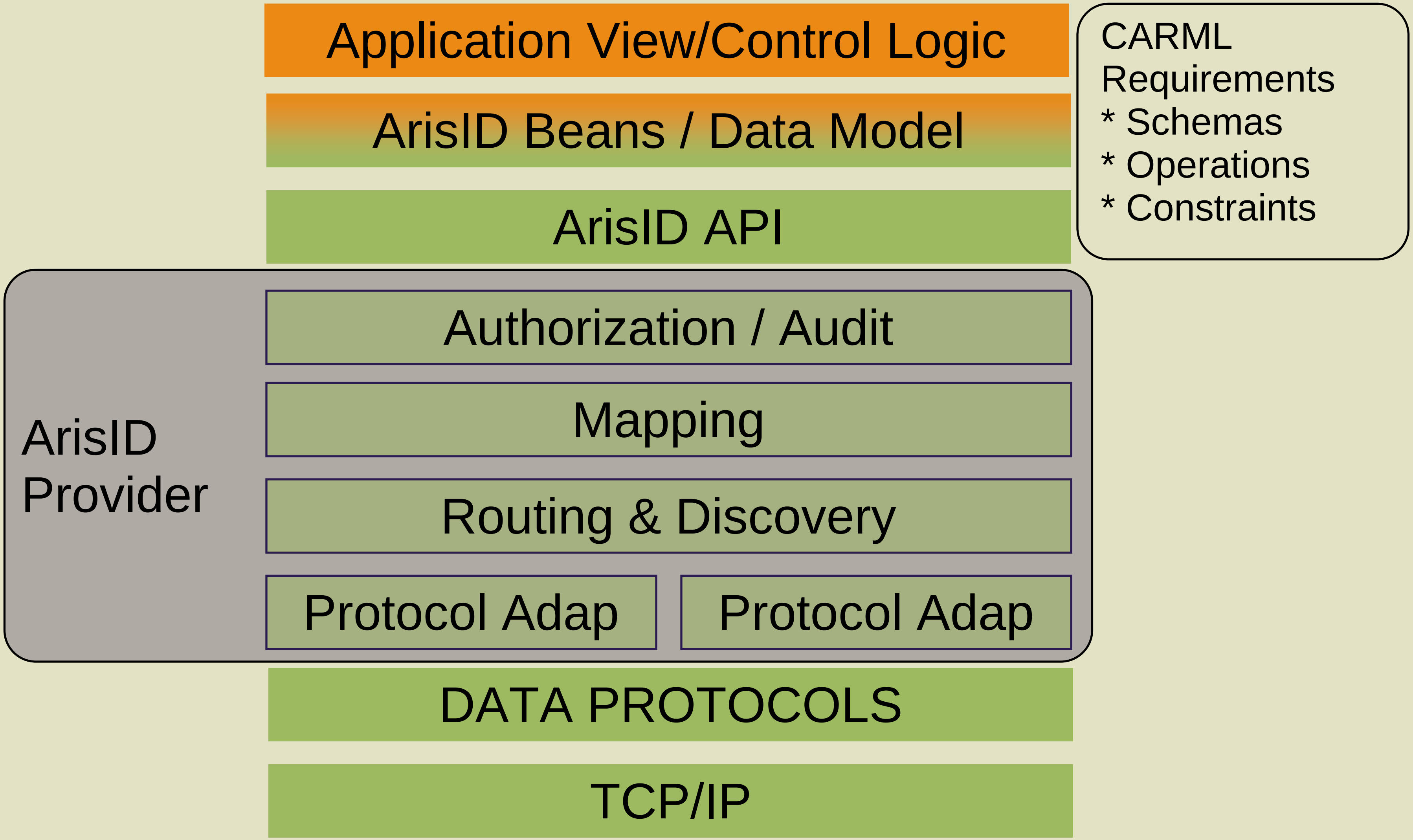
Cfg Mgmt

Cxn Mgmt

DATA PROTOCOL

TCP/IP

Re-think Identity APIs



Application View/Control Logic

ArisID Beans / Data Model

ArisID API

ArisID Provider

Authorization / Audit

Mapping

Routing & Discovery

Protocol Adap

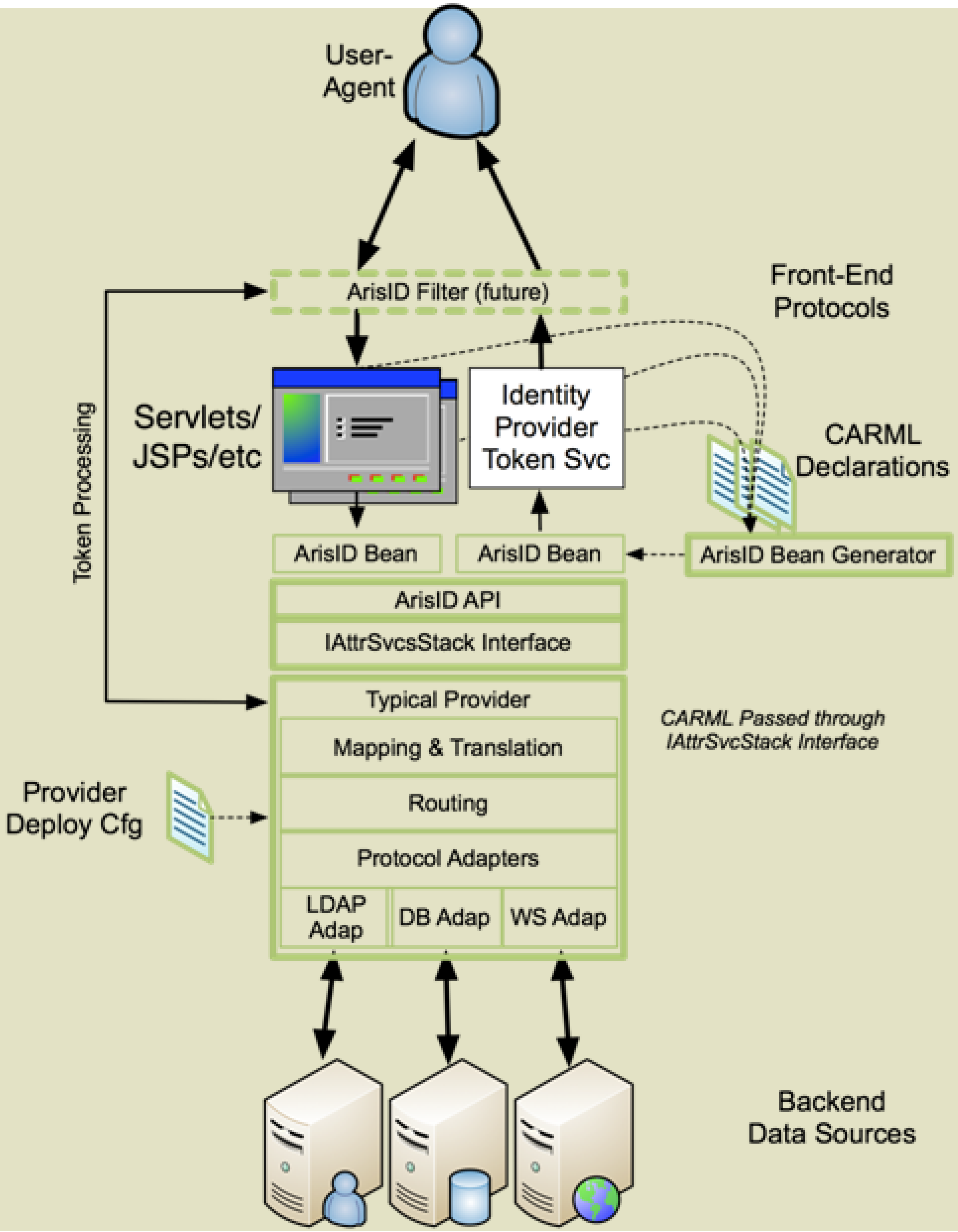
Protocol Adap

DATA PROTOCOLS

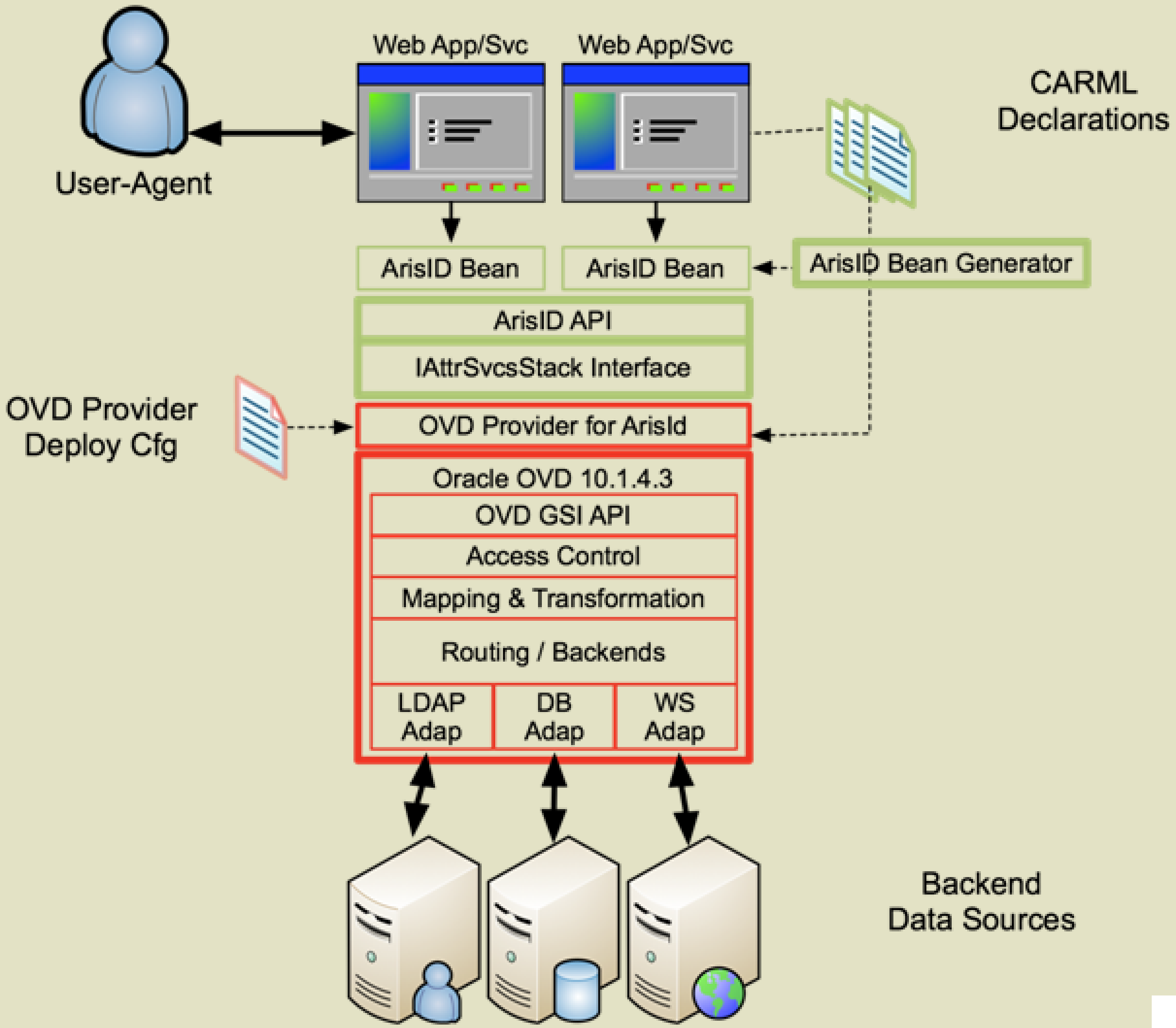
TCP/IP

CARML Requirements
* Schemas
* Operations
* Constraints

ArisID Architecture

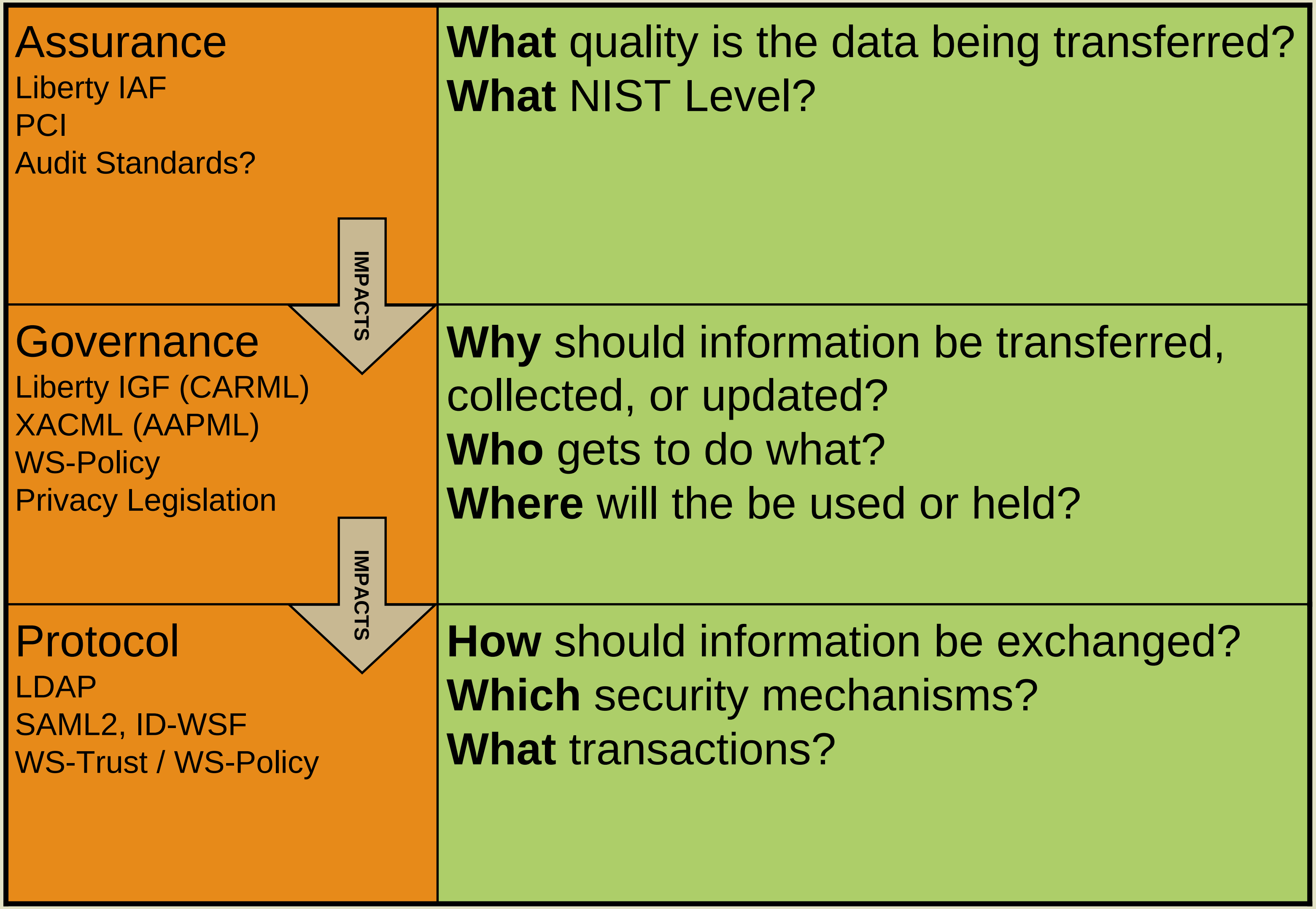


OVD Provider for ArisID



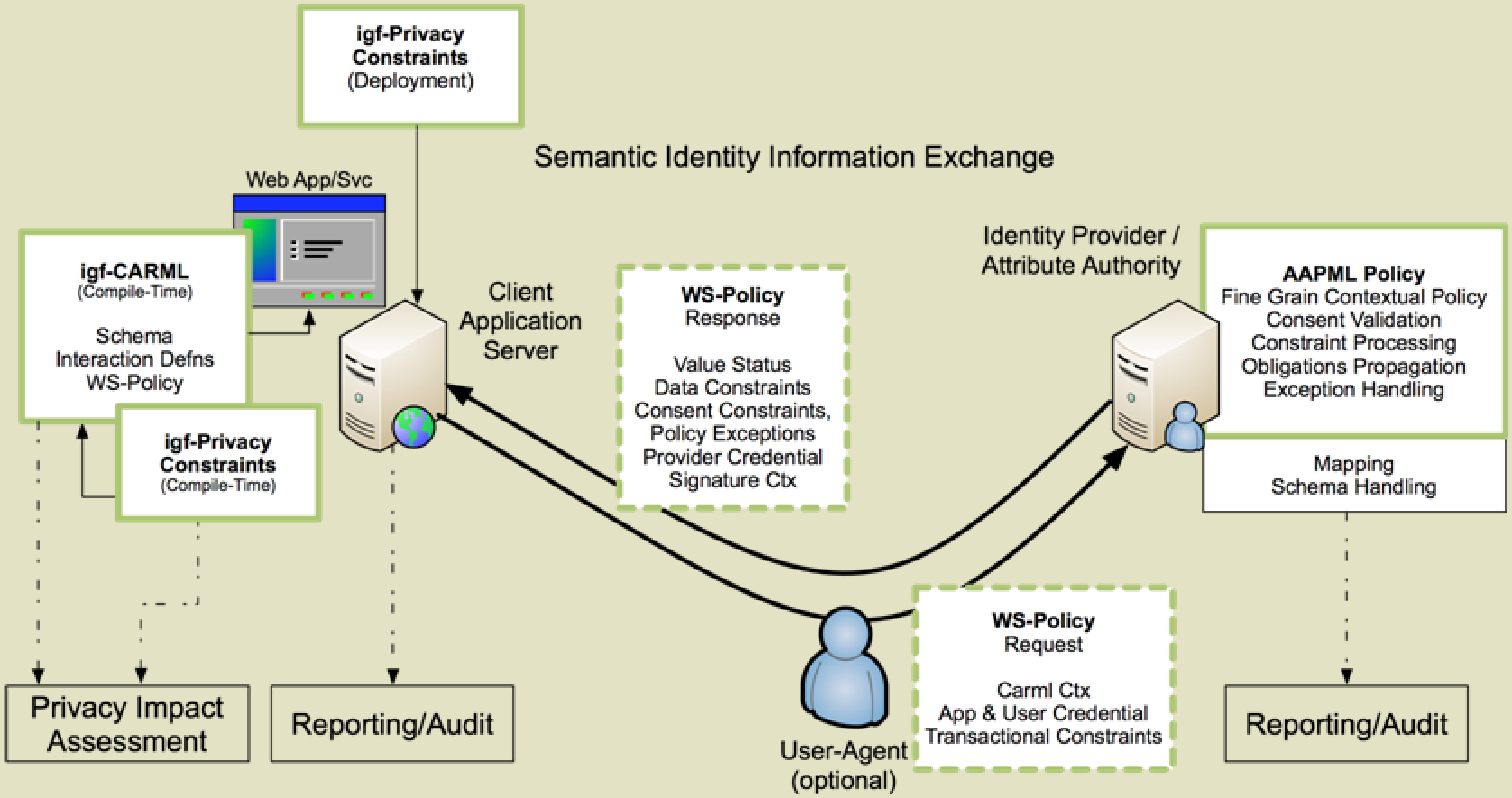
- How does IGF work in practice?

