Attendance

Active Members

Tony Gullotta, Access360
Gavenraj Sodhi, Business Layers
Yoav Kirsch, Business Layers
Tim Moses, Entrust
Bill Games, Sig.net
Darran Rolls, Waveset

Prospective Members

Steve Henning, Access360
Dave Taber, IBM
James Tauber, Mvalent
Ed Grossman, Sig.net

1) Agenda Review

(USE CASES ARE IN RED)

2) Things to do

- a. Project Plan – dates/next steps
- b. F2F Dates
  - i. March 25/26 West Coast (Business Layers)
  - ii. May 14/15 East Coast
- c. Use Case sub-committee
- d. Complete Query
- e. Explore move/remove domain model
- f. Explore schema

    g. Explore Replace
    h. 30 – day submission issue
    i. Logo + T-shirts
    j. Requirements comprehensive doc
    k. Clear statement before UC describes <ID> and ID ….
    l. BTP for resources
    m. DSML v2
    n. Business case paper that explains the purpose, scope, and value of this effort
        i. ? What level of U/C detail in this ?

3) Road Map
    a. Use Case/Requirements
        i. End of March
        ii. Formation of Use Case/R Sub-committee
        iii. Editor role (Gavenraj)
        iv. Common Format (UML)/UC
            1. Requirements/Statements
            2. U/C models
            3. Business Cases
        v. Draft: F2F March 26th
    b. Domain Model/Glossary
        i. End of March
    c. Research/Protocol Analysis
    d. Bindings
    e. First Draft of Specification
        i. May 14th
    ~~f. 30-day submission date~~

g. Formation of UC/R committee

h. Common format: UML/UC

   i. Requirements/Statements

   ii. U/C models

   iii. Business Cases

i. Draft F2F 26th of March

```
<VID>
          <PSTID>
             ----
             ----
          <PSTID>
             ----
             ----
<VID>
```

4) Provision Operations

   a. Add/Create

      i. PSP

         1. Introduces <VID> that relates PSTID's

         2. Within a given PSP, <VID> attributes can be obtained from its owning RA possibly via SAML Attribute Assertions

         3. VID = Virtual ID – is unique to Requesting Authority (RA) for each PSP

         ~~4. Should support optional parameters for:~~

            ~~a. Schedule (Start Date) – Abstract~~

         5. ~~RA – PSP requests encapsulate PSP-PST requests adding “transactional semantics” + the return of a VID~~

         ~~6. Multiple add/creates for the same <PSTID> errors out. Don't support multiple <VID> per request.~~

      ii. PST

        1. Add/create instance of an object managed by PST
        2. Provide attribute values for required
        3. PSP can define the <PSTID>
        4. PST can generate <PSTID> and return it its PSP
        5. Multiple adds for same <PSTID> errors out

b. Modify

    i. PST

        1. PSP must supply <PSTID>
        2. Supports single attribute modify (like LDAP)
        3. If <PSTID> does not exist – error out
        4. Supports Async/Sync
        5. Support Batch
        6. Partial Complete

    ii. PSP

        1. Support just <VID> and have specified attribute sync'd
        2. As per add.

c. Delete (**From now on, only unique items are stated**)

    i. PST

        1. Just <PSTID> required
        ~~2. Support for partial completion with detailed response~~
        ~~3. Support Async/Sync~~

    ii. PSP

        1. Just need <VID> as minimum
        2. Support PST deletes for all PST's related to <VID>
        3. This should feel just like a batch request implicitly relates to all <stop on failure> <order etc>
        4. Support for explicit <PSTID> deletes

d. Query

    i. PST

        1. Search PST by any combination of known attributes to identity a <PSTID> - filler semantics as per LDAP
        2. Support size limits to restrict returned data with well defined "data set returned" semantics

3. Specified list of attributes required

ii. RA → PSP

1. Ability to query extended parts of the PSP’s object model
2. Any of the PST query requirements for a given PST query requirements for a given PST
3. Query (can return specified attributes)

a. A <PSTID> for <VID>

b. Available services (PST’s)

c. List of <VID> for requester

4. Transaction queries for

a. Pending requests

b. Historical reports

e. Rename/Move

i. PSP

1. Ability to change any attribute of <VID>
2. PSP ~~implementation~~ should maintain integrity when changing <VID> attributes

ii. PST

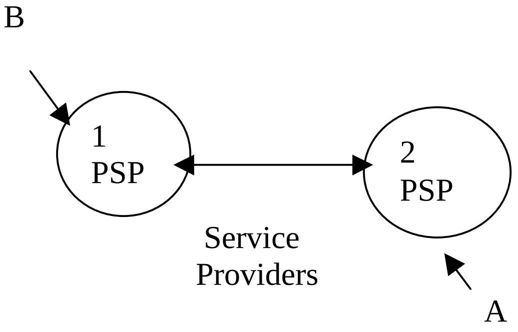
1. Ability to change any attribute of <PSTID>
2. Optional support – but if done must again support referential integrity of model

# Master/Slave

Global “Verb” Requirements

- Specification of <PID>
- Support for Sync/Async with support for query status in Async
- Ability to cancel Sync/Async
- Partial Completion – Status Response
- Batch with support for mixed ‘verbs’
  - Ordering
  - Stop on Fail
- If a PSP abstracts PST’s for what ever purpose (round robin) the semantics should be consistant

