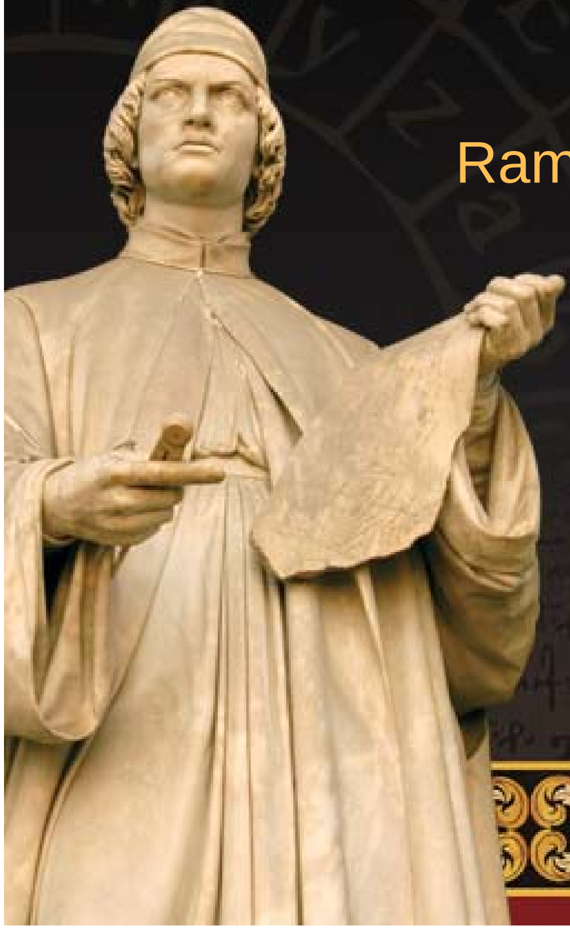
RSA CONFERENCE 2007

Interoperable Provisioning in a Distributed World



Mark Diodati, Burton Group
Ramesh Nagappan, Sun Microsystems
Sampo Kellomaki, SymLabs

02/08/07 – IAM 302

Contacts

- Mark Diodati (mdiodati@burtongroup.com)
- Ramesh Nagappan (Ramesh.Nagappan@Sun.COM)
- Sampo Kellomaki (sampo@symlabs.com)

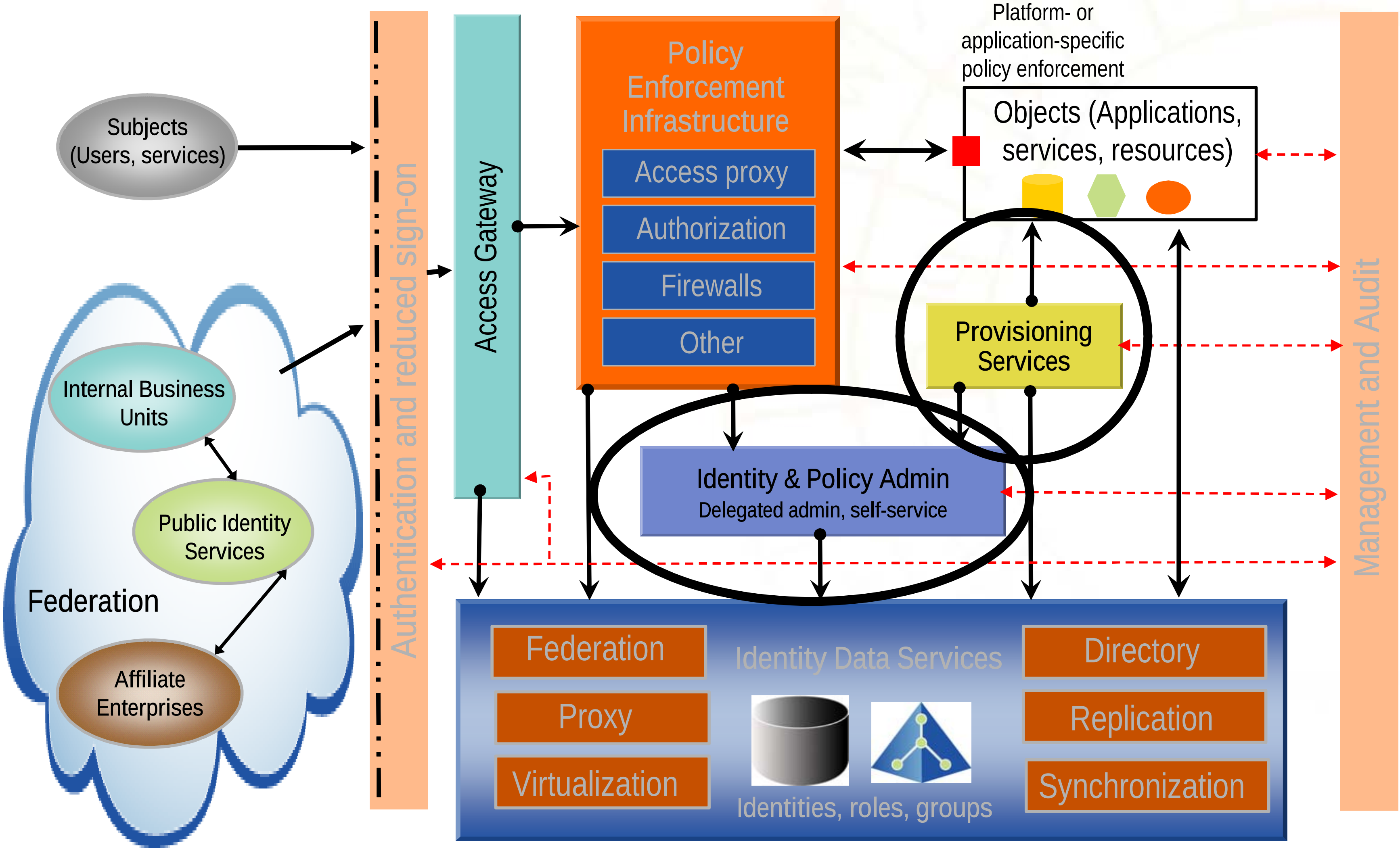
References

- OASIS PSTC SPML 2.0 Specifications
  - http://docs.oasis-open.org/provision/spml-2.0-cd-01/pstc-spml2-cd-01.pdf
- OpenSPML 1.0 Toolkit
  - www.openspml.org
- JAX-WS 2.0 Reference Implementation
  - https://jax-ws.dev.java.net/
- Identity provisioning with SPML – Patterns and Best practices.
  - www.coresecuritypatterns.com
- Sun Java System Identity Manager (Supports SPML 2.0)
  - Download at http://www.sun.com/download/products.xml?id=453fe041
- SPML: Gaining Maturity (Burton Group research document)
  - www.burtongroup.com/spml