Assurance, Governance and Run-Time Protocols



Assurance Liberty IAF PCI Audit Standards?	**What** quality is the data being transferred? **What** NIST Level?
Governance Liberty IGF (CARML) XACML (AAPML) WS-Policy Privacy Legislation	**Why** should information be transferred, collected, or updated? **Who** gets to do what? **Where** will the be used or held?
Protocol LDAP SAML2, ID-WSF WS-Trust / WS-Policy	**How** should information be exchanged? **Which** security mechanisms? **What** transactions?

IGF Interactions



igf-Privacy Constraints (Deployment)

Semantic Identity Information Exchange

Web App/Svc

igf-CARML (Compile-Time)

Schema
Interaction Defns
WS-Policy

igf-Privacy Constraints (Compile-Time)

Client Application Server

WS-Policy
Response

Value Status
Data Constraints
Consent Constraints,
Policy Exceptions
Provider Credential
Signature Ctx

Identity Provider / Attribute Authority

AAPML Policy
Fine Grain Contextual Policy
Consent Validation
Constraint Processing
Obligations Propagation
Exception Handling

Mapping
Schema Handling

WS-Policy
Request

Carml Ctx
App & User Credential
Transactional Constraints

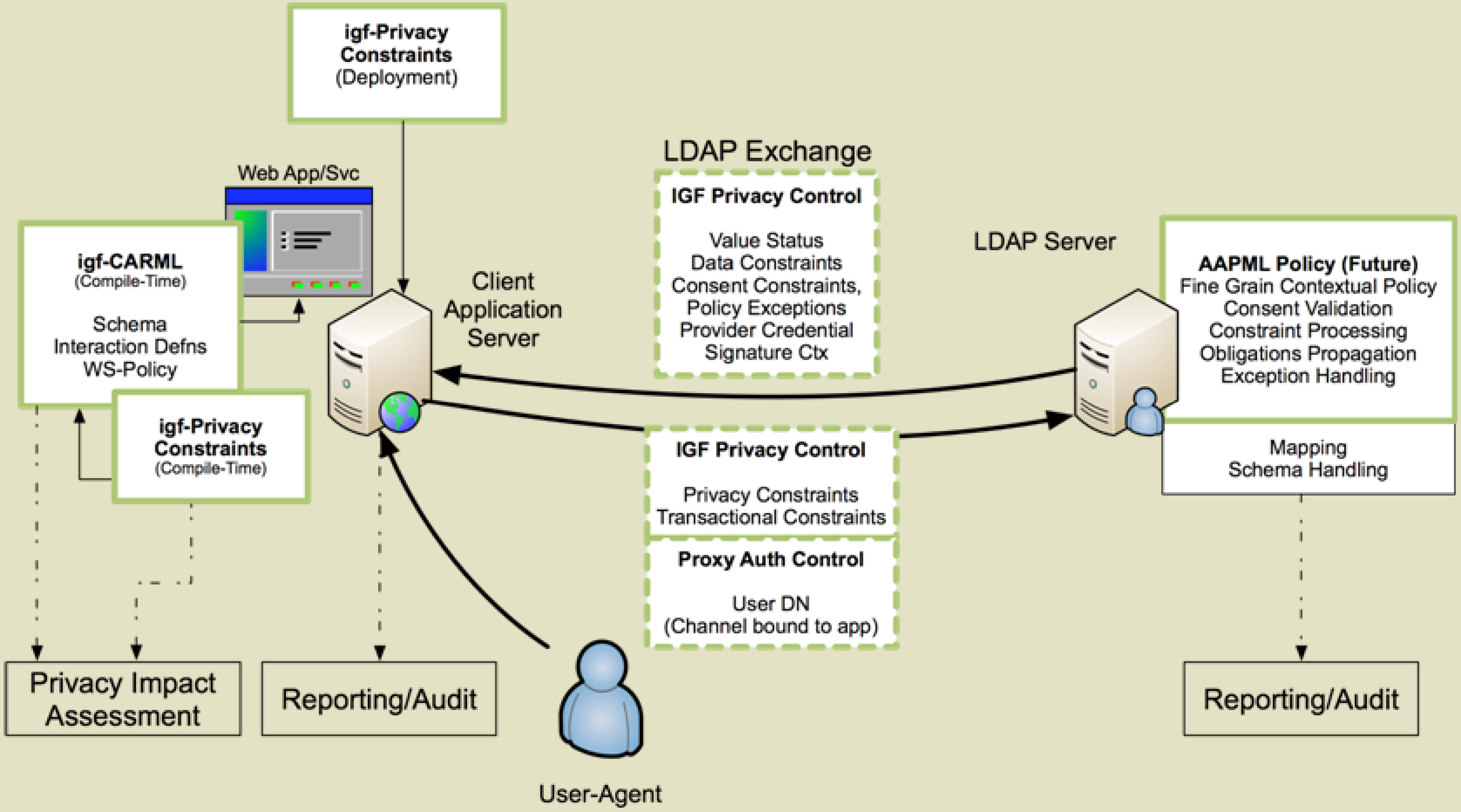
User-Agent (optional)

