ACAMP2010 -FederatedProvisioningAndSPMLStandards

Wiki space for work on 2010 Advance CAMP Action Item:

Determine How Federated Provisioning Should Work and Participate in SPML Standards Work to Support it

Note: Discussion is underway on possibly creating a working group on provisioning. See Chad's email

	Overview
Deliverables/Goals	Implemented and adopted standard and software
Group Members	Tom Zeller, U. Memphis (lead), Keith Hazelton & Brad Schwoerer, (U. Wisc). Steven Carmody (Brown), Jens Haeusser (UBC), Nate Klingenstein (Internet2), Jeremiah Adams (UC Boulder), Benn Oshrin (Internet2), Chad La Joie (Itumi)
Status	Work In Progress
Mailing List	<provision@internet2.edu> To subscribe, send mail to <pubsympa@internet2.edu> with the **SUBJECT**: `sub provision FirstName LastName`

PSTC Re-Start

Fortunately, the OASIS Provisioning Services TC has been restarted, public mail list archive here.

As of this writing, the nature of SPML redevelopment has not been defined. However, there appears to be clear agreement regarding the need for a simple adoptable standard, perhaps with the addition of "reasonable defaults" to the specification.

There is interest in standardizing attributes used for provisioning, ala inetOrgPerson, and analog to SAMLv2.

Provisioning across organizational boundaries appears to be a driver behind the desire for SPML enhancement. It would be good to define "Federated Provisioning".

Federated Provisioning : Semantics

Federated provisioning may mean "the provisioning of federation" or "provisioning over a federated protocol" or a combination: "the provisioning of federation over a federated protocol".

For reference, InCommon defines a federation as :

> "A federation is an association of organizations that use a common set
> of attributes, practices and policies to exchange information about
> their users and resources in order to enable collaborations and
> transactions."

The provisioning of federation can be thought of as the provisioning of linkages between objects in a federation. These linkages may themselves define a federation.

Provisioning over a federated protocol would leverage a federation to maintain the trust relationship between a provisioning requester and a provisioned target.

[This is a summary of a thread on the PSTC archives.]

Call for Use Cases

Use cases which will assist in the further development of SPML are desirable, please send ideas to <provision@internet2.edu>, or submit them to the OASIS PSTC either as a member of via the comments mechanism. If you do not with to participate in the PSTC, I (TomZ) will be happy to help your use case along.

Here is an example use case from JHUAPL.

These provisioning use cases may also be of interest to the OASIS SSTC regarding the Change Notify proposal to SAML.

Requests for use cases have been sent to grouper-dev, macc-paccman, and this AI's list, as well as out-of-band.

Use Case : Federated Group Provisioning

A resource accessed by members of a federation may not necessarily be web based. Examples are file system locations or mail groups where authorization is provided by an LDAP directory, specifically a group in an LDAP directory.

Assuming that identities for non-local members are maintained out-of-band, an LDAP authorization group may be comprised of two groups, one consisting of local members and a second group consisting of non-local members. Assume that the membership of the non-local authorization group is maintained by a federated partner, since the federated partner is authoritative for identities in its domain.

Access to a resource by members of a federation may be provisioned via synchronization of a group between federated partners.

This synchronization, for federated partners using Grouper, could take the form of provisioning a non-local group from a local group via a Grouper changelog consumer. Another form of synchronization may use the draft SAML Change Notify proposal.

Use Case : Federated Privilege and Access Management Provisioning, XACML
...

Call for Interest or Position Statement

Provisioning and federated provisioning emerged as topics of interest at ACAMP. It would be great if interested parties could collaborate on some sort of statement summarizing interest from higher-ed. For example, "we really need OSS supporting federated provisioning and here's why ..."

Please feel free to use this space to collaborate.

...

Development

A provisioning library implementation is a good thing. Perhaps we should contribute to OpenSPML or roll our own ?

TODO

- Gather participants.

- Agree on deliverables, especially regarding federated provisioning standards.

-

Deliverables

- Glossary of provisioning terminology based on SPMLv2 - quick win ?

- Survey of provisioning software currently in use via ACAMP or educause - quick win ?

- Classic provisioning software - by next I2MM or ACAMP ?

- Federated provisioning software - ?

-

Working Area

- As mentioned during ACAMP, initializing a provisioning glossary based on the SPMLv2 spec might be a good starting point. The graceful provisioning operations could be discussed and hopefully we can agree on common terminology and technical examples for LDAP directory services such as Active Directory.

- Federated, just-in-time, and "classic" (in advance of usage) provisioning are different - we might further define and characterize these. Interest of participants will likely vary.

- Collaboration on "classic" provisioning software and tools is desireable. Correlate with UNC-SPML AI.

-

ACAMP AI Conference Call 2010-09-29

Report :

There is a rather fortuitous interest in provisioning, especially federated provisioning, in the PSTC and SSTC as well as I2.

Sucesses :

- participation in PSTC and SSTC
- starting to define scope of federated provisioning

Roadblocks :

- need more use cases

Deliverable/goal for final AI call in mid-November :

- perhaps determined via I2MM Fall 2010

Beyond mid-November :

- someday, real software