Agenda

- ***Presentation – Mark Diodati***
- Presentation – Ramesh Nagappan
- Presentation – Sampo Kellomaki
- References

Identity Management - Provisioning



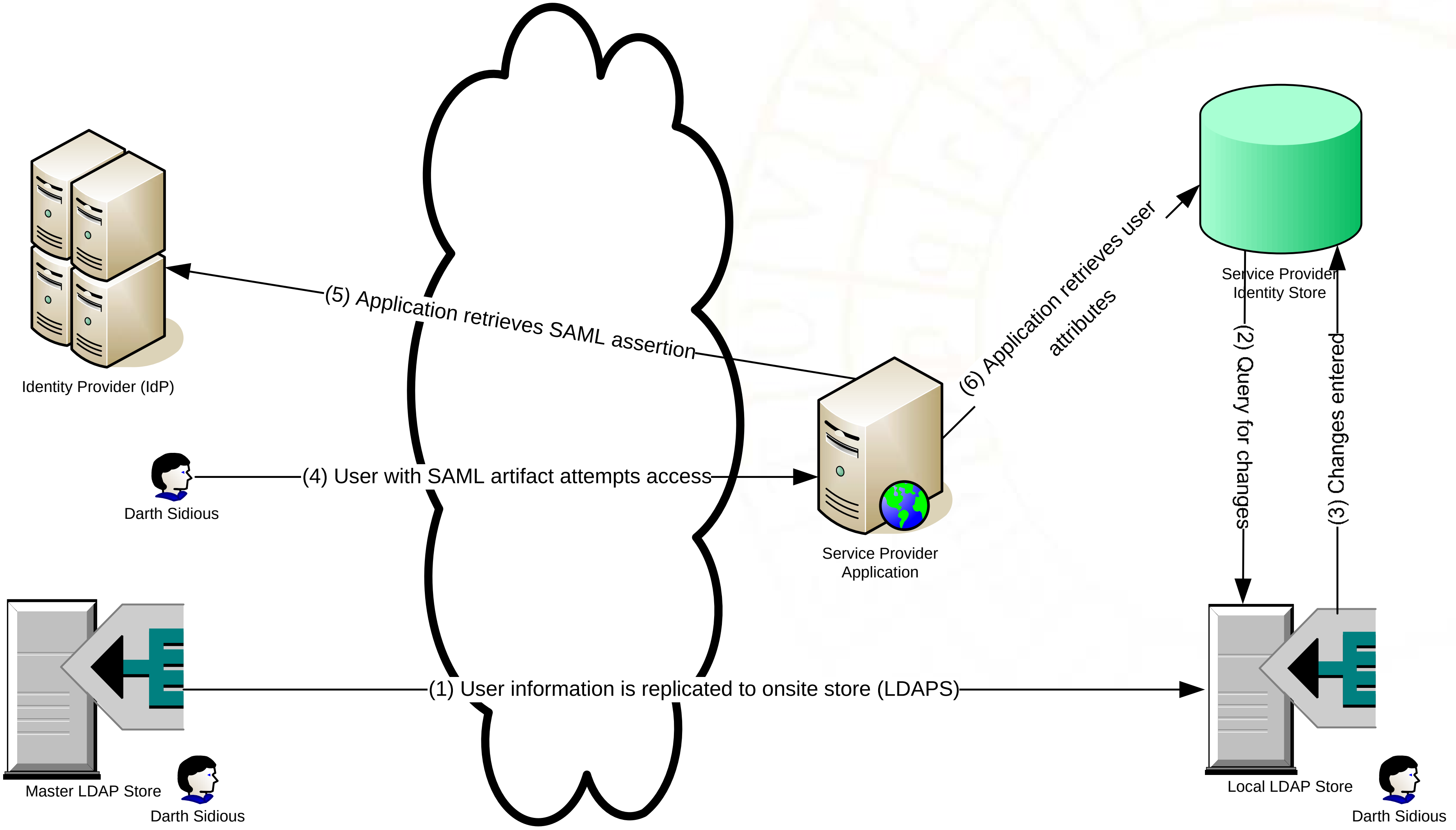
Federated Provisioning

- The federation standards and products are mature from a technology perspective
  - Provide good user SSO (authentication) for web applications
  - Possess some authorization capabilities
  - Lack user identity provisioning capabilities
- Many (most) service provider (SP) applications require a non-ephemeral identity
  - The identity provider (IdP) and SP must agree upon a provisioning protocol to meet this requirement
- ***How are identities provided to the SP?***