Privacy Impact Assessment

Reporting/Audit

Reporting/Audit

IGF and LDAP



igf-Privacy Constraints (Deployment)

Web App/Svc

igf-CARML (Compile-Time)

Schema
Interaction Defns
WS-Policy

igf-Privacy Constraints (Compile-Time)

Client Application Server

LDAP Exchange

IGF Privacy Control

Value Status
Data Constraints
Consent Constraints,
Policy Exceptions
Provider Credential
Signature Ctx

LDAP Server

AAPML Policy (Future)
Fine Grain Contextual Policy
Consent Validation
Constraint Processing
Obligations Propagation
Exception Handling

Mapping
Schema Handling

IGF Privacy Control

Privacy Constraints
Transactional Constraints

Proxy Auth Control

User DN
(Channel bound to app)

Privacy Impact Assessment

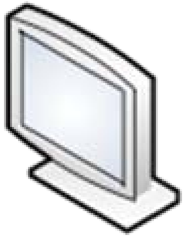
Reporting/Audit

User-Agent

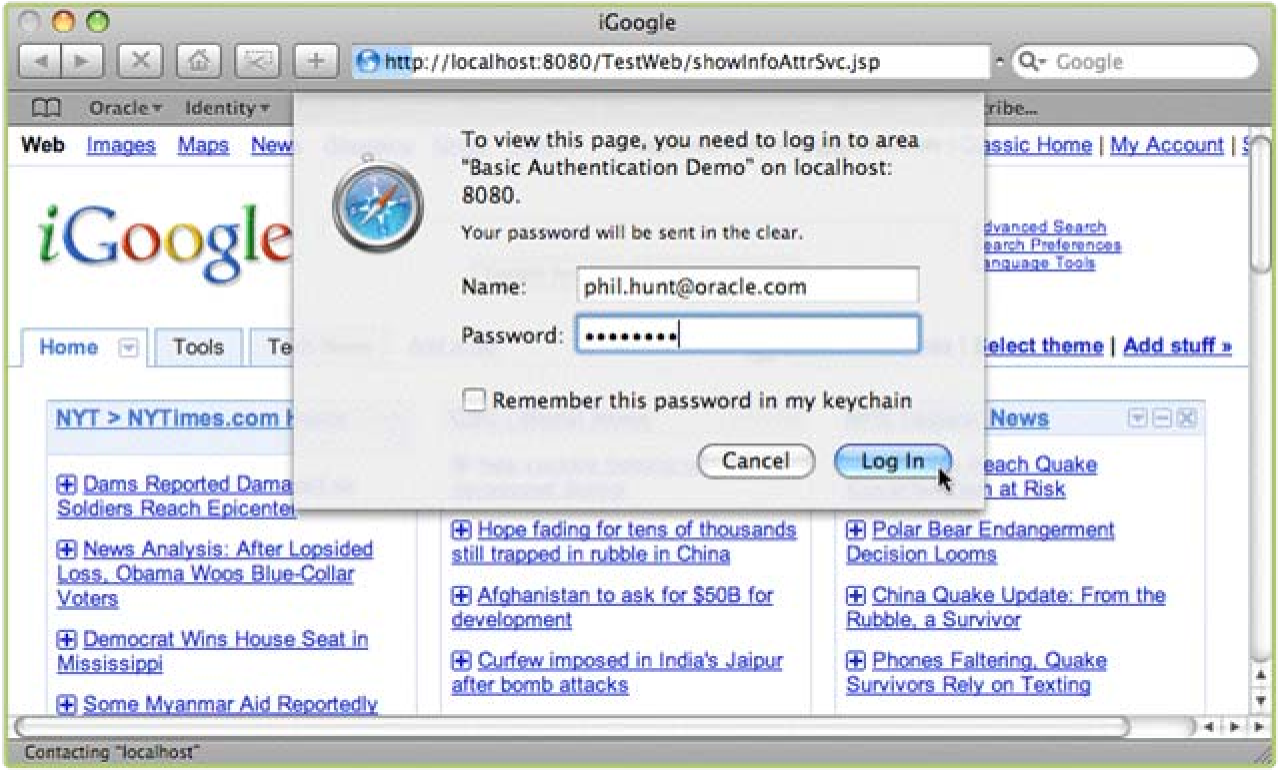
Reporting/Audit

- Demonstration

Container Triggered Authentication



Basic Authentication
(or Form or SAML
or Cardspace)



iGoogle

http://localhost:8080/TestWeb/showInfoAttrSvc.jsp

To view this page, you need to log in to area "Basic Authentication Demo" on localhost: 8080.

Your password will be sent in the clear.

