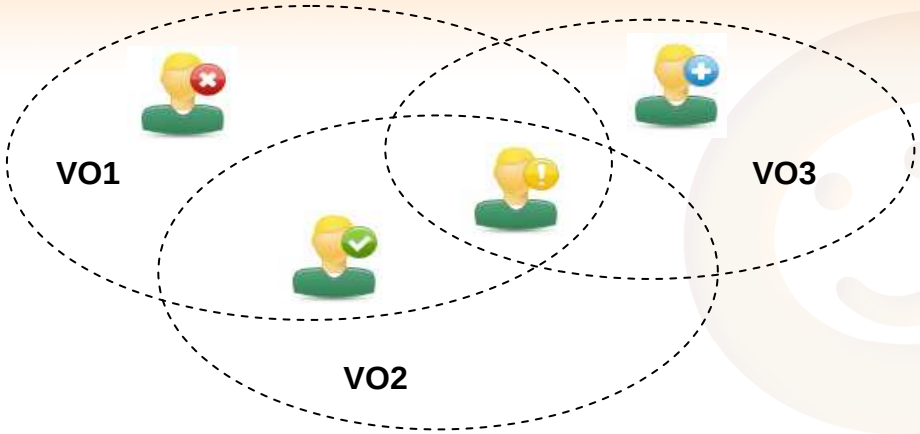


Le Attribute Authority e il Virtual Organization Management

Roberto Gaffuri – Politecnico di Milano

Agenda

- Concetti base (dal group mgn. al VO mgn.)
- Soluzione SAML 2 (Shib) based
- Cenni alle piattaforme collaborative emergenti

Cos'è una Virtual Organization?

Definizione: "Una Virtual Organization (VO) è un gruppo di individui che collaborano attraverso l'uso di servizi online" (*Chad la Joie –Internet2)*