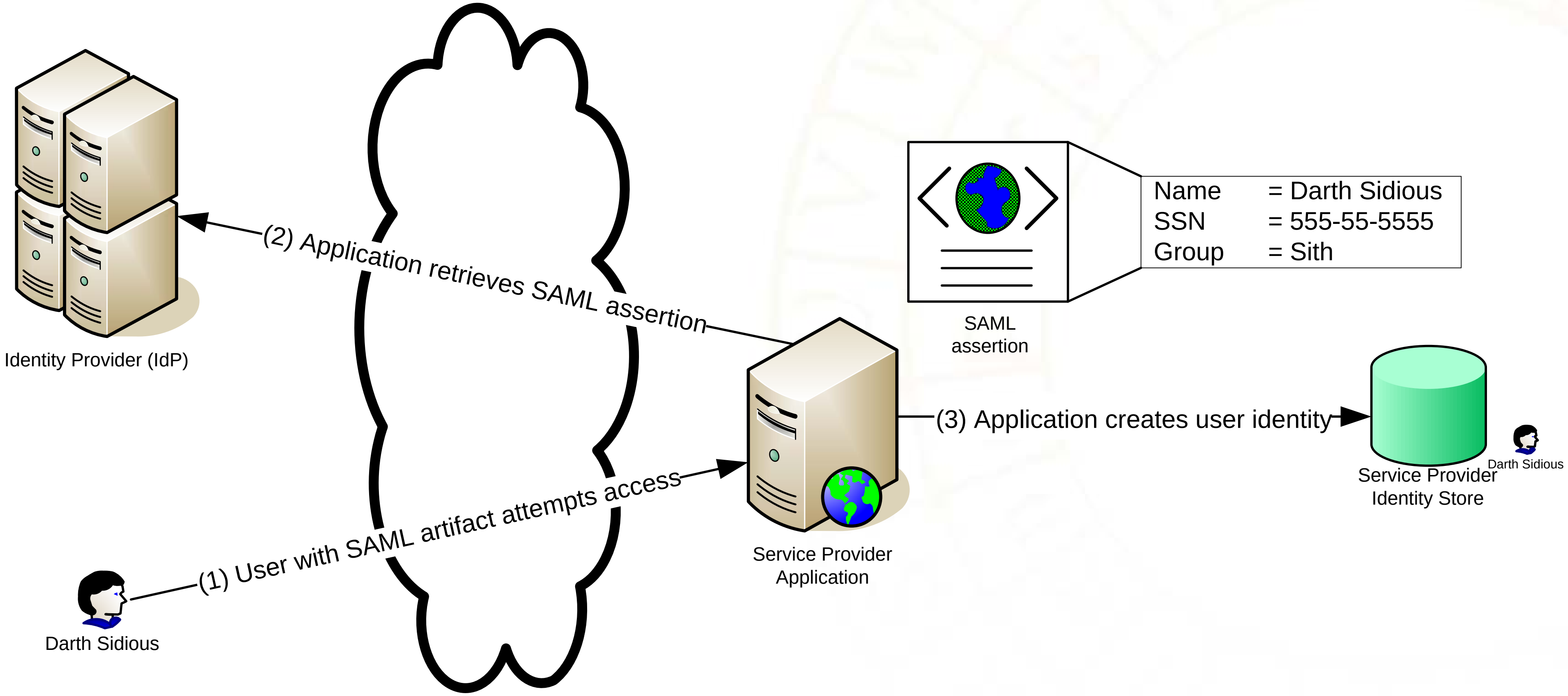
Batch Approach

- Using an out-of-band process, the IdP sends using provisioning information (adds, changes, deletions) to the SP
- Excel spreadsheet, EDI, or other
- Benefits
  - Low technology barrier
- Challenges
  - Slower updates can introduce service and liability issues
  - IdP may not have a mechanism to verify user identities status
  - May introduce burdensome manual processes for both the IdP and the SP

LDAP Replication Approach


Identity Provider (IdP)
(5) Application retrieves SAML assertion
(6) Application retrieves user attributes
Service Provider Identity Store
Darth Sidious
(4) User with SAML artifact attempts access
Service Provider Application
(2) Query for changes
(3) Changes entered
(1) User information is replicated to onsite store (LDAPS)
Master LDAP Store
Darth Sidious
Local LDAP Store
Darth Sidious

Assertion Approach


Identity Provider (IdP)
(2) Application retrieves SAML assertion
SAML
assertion
(3) Application creates user identity
Service Provider
Identity Store
Darth Sidious
Service Provider
Application
(1) User with SAML artifact attempts access
Darth Sidious

Name	= Darth Sidious
SSN	= 555-55-5555
Group	= Sith

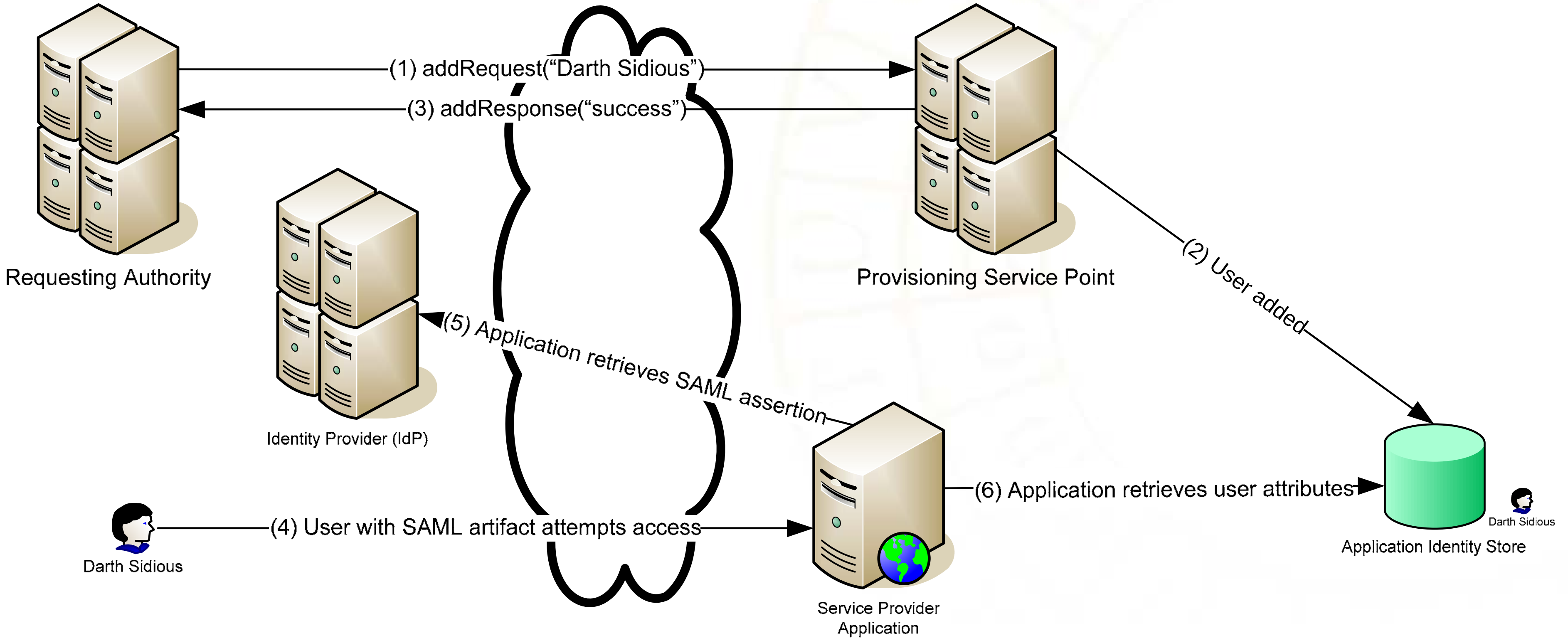
Services Provisioning Markup Language (SPML)