Name: phil.hunt@oracle.com

Password: ••••••••

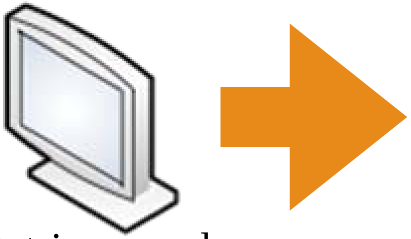
□ Remember this password in my keychain

Cancel | Log In

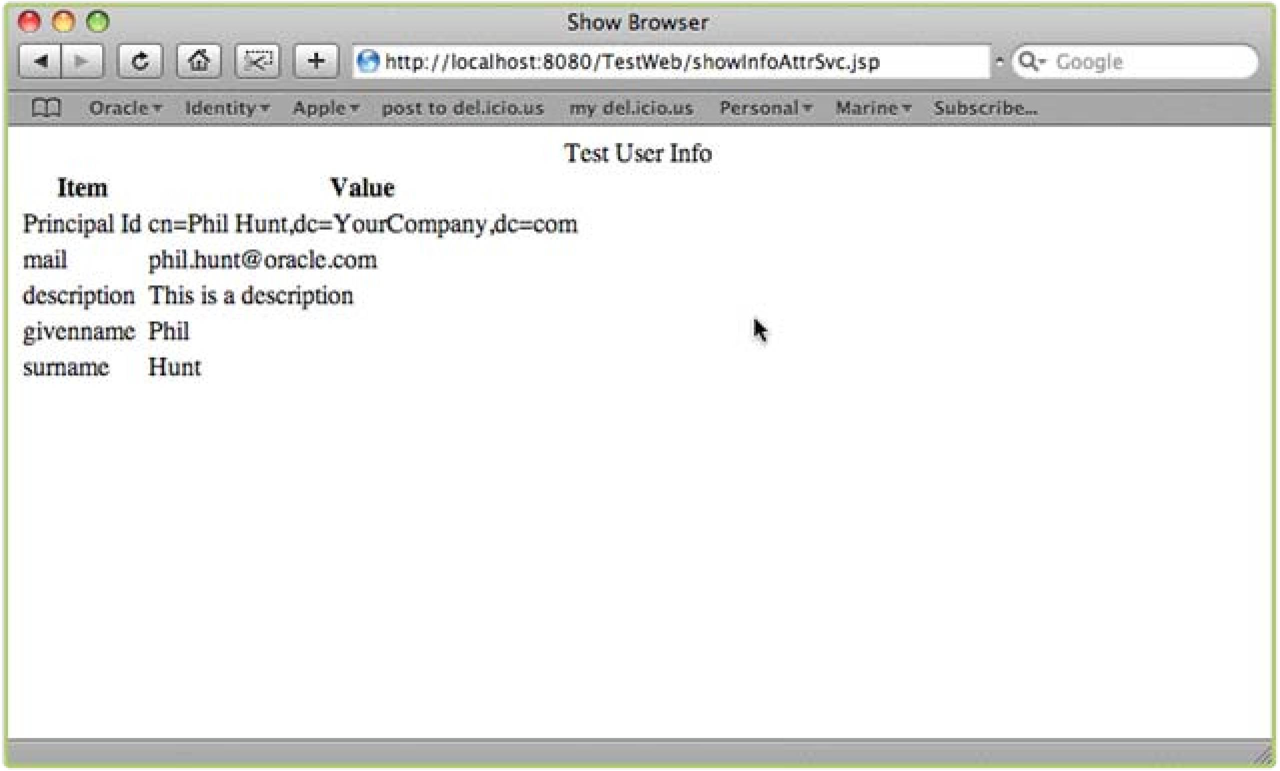
Contacting "localhost"

Oracle
Identity
Web
Images
Maps
New
Classic Home | My Account
Advanced Search
Search Preferences
Language Tools
Home
Tools
Select theme | Add stuff »
NYT > NYTimes.com
News
Dams Reported Dama... Soldiers Reach Epicente...
News Analysis: After Lopsided Loss, Obama Woos Blue-Collar Voters
Democrat Wins House Seat in Mississippi
Some Myanmar Aid Reportedly
Hope fading for tens of thousands still trapped in rubble in China
Afghanistan to ask for $50B for development
Curfew imposed in India's Jaipur after bomb attacks
...each Quake ...at Risk
Polar Bear Endangerment Decision Looms
China Quake Update: From the Rubble, a Survivor
Phones Faltering, Quake Survivors Rely on Texting
Google

JSP Execution



JSP Retrieves and Displays Authenticated User Information



Test User Info

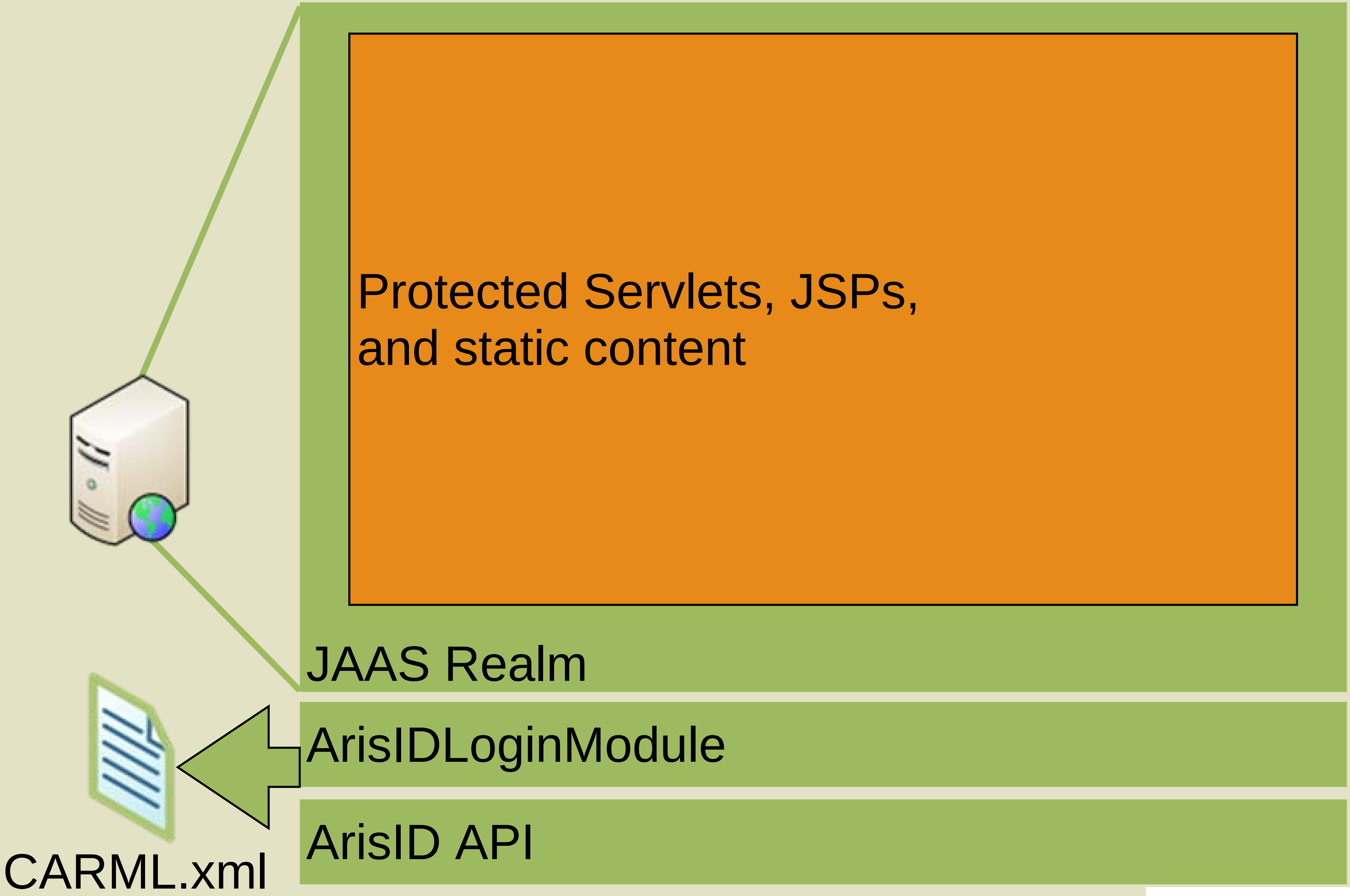
Item	Value
Principal Id	cn=Phil Hunt,dc=YourCompany,dc=com
mail	phil.hunt@oracle.com
description	This is a description
givenname	Phil
surname	Hunt