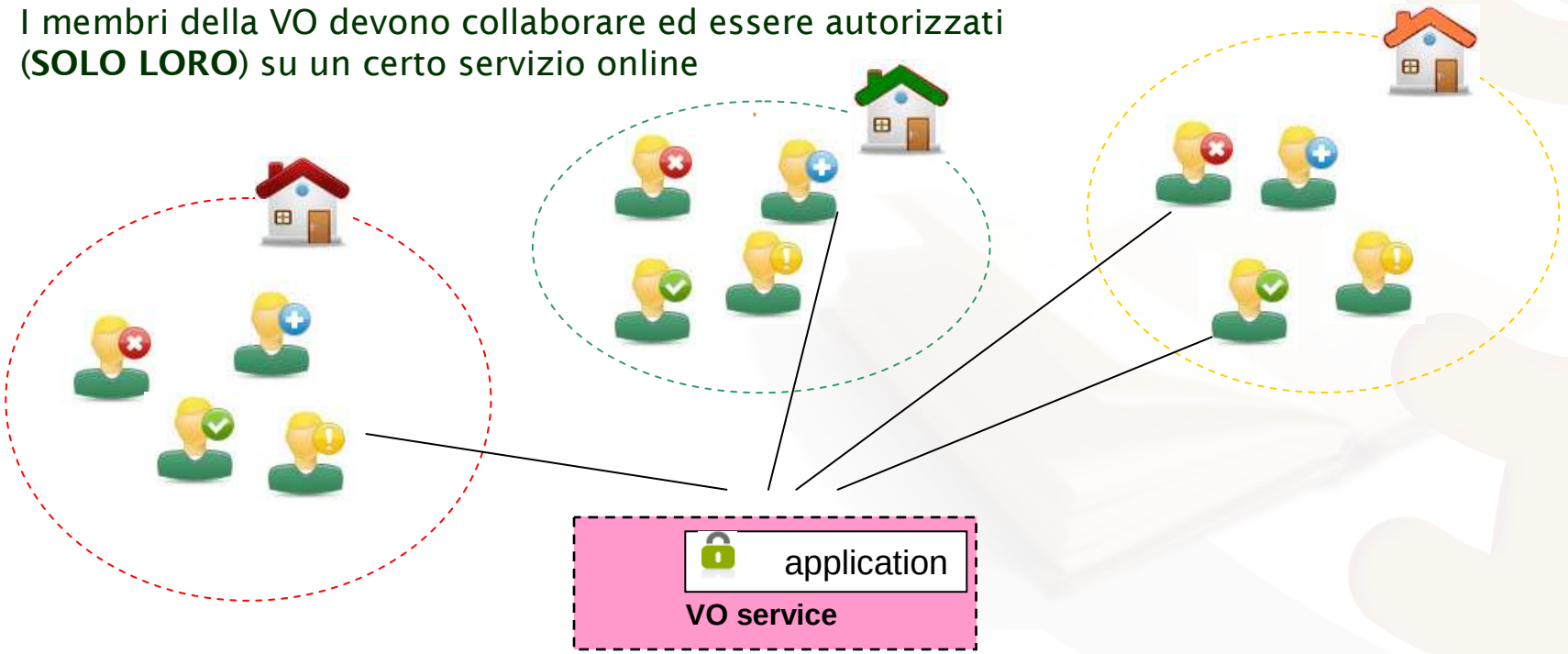
VO = People + Services

Esempi di VO:

- Il comitato tecnico scientifico di IDEM che collabora su un wiki condiviso (i membri appartengono all stessa federazione)
- Un gruppo di ricercatori che lavorano ad un progetto di ricerca e devono accedere a risorse collaborative in rete (i membri appartengono a diverse federazioni)

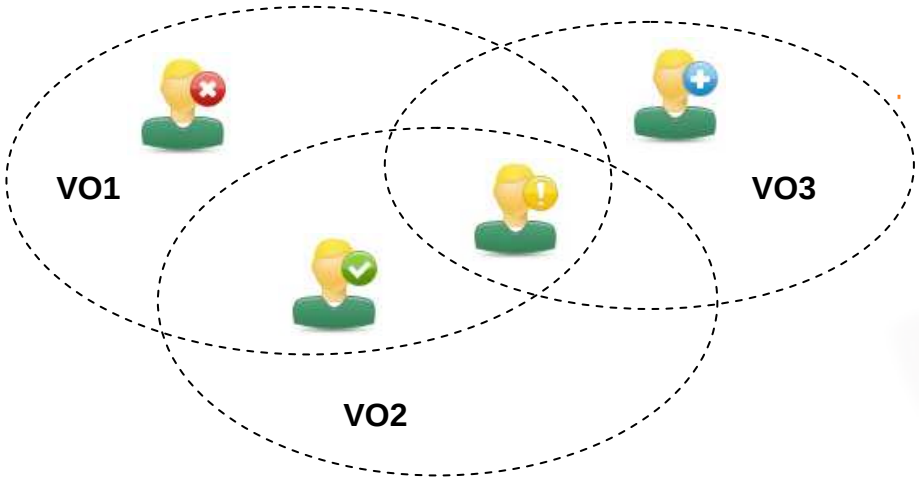
Caratteristiche di una VO

- Membri della VO appartengono ad organizzazioni diverse (anche di federazioni diverse). Non appartengono alla medesima gerachia di controllo
- I membri della VO non hanno attributi provenienti dalla propria organizzazione (es. affiliation) che li possano accomunare
- I membri della VO devono collaborare ed essere autorizzati (**SOLO LORO**) su un certo servizio online



Come autorizzare ad un servizio solo i membri di una VO?

Idea: ai membri di una VO è dato un attributo comune (VO attribute) che definisce l'appartenenza alla VO



VO Attribute:


IsMemberOf=VO3


IsMemberOf=VO1,VO2,VO3


IsMemberOf=VO1,VO2


IsMemberOf=VO1

Vincolo: le Home Organization dei membri di una VO non hanno autorità sui VO attributes

La sfida all'AAI delle VO

- Definire una terza parte in grado di:

  -> amministrare le VO aggiungendo i VO services e i gruppi di utenti cross istituzione/federazione che ne fanno parte (**VO Management**)

  -> fungere da autority per i VO attributes (**Attribute Authority**)

- Fare in modo che i VO services siano in grado di aggregare attributi provenienti dalla VO platform (**group membership attributes**) e attributi provenienti dalle home-org dell'utente (**identity attributes**)

Géant GN3 Project (2009-2013)