- SPML v1 approved in 2003
  - Some “Essential” operations were not included (had to be customized)
  - Some errors in XML schema
- SPML v2 OASIS standard approved in spring of 2006
  - “Essential” functions included
- Three profiles
  - DSML (most commonly used and existed in v1)
  - XSD (new in v2, from WS-Provisioning proposal)
  - SAML (currently in development) to provide tighter integration of user attributes
- Good provisioning vendor support
  - Widely adopted by the provisioning vendors (Sun, CA, BMC, HP, Oracle, Siemens)
- Improving target vendor support
  - Citrix, SAP, MaxWare

SPML

- Benefits
  - Interoperable provisioning (no custom connectors required)
  - Reliability
  - Some auditing and correlation
- Challenges
  - Requires a separate channel for federated provisioning
  - User schema will likely require pre-agreement
  - Does not provide protocol security (by intent)
    - Authentication and confidentiality - use HTTPS and/or WS-Security 2004
    - Authorization – may be achieved via certificate trust list or may require more advanced authorization features in the future
      - Provisioning tools can provide authorization capabilities

SPML – Federated Provisioning


(1) addRequest("Darth Sidious")
(3) addResponse("success")
Requesting Authority
Provisioning Service Point
(2) User added
Identity Provider (IdP)
(5) Application retrieves SAML assertion
(6) Application retrieves user attributes
Darth Sidious
Application Identity Store
Darth Sidious
(4) User with SAML artifact attempts access
Service Provider Application

Agenda

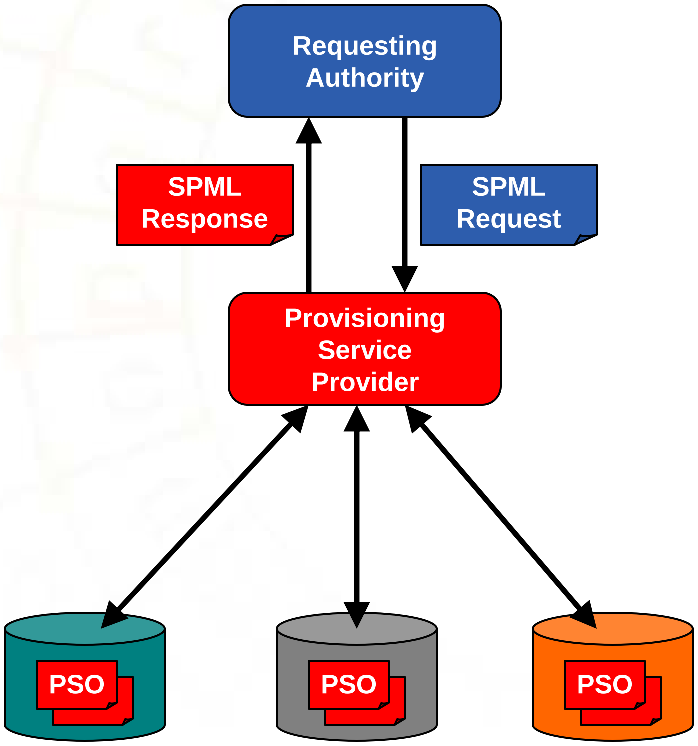
- Presentation – Mark Diodati
- ***Presentation – Ramesh Nagappan***
- Presentation – Sampo Kellomaki
- References

The State of SPML 2.0

- SPML 2.0 has been ratified as an OASIS standard.
- Builds on the concepts of SPML 1.0 specifications.
  - Maintains the core protocol, basic roles, operations, data types and elements.
  - Core protocol enables interoperability among Provisioning service providers.
- Defines modal mechanisms for executing provisioning synchronously or asynchronously.
- Defines the notion of SPML Profiles.
  - Profiles define the agreement protocol between requestor and service provider.
  - SPML v2 XSD Profile and DSML v2 Profile
    - DSML v2 profile provides the backward compatibility with SPML 1.0 and to support LDAP and X.500 directory services
  - SPML v2 SAML 2.0 Profile is on its way !
- SPML 2.0 supports extended operations as “Capabilities”.

SPML 2.0 - Logical components

- Requesting Authority (RA)
  - Client initiating the SPML requests to the provisioning system.
- Provisioning Service Provider (PSP)
  - The identity provisioning system that listens, receives, processes SPML requests and returns responses.
  - Executes provisioning operations.
- Provisioning Service Target (PST)
  - Actual resource where operations are performed.
- Provisioning Service Object (PSO)
  - Represents the data entity on a PST. (ex. User account)



Provisioning Service Targets

SPML 2.0: Operations & Capabilities

- Core Operations (Mandatory)
  - SPML 2.0 conformant providers must implement all of them
  - Basic Operations
    - *addRequest*
    - *modifyRequest*
    - *deleteRequest*
    - *lookupRequest*
  - Discovery Operation
    - *listTargets*

- Optional Capabilities
  - Operations that apply to a specific target and supported by a provider.
  - SPML 2.0 defines a set of standard capabilities
    - *Async capability*
    - *Batch capability*
    - *Bulk capability*
    - *Password capability*
    - *Search capability*
    - *Suspend capability*
    - *Updates capability*
  - Allows PSP define custom capabilities.