- 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

Container Security


Protected Servlets, JSPs, and static content

JAAS Realm

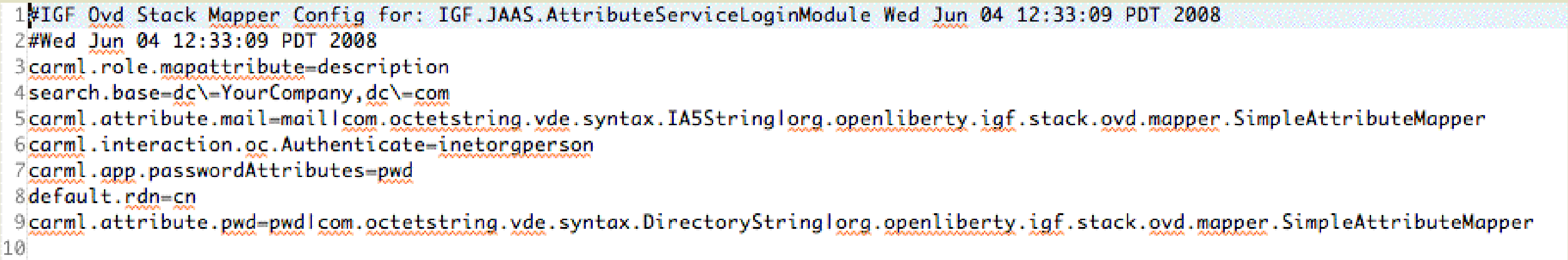
ArisIDLoginModule

ArisID API

CARML.xml

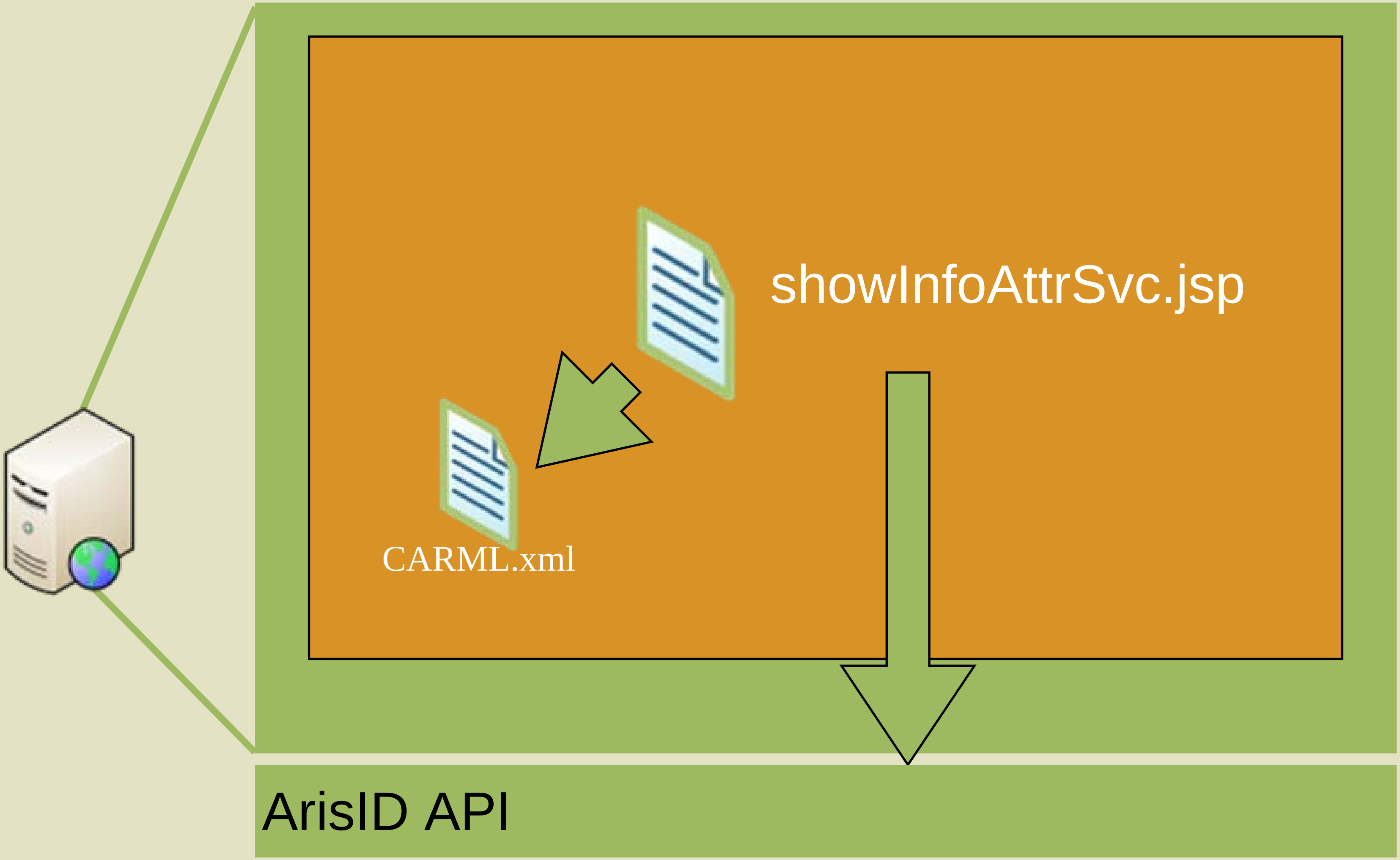
- JAAS ArisIDLogin Module is an IGF Client.

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



```
#IGF Ovd Stack Mapper Config for: IGF.JAAS.AttributeServiceLoginModule Wed Jun 04 12:33:09 PDT 2008
#Wed Jun 04 12:33:09 PDT 2008
carml.role.mapattribute=description
search.base=dc\=YourCompany,dc\=com
carml.attribute.mail=mail|com.octetstring.vde.syntax.IA5String|org.openliberty.igf.stack.ovd.mapper.SimpleAttributeMapper
carml.interaction.oc.Authenticate=inetorgperson
carml.app.passwordAttributes=pwd
default.rdn=cn
carml.attribute.pwd=pwd|com.octetstring.vde.syntax.DirectoryString|org.openliberty.igf.stack.ovd.mapper.SimpleAttributeMapper
```