1. GÉANT network
2. Wider range of services
3. **Joint Research Activities**
   - JRA1: Future Network
   - JRA2: Multi-domain Resources and Services
   - **JRA3: Enabling Communities**
     - Task 1: Roaming developments
     - **Task 2: Identity Federations**
       - **Sub-Task I: Virtual Organizations**
     - Task 3: Composable Services
4. Networking Activities

http://wiki.geant.net/bin/view/JRA3/VirtualOrganizations

Soluzione "Shibboleth-only" – Switch

Status update on the SWITCH Virtual Organization Pilot

(Lukas Hämmerle – Vienna 23 Novembre 2010)

SWITCH
Serving Swiss Universities

- **FASE 1 :**

Giugno 2009: Chad la Joie propone un architettura di riferimento Shibboleth-only (no other APIs/libraries)
https://spaces.internet2.edu/display/~lajoie@idp.protectnetwork.org/VOPlatform

- **FASE 2:**

SWITCH appronta un proof-of-concept con un test case che coinvolge alcuni partner (GEANT JRA3-T2).
Viene utilizzato GMT (Group Managment Tools) come piattaforma per la gestione delle VO

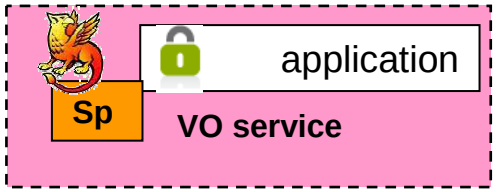
- **FASE 3:**

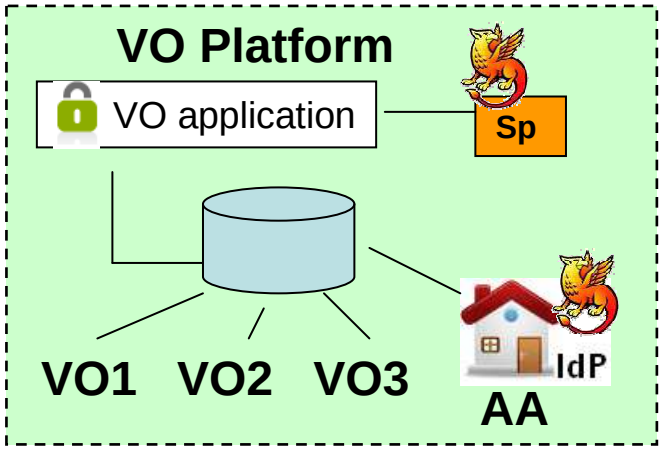
Ottobre 2010 parte ufficialmente una fase di open pilot per SWITCHaai (http://www.switch.ch/vo)
Public Project web page: https://forge.switch.ch/redmine/projects/vo-pilot/
Contact: vo-pilot@switch.ch
Viene sviluppato il tool **COMATO** come VO Mgm. Web Interface: https://test.collaboration.switch.ch/comato

- **FASE 4:**

Fase Pilota finisce a Febbraio 2011
Produzione Marzo 2011 (Codice probabilmente sarà reso open source)

I componenti AAI coinvolti





User Home Organization

- Autentica il membro della VO ed è autorità per le informazioni base dell'identità

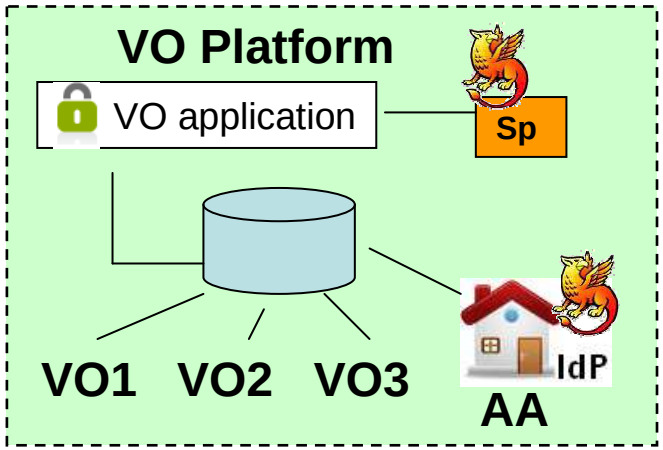
Virtual Organization Service

- Sono i servizi utilizzati dai membri di una VO per svolgere qualche compito online