Anatomy of a SPML 2.0 Message

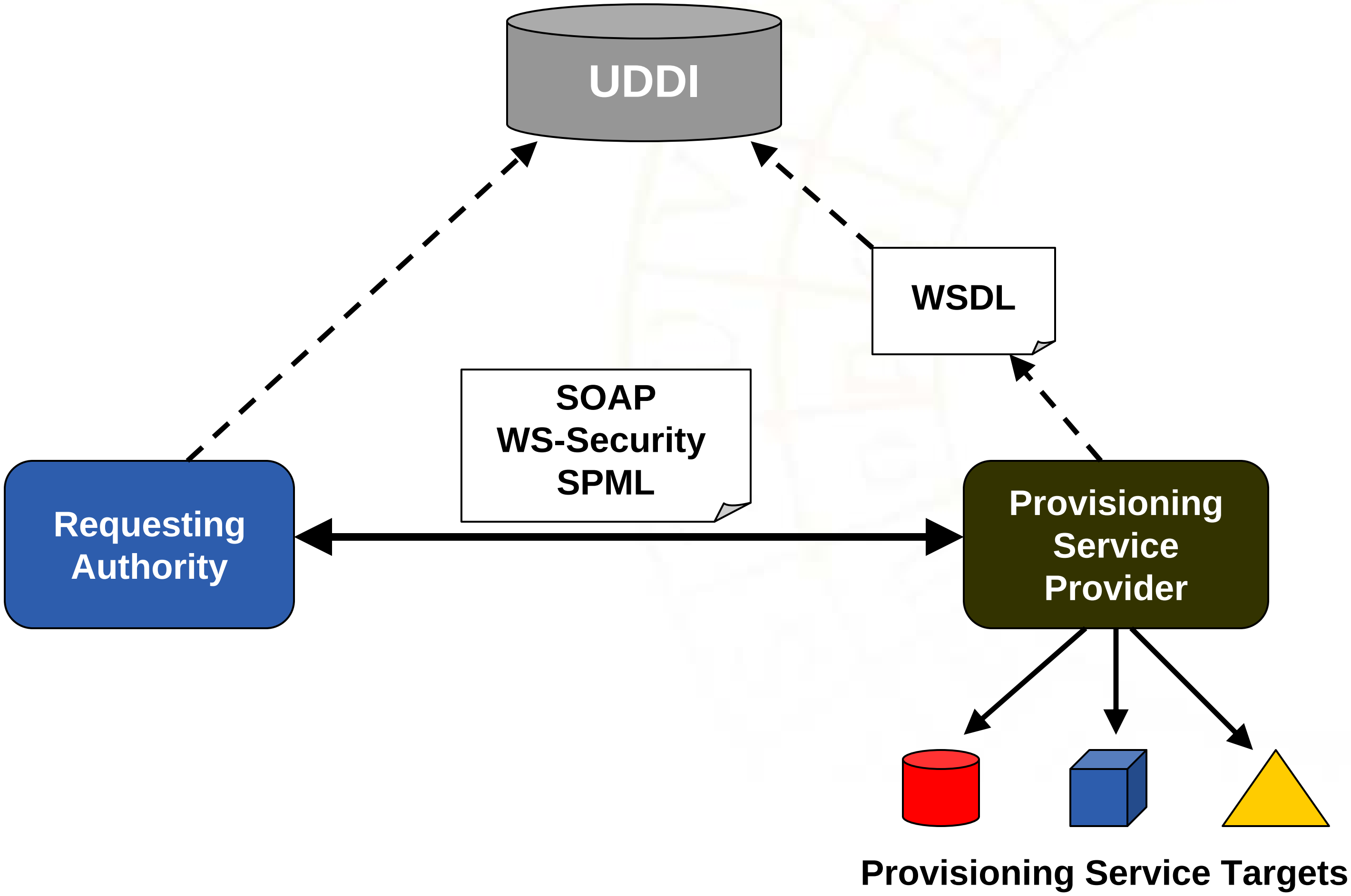
Request Message

```
<addRequest
    xmlns='urn:oasis:names:tc:SPML:2:0'
    requestID='rid-spmlv2'
    executionMode='synchronous‘ targetID=‘xyz1`>

<openspml:operationalNameValuePair xmlns:openspml=
'urn:org:openspml:v2:util:xml'
name='session' value='AAALPgAAYD0A'/>

<data>

<dsml:attr xmlns:dsml=
'urn:oasis:names:tc:DSML:2:0:core' name='accountId'>

<dsml:value>mySPMLTestId</dsml:value>

</dsml:attr>

<dsml:attr xmlns:dsml=
'urn:oasis:names:tc:DSML:2:0:core'
name='objectclass'>

<dsml:value>JavaGuy</dsml:value>

</dsml:attr>

<dsml:attr xmlns:dsml=
'urn:oasis:names:tc:DSML:2:0:core' name=‘password'>

<dsml:value>mypasswd</dsml:value>

</dsml:attr>

</data>

</addRequest>
```

Response Message

```
<addResponse xmlns='urn:oasis:names:tc:SPML:2:0'
    status='success' requestID='rid-spmlv2‘
     targetID=‘xyz1`>

<openspml:operationalNameValuePair
     xmlns:openspml='urn:org:openspml:v2:util:xml'
      name='session' value='AAALPgAAYD0A'/>

<pso>

<psoID ID=‘mySPMLTestId'/>

<data>

<dsml:attr xmlns:dsml='urn:oasis:names:tc:DSML:2:0:core‘
 name='accountId'>

<dsml:value>mySPMLTestId</dsml:value>

</dsml:attr>

<dsml:attr xmlns:dsml='urn:oasis:names:tc:DSML:2:0:core‘
 name='objectclass'>

<dsml:value>JavaGuy</dsml:value>

</dsml:attr>

<dsml:attr xmlns:dsml='urn:oasis:names:tc:DSML:2:0:core'
  name=‘password'>

<dsml:value>mypasswd</dsml:value>

</dsml:attr>

</data>

</pso>

</addResponse>
```