JSP Execution

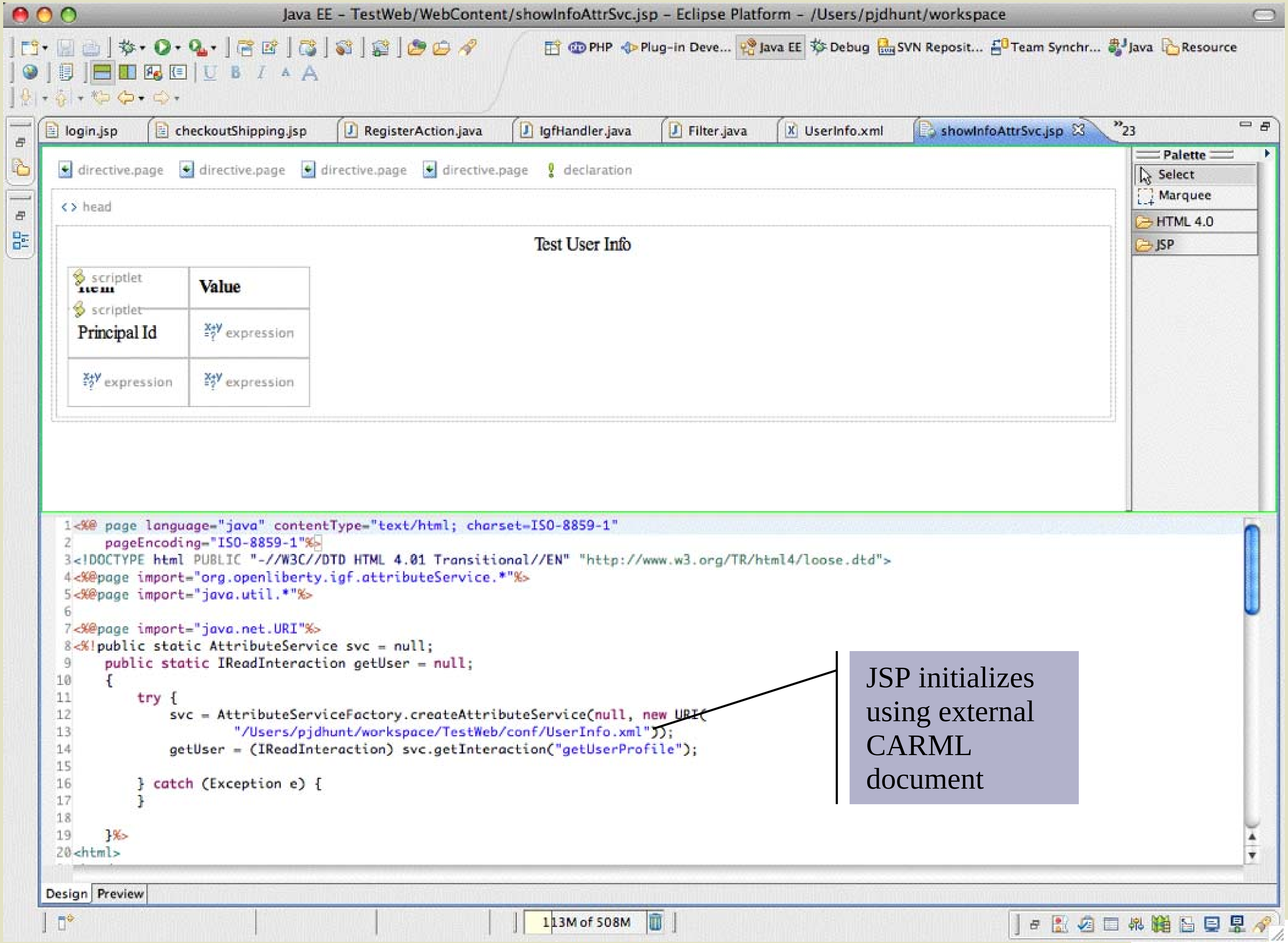


showInfoAttrSvc.jsp

CARML.xml

ArisID API

JSP Script To Show User Information



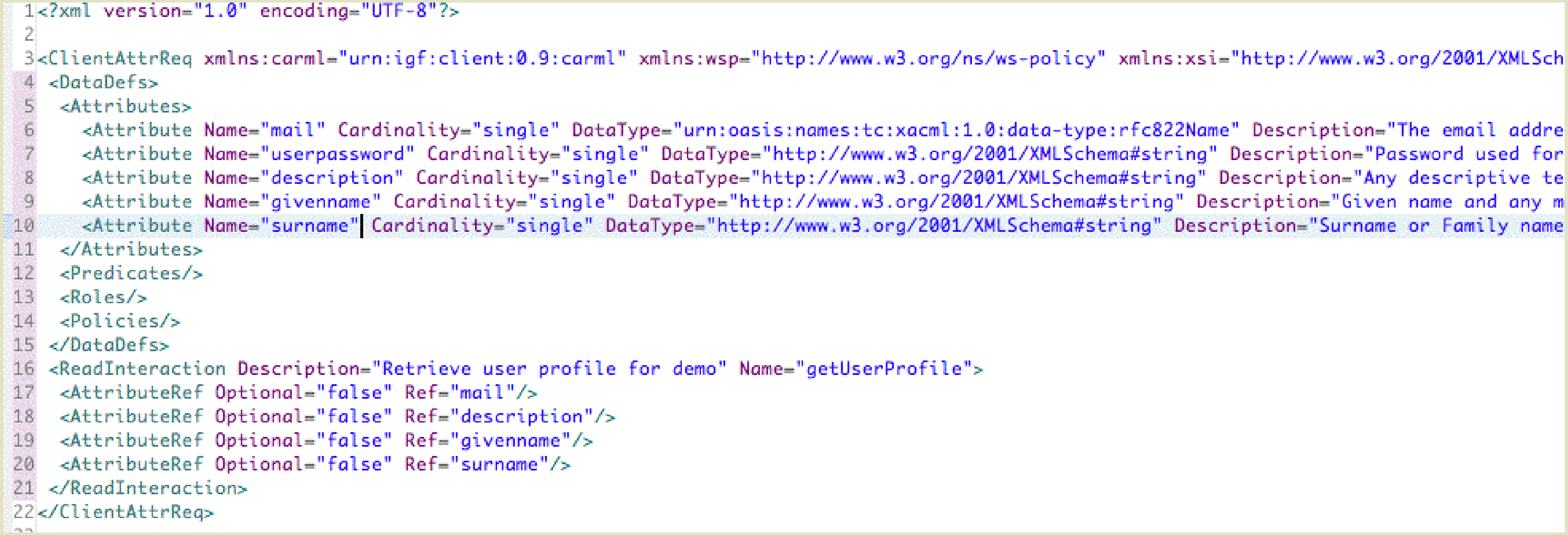
Test User Info

Item	Value
Principal Id	expression
expression	expression

```
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"
    pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<%@page import="org.openliberty.igf.attributeService.*"%>
<%@page import="java.util.*"%>

<%@page import="java.net.URI"%>
<%!public static AttributeService svc = null;
    public static IReadInteraction getUser = null;
    {
        try {
            svc = AttributeServiceFactory.createAttributeService(null, new URI(
                    "/Users/pjdhunt/workspace/TestWeb/conf/UserInfo.xml"));
            getUser = (IReadInteraction) svc.getInteraction("getUserProfile");

        } catch (Exception e) {
        }

    }%>
<html>
```

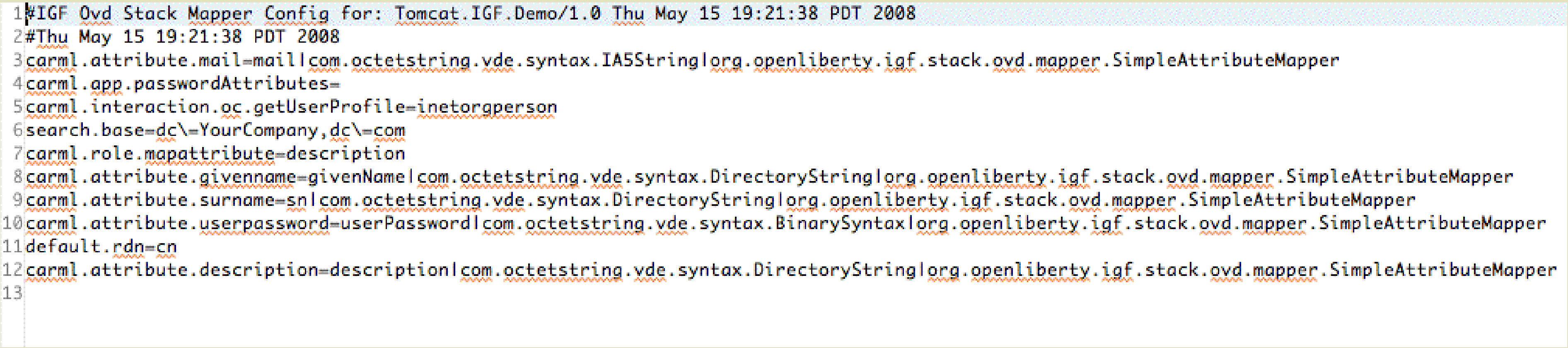
JSP initializes using external CARML document

CARML Declaration



```
<?xml version="1.0" encoding="UTF-8"?>

<ClientAttrReq xmlns:carml="urn:igf:client:0.9:carml" xmlns:wsp="http://www.w3.org/ns/ws-policy" xmlns:xsi="http://www.w3.org/2001/XMLSch
 <DataDefs>
  <Attributes>
    <Attribute Name="mail" Cardinality="single" DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name" Description="The email addre
    <Attribute Name="userpassword" Cardinality="single" DataType="http://www.w3.org/2001/XMLSchema#string" Description="Password used for
    <Attribute Name="description" Cardinality="single" DataType="http://www.w3.org/2001/XMLSchema#string" Description="Any descriptive te
    <Attribute Name="givenname" Cardinality="single" DataType="http://www.w3.org/2001/XMLSchema#string" Description="Given name and any m
    <Attribute Name="surname" Cardinality="single" DataType="http://www.w3.org/2001/XMLSchema#string" Description="Surname or Family name
  </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>
```