Virtual Organization Platform

- Un insieme di componenti software in grado gestire delle VOs e di offrire ai VO Services informazioni di memberships degli utenti

Funzioni della VO platform



Gestione delle VOs:

- creazione/rimozione di una VO, inserimento dei VO services che sottoscrivono una certa VO

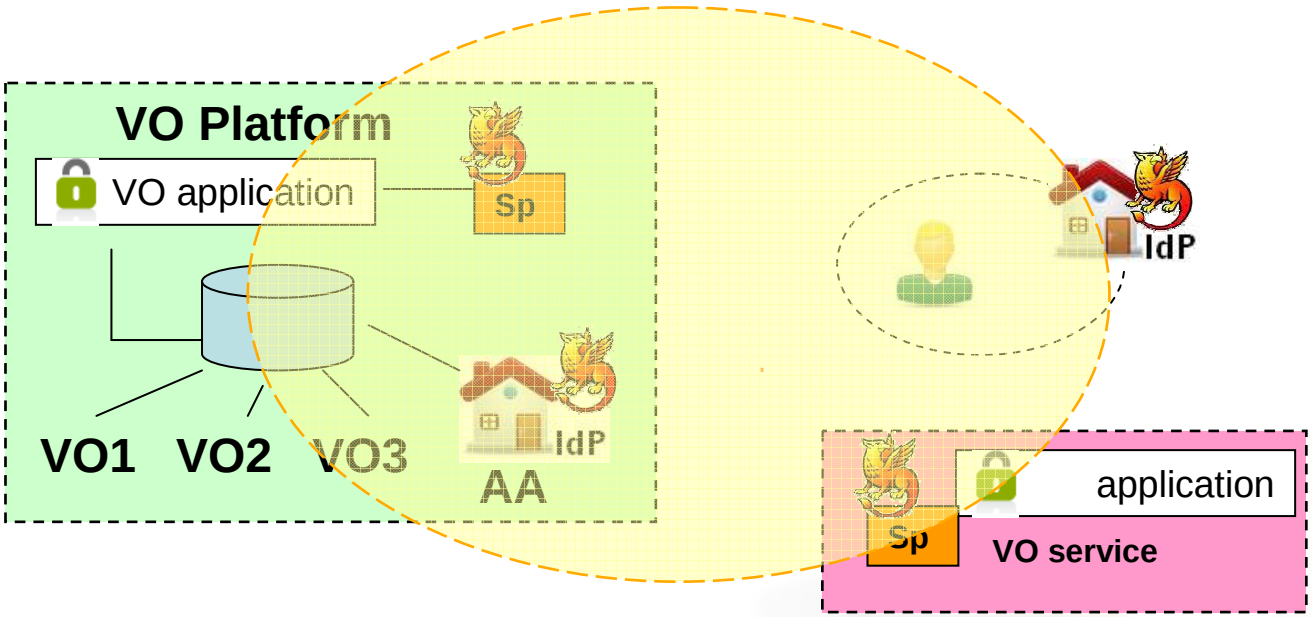
Gestione dei VO members:

- Invito/Inserimento/rimozione di un utente in una data VO

Attribute authority:

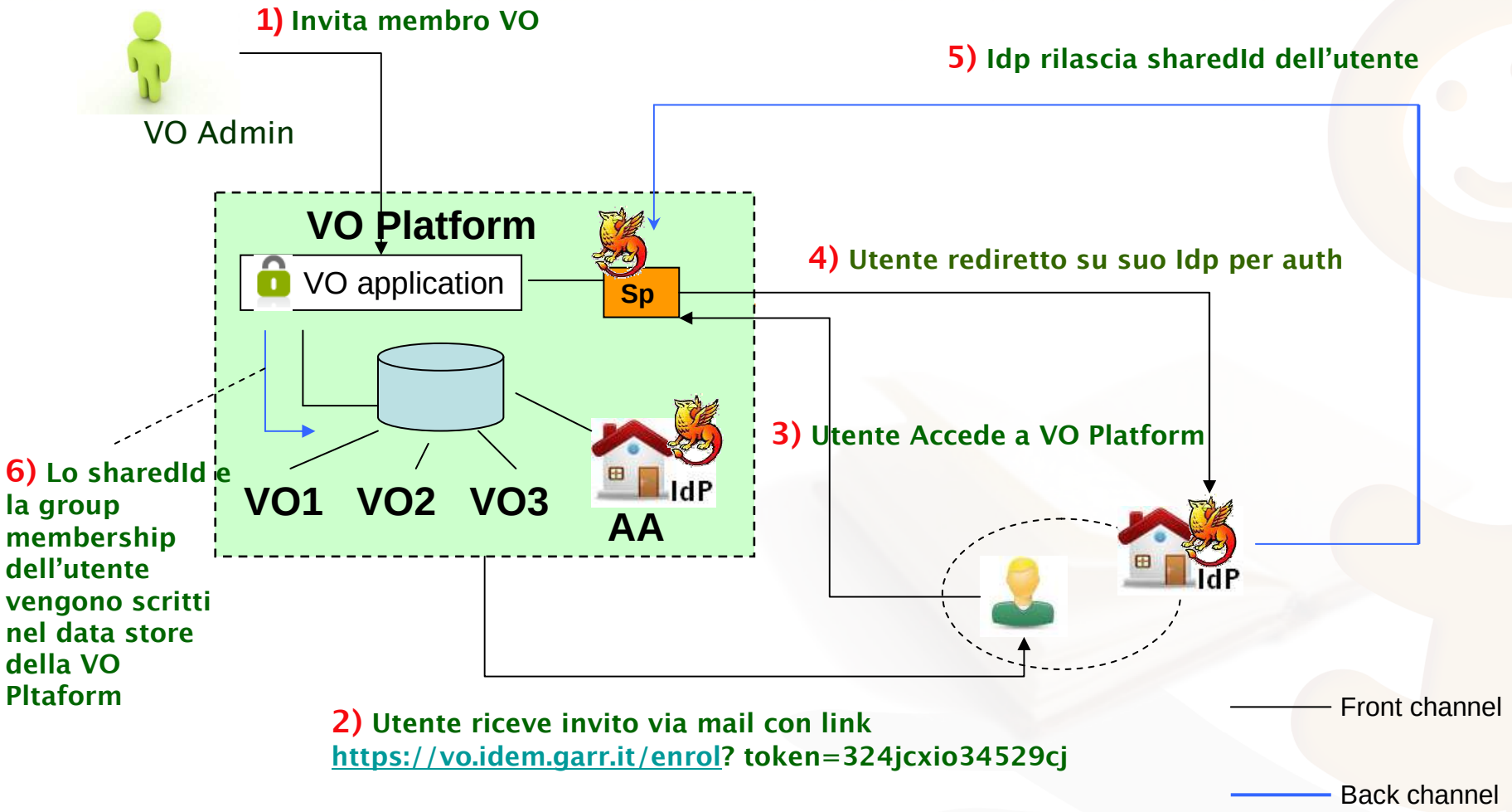
- Esposizione ai VO Services degli attributi di membership degli utenti