- PSP verbs support an abstract for schedule semantics
- PSP verbs are a for a single <VID>
- PSP requests encapsulate PST requests while allowing for implied batches
- **<PSTID> - is unique identifier for a given PST**



Relate provisioning activities outside of Batch

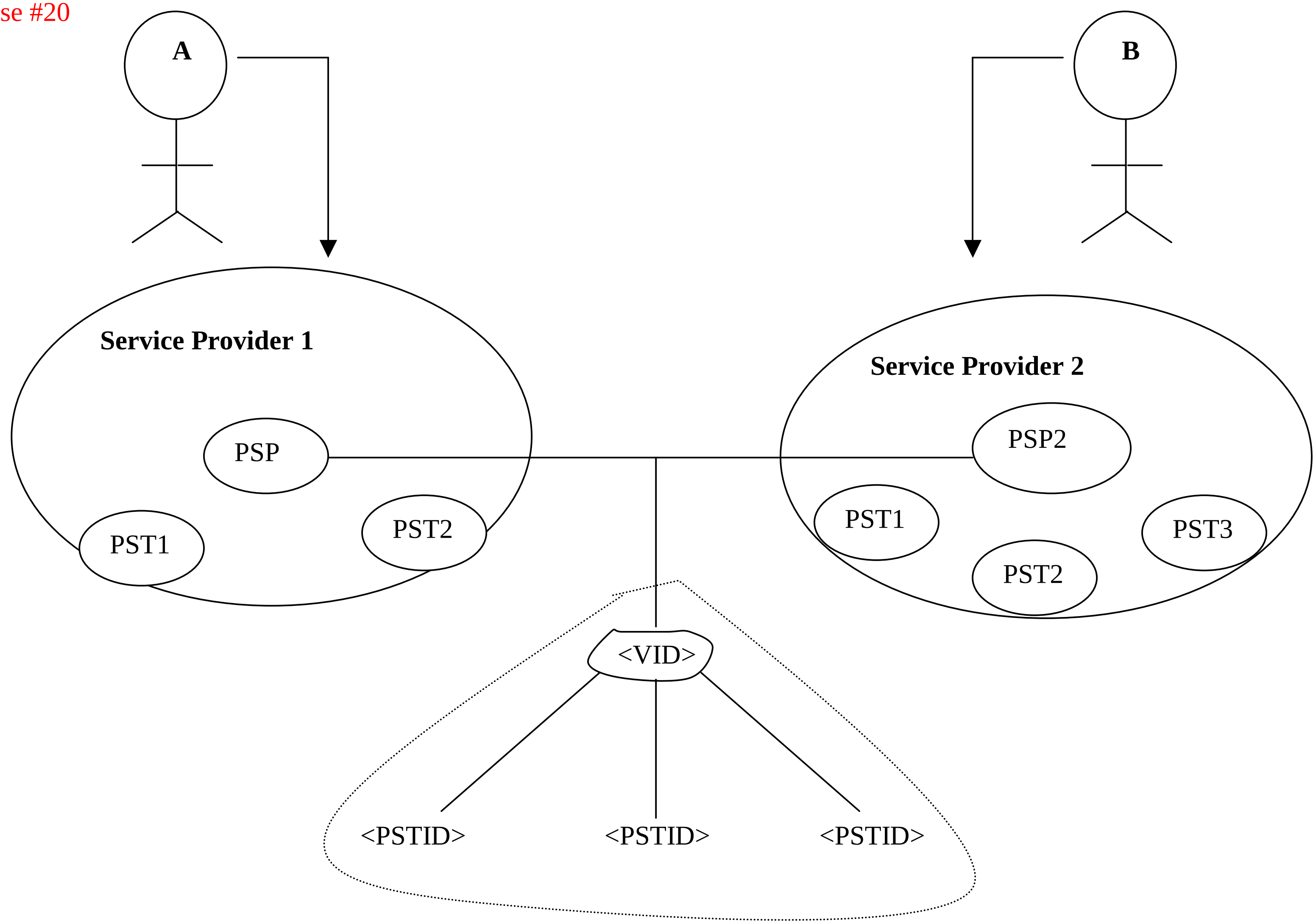
PST add/create command with accompanying VID information and scheduling

Requests can be associated outside a to a Virtual Identity.

Schema

- Support dynamic query of a managed schema
- Definition of a schema to support
  - Attribute lists (of them)
  - Attribute modifiers
  - Comprehensive type expression to include composite types
  - Required/optional
  - Support multi-value attributes
- Extensive
- Possible mechanism for operations on an object. E.g., how do I use PSML to do a reboot
- In general, schema should be ‘OO’
- Means of defining primary key for added record to support compound attr.
- Support “name spaces”

Use Case #20



Identity not verified.

Questions/Issues

Support for:

- Provisioning to non-use ….
- Where does the implementation of a request get deferred? Conformance issues support….
- What's in protocol 'V' implementation
- Lightweight protocol – allow for minimal implementations for RA
- Do we need to define attributes actions separately?
- ~~Detailed view of use case~~
- Do we need a transaction object?
- ~~The PST can be anything~~
- Are attributes mandatory?
- Do we need an understanding of an order?