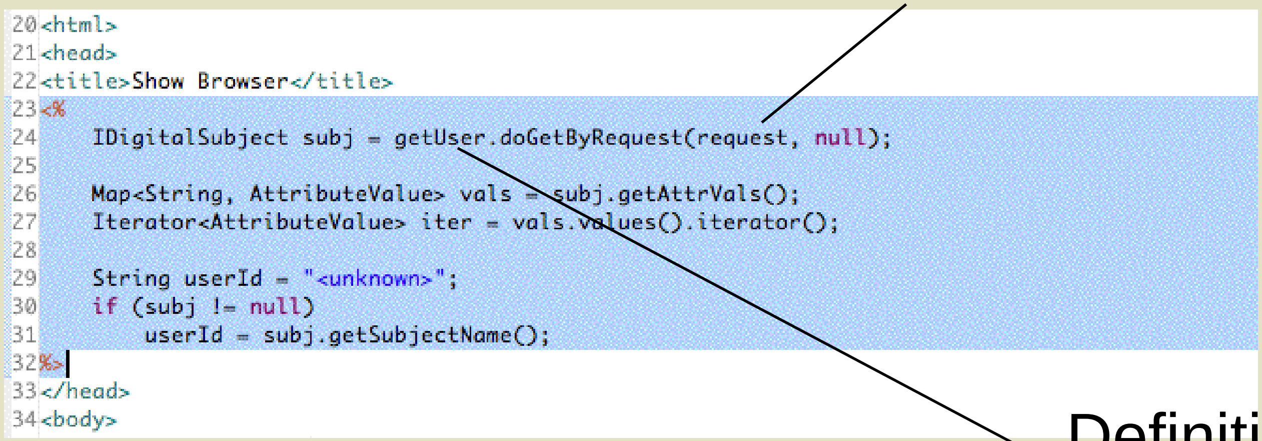
OVD Mapping of CARML Declaration



```
#IGF Ovd Stack Mapper Config for: Tomcat.IGF.Demo/1.0 Thu May 15 19:21:38 PDT 2008
#Thu May 15 19:21:38 PDT 2008
carml.attribute.mail=mail|com.octetstring.vde.syntax.IA5String|org.openliberty.igf.stack.ovd.mapper.SimpleAttributeMapper
carml.app.passwordAttributes=
carml.interaction.oc.getUserProfile=inetorgperson
search.base=dc\=YourCompany,dc\=com
carml.role.mapattribute=description
carml.attribute.givenname=givenName|com.octetstring.vde.syntax.DirectoryString|org.openliberty.igf.stack.ovd.mapper.SimpleAttributeMapper
carml.attribute.surname=sn|com.octetstring.vde.syntax.DirectoryString|org.openliberty.igf.stack.ovd.mapper.SimpleAttributeMapper
carml.attribute.userpassword=userPassword|com.octetstring.vde.syntax.BinarySyntax|org.openliberty.igf.stack.ovd.mapper.SimpleAttributeMapper
default.rdn=cn
carml.attribute.description=description|com.octetstring.vde.syntax.DirectoryString|org.openliberty.igf.stack.ovd.mapper.SimpleAttributeMapper
```

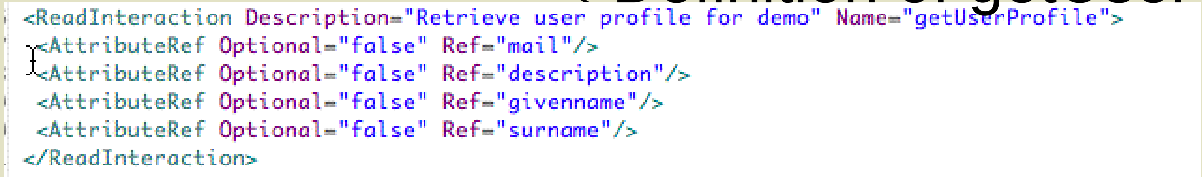
Look-up authenticated user information

User Context / Session Info



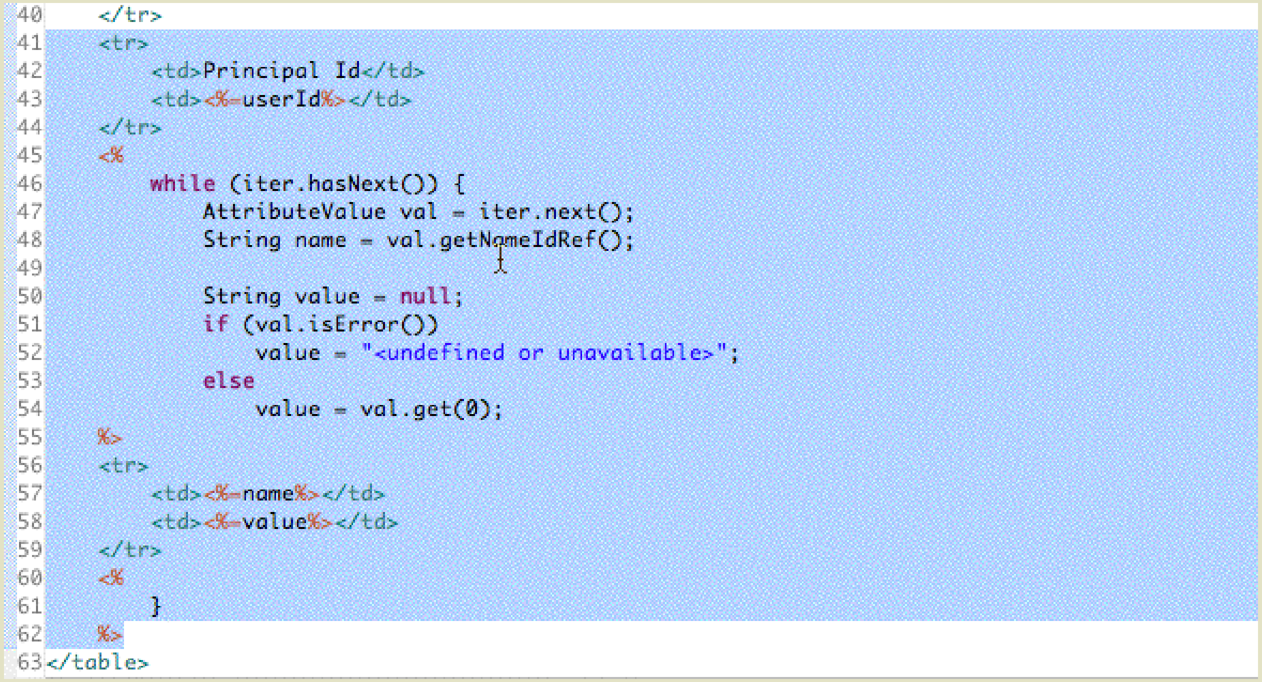
```
<html>
<head>
<title>Show Browser</title>
<%
    IDigitalSubject subj = getUser.doGetByRequest(request, null);

    Map<String, AttributeValue> vals = subj.getAttrVals();
    Iterator<AttributeValue> iter = vals.values().iterator();

    String userId = "<unknown>";
    if (subj != null)
        userId = subj.getSubjectName();
%>
</head>
<body>
```

Definition of getUser



```
<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>
```

Display retrieved information



```
    </tr>
    <tr>
        <td>Principal Id</td>
        <td><%=userId%></td>
    </tr>
    <%
        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);
    %>
    <tr>
        <td><%=name%></td>
        <td><%=value%></td>
    </tr>
    <%
        }
    %>
</table>
```

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

Learn More

- Web
  - http://www.openliberty.org/wiki/index.php/ProjectAris
  - ArisID Providers:
    - http://www.oracle.com/technology/tech/standards/idm/igf/arisid/index.html

- Inquiries to
    - phil.hunt@oracle.com
    - prateek.mishra@oracle.com
  - Blogs:
    - http://independentid.com - Phil
    - http://blogs.oracle.com/identityprivacy - Prateek