Interazioni base tra i componenti

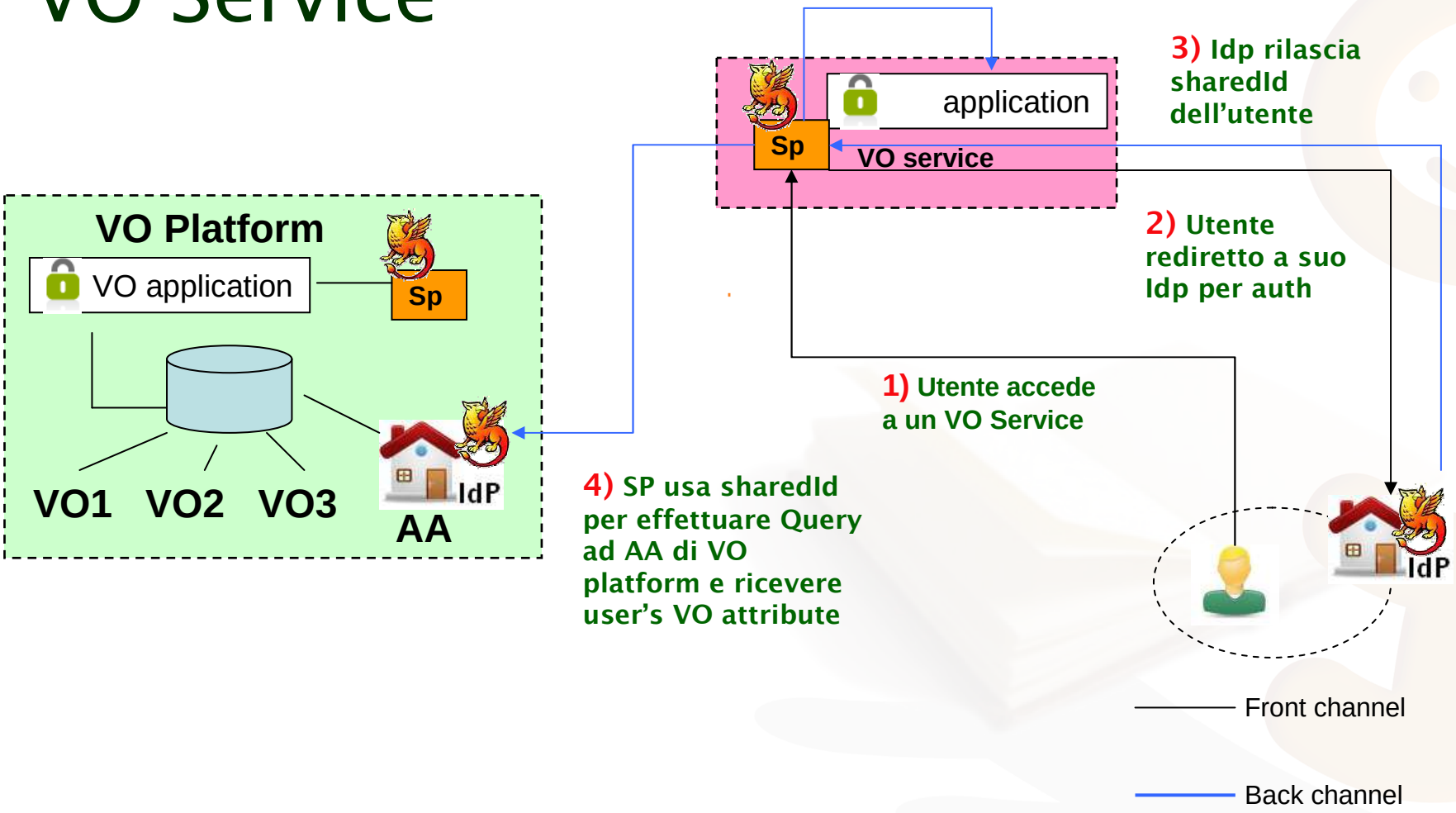


- Registrazione di un nuovo membro della VO
- Accesso ad un VO Service da parte di un membro della VO

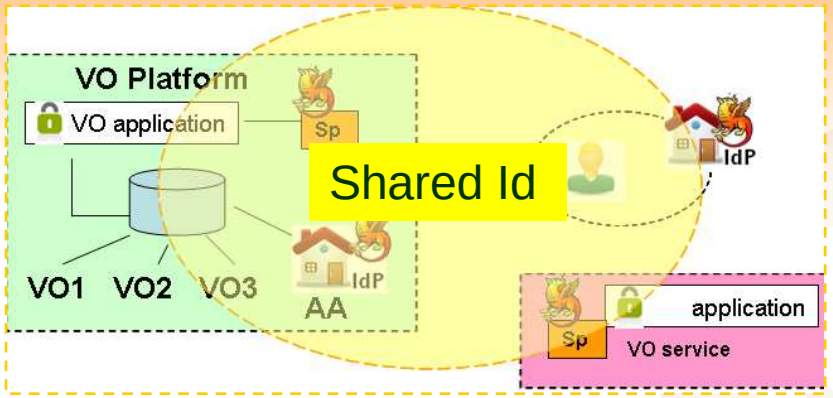
Registrazione nuovo VO member



Accesso ad un VO Service



Shared-Id?



- **A chi deve essere noto?**

  -> Home Org Idp, VO Services, VO Platform

- **Opzione 1:** Attributo identificativo esplicito (es. EdupersonePrincipleName)

  -> Semplice da implementare ma debole dal punto di vista della riservatezza (se le VOs spaziano tra molte organizzazioni si espone a "data correlation attack")

- **Opzione 2:** Attributo