



VOOT

WP3 meeting, Vienna

Michal Procházka | CESNET | 10. 3. 2016 | WP3

VOOT



- Simple protocol for accessing information about users' group memberships
- Read-only protocol
- Designed to be used in cross-organization environment
- Two versions exist: VOOT 1.0 and VOOT 2.0

History



- VOOT 1.0
 - JSON notation
 - Authentication
 - Basic Auth
 - OAuth2
- VOOT 2.0
 - JSON notation
 - Based on SCIM
 - Just OAuth2 authentication
 - Not backward compatible with VOOT 1.0

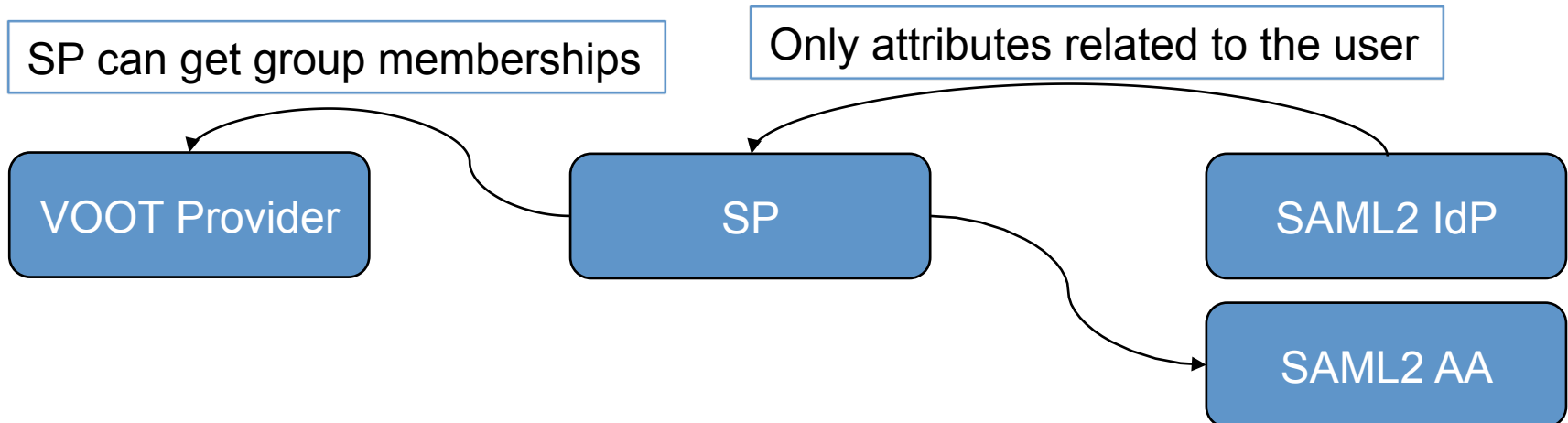
VOOT vs. SAML2

- VOOT

- Data are requested by the service directly
- Users' group memberships
- List of group members
- Supports out-of-bound queries

- SAML2

- Data are transported with the login flow
- Possibility to ask via AA
 - Security considerations
- Receives only data related to the user

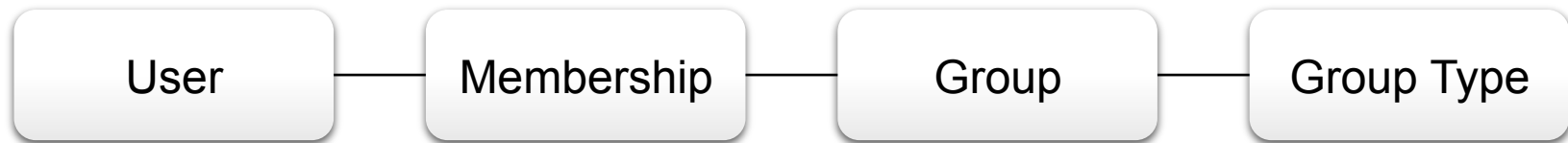


VOOT 2.0



- Extension of SCIM
- Adds new data type Translatable String
- Single purpose protocol
 - Get information about the membership and groups
- Relies on external authentication – OAuth2
- Supports inactive/expired memberships

Data Model



User



- User is identified just by an ID
- Rest of information can be carried as SCIM properties
- VOOT provider must map user from OAuth2 authN

Group object



- Static information about the group, can be cached
- Required properties
 - Id
 - displayName
- Optional properties
 - description
 - type
 - notBefore
 - notAfter
 - public
 - active
 - sourceId
 - membership

Group object example

```
{  
  "id": "8878ae43-965a-412a-87b5-38c398a76569",  
  "displayName": "MAGIC WP3 Members",  
  "sourceId": "collaboratorio:magic"  
}
```

Membership object



- No required properties, {} means user is member
- Optional properties
 - basic (member, admin, owner)
 - displayName
 - active
 - notBefore
 - notAfter
 - may
 - userId
 - groupId

Membership object example

```
{
  "basic": "admin",
  "displayName": {
    "en": "WP Leader",
    "cs": "Vedoucí WP"
  },
  "notBefore": "2015-05-01T00:00:00Z",
  "notAfter": "2017-05-31T00:00:00Z",
  "active": true,
  "userId": "gustavo@magic-project.com",
  "email": "gg@redclara.net",
  "groupId": "8878ae43-965a-412a-87b5-38c398a76569"
}
```

GroupType object

- Defines commonalities between types of groups
- Required properties
 - Id
 - displayName
- Example

```
{  
  "id": "magic:mailinglists",  
  "displayName": {  
    "en": "Mailing lists",  
    "cs": "Mailové listy"  
  }  
}
```

Endpoints



Endpoint	Description
/me/groups	The group memberships of the current user
/me/groups/{groupid}	My membership of this particular group
/groups/{groupid}	Details about a group
/groups/{groupid}/members	Members of a group
/groups	List all groups
/grouptypes	List all group types
/user/{userid}/groups	The group memberships of the specified user
/user/{userid}/groups/{groupid}	A specified users membership of this particular group

Use Cases



- Access Control
 - An application can get the user's group memberships or group members and do the authZ
- Invitation
 - E.g. collaboration tools where users need to be known in advance
- IAM systems synchronization
 - Synchronise groups among different IAM systems

Deployments



- Perun (VOOT 1.0)
- SurfConext/OpenConext (VOOT 1.0)
- Feide Connect (VOOT 1.0?)
- Grouper plugin (VOOT 1.0)



<http://openvoot.org>

michalp@ics.muni.cz

Michal Procházka | CESNET | 10. 3. 2016 | WP3