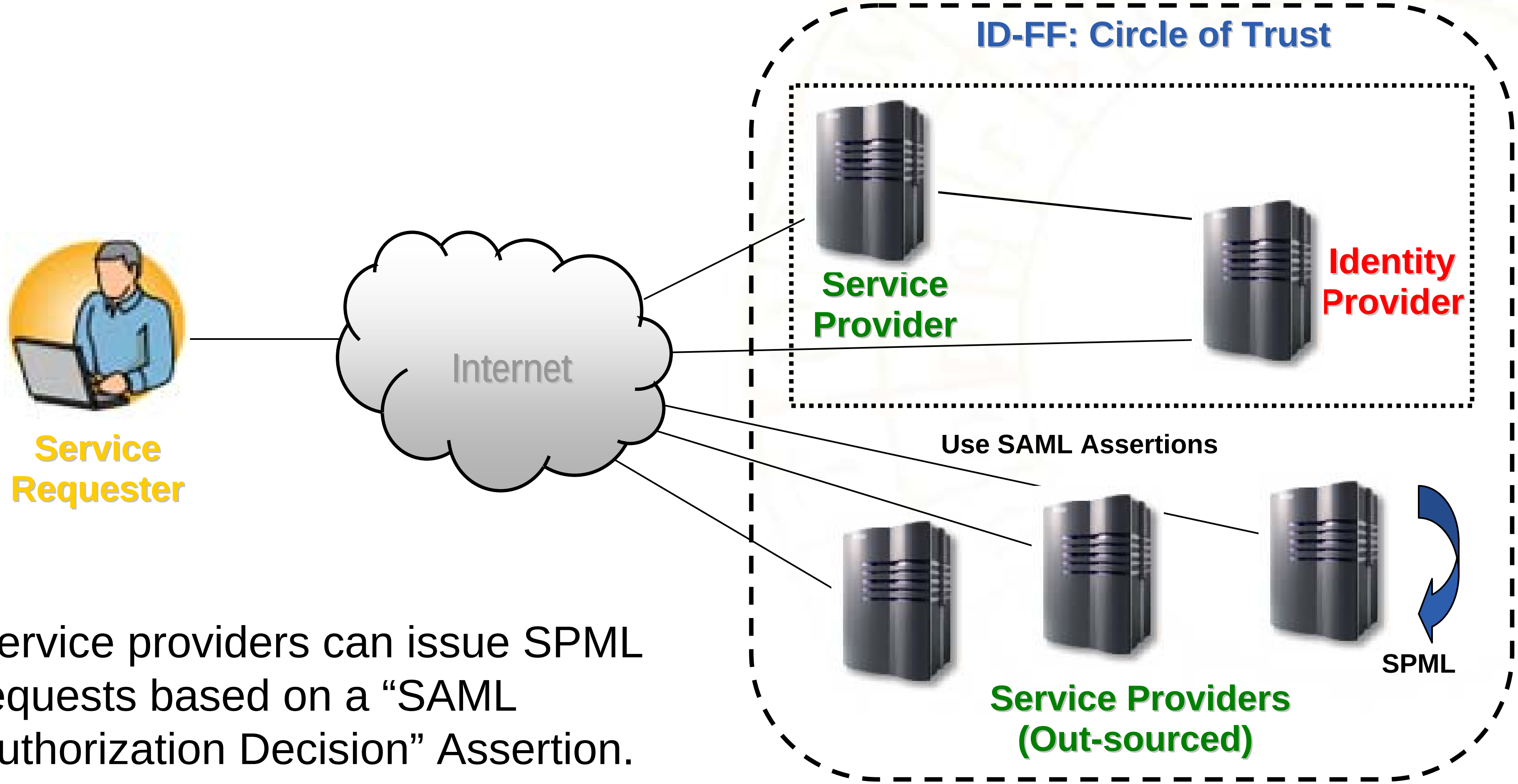
SPML Based Provisioning via Web Services



SPML Relationship with WS-Security and SAML

- SPML recommends the use of SSL/TLS protocols and WS-Security for ensuring Transport-layer and Message-layer security.
  - SPML can take advantage of SOAP/HTTPS transport provisioning requests and responses.
  - XML Encryption and XML Digital Signature allows to ensure SPML message/element-level confidentiality and integrity.
  - WS-Security tokens (X.509, SAML Token) to authenticate provisioning service providers.
- SPML supports the principles of using SAML 2.0 and Project Liberty Alliance standards.
  - SPML requests and responses can make use of SAML assertions as a authentication context between the requesting authority and provisioning systems.
  - SAML assertions from an Identity provider can be used to qualify a subject on a provisioning target.

Role of SPML in Identity Federation (Liberty ID-FF)



Service providers can issue SPML requests based on a “SAML Authorization Decision” Assertion.

- Helps dynamic/on-demand provisioning of roles, privileges, resources etc.

Implementing SPML with Java

- OpenSPML 1.0 Toolkit
  - Comprehensive vendor-independent Java API toolkit for SPML 2.0.
  - Java classes for constructing/parsing SPML requests and responses support implementing a SPML 2.0 conformant requesting authority.
  - Supports SPML 2.0 profiles (DSML v2 and XML Schema) and its supporting Java/XML bindings.
  - Web container pluggable SOAP runtime for sending/receiving SPML messages via SOAP over HTTP.
- JAX-WS 2.0
  - Java API toolkit for developing WS-I Basic Profile 1.1 compliant XML Web Services.
  - Helps to build SPML Web Services with WS-Security.
    - OpenSPML Toolkit can be plugged for creating SPML constructs.

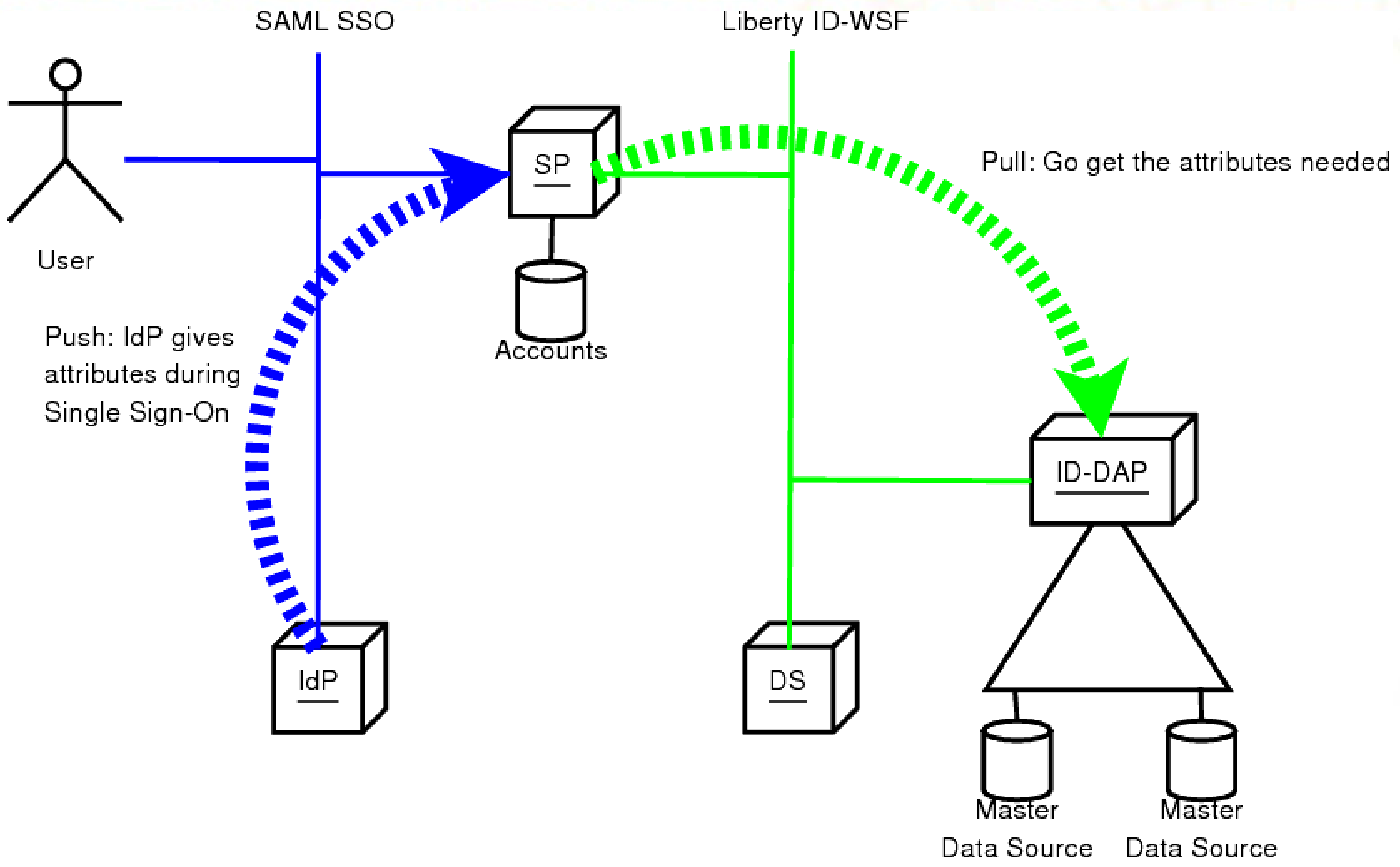
Agenda

- Presentation – Mark Diodati
- Presentation – Ramesh Nagappan
- ***Presentation – Sampo Kellomaki***
- References

Liberty Provisioning Initiatives

- For avoidance of doubt
  - Trusted Module provisioning (liberty-idwsf-prov-v1.0-02.pdf)
  - Very specific target: Advanced Clients and Trusted Modules
    - Not applicable in this domain
  - General provisioning
    - Some marketing requirement floated
    - No specific approach chosen
    - SPML, enhanced with ID-WSF, could be an option

ID-DAP Overview



Pull: Go get the attributes needed

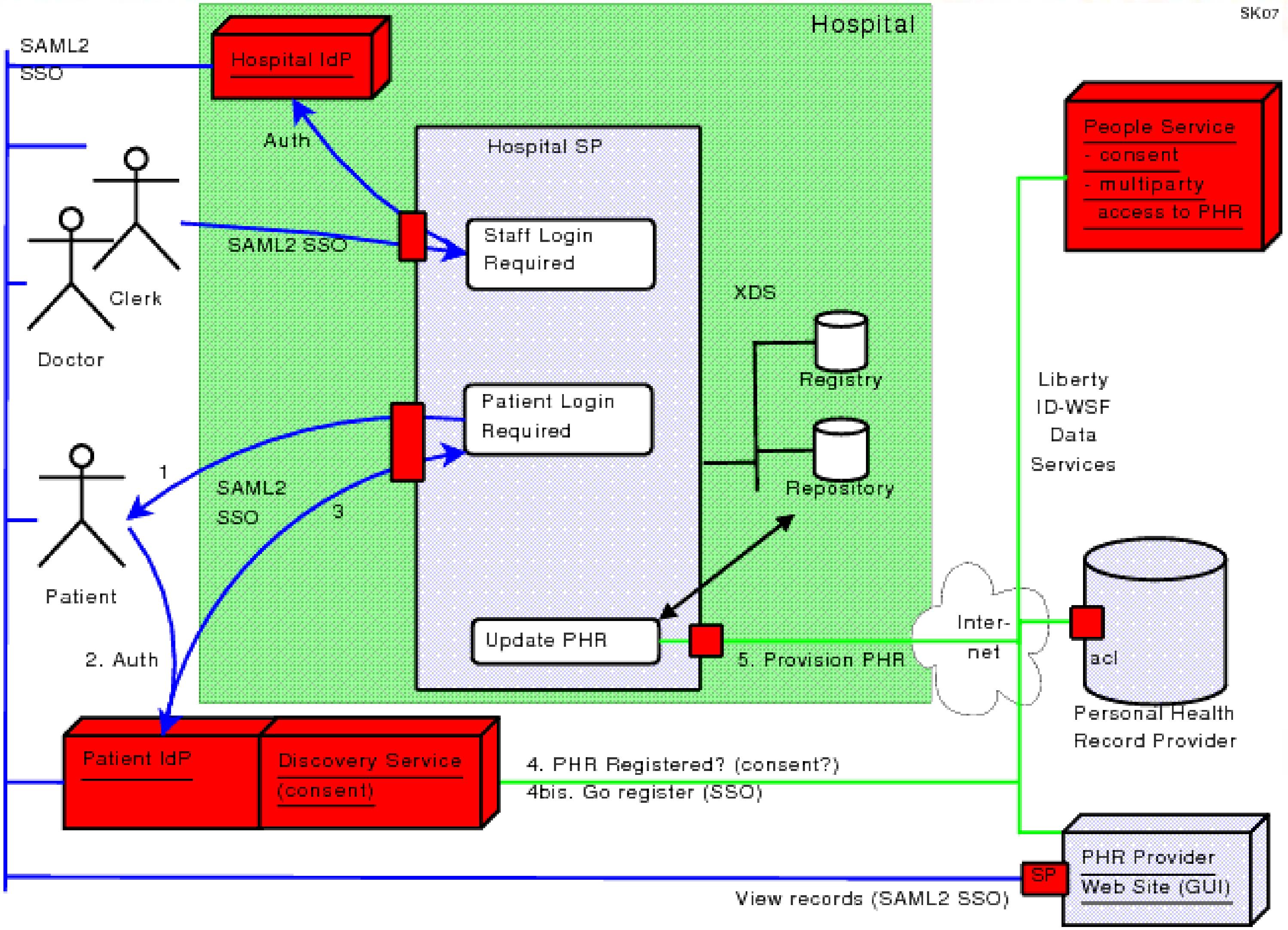
Push: IdP gives attributes during Single Sign-On

Slide 24

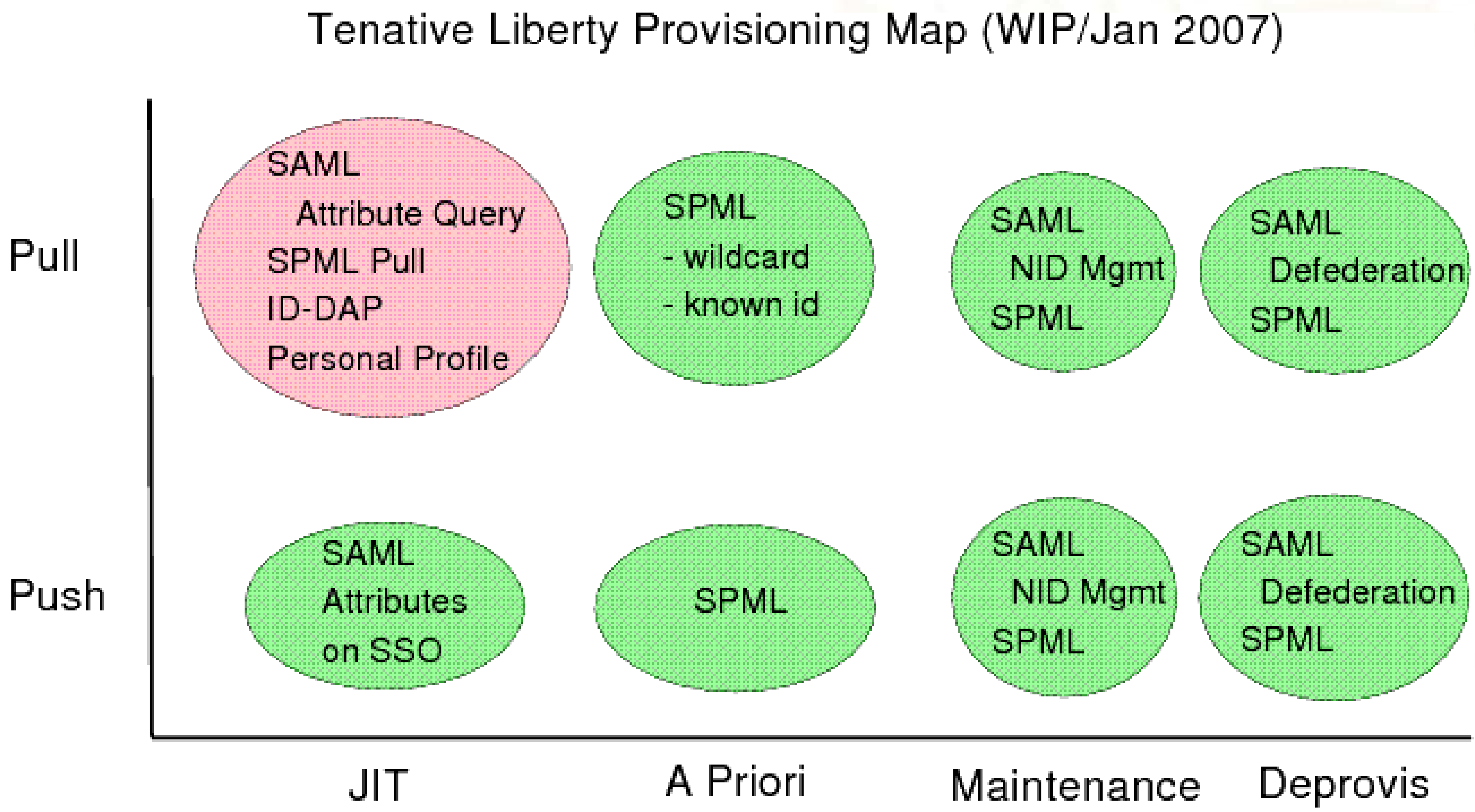
MED1 If this is not a specification or a standard, we cannot discuss in detail, since it breaks interoperability.

Mark Diodati, 1/26/2007

Health Care Use Case



Tentative Liberty Provisioning Map



Tenative Liberty Provisioning Map (WIP/Jan 2007)

	JIT	A Priori	Maintenance	Deprovis
Pull	SAML Attribute Query SPML Pull ID-DAP Personal Profile	SPML - wildcard - known id	SAML NID Mgmt SPML	SAML Defederation SPML
Push	SAML Attributes on SSO	SPML	SAML NID Mgmt SPML	SAML Defederation SPML

Panel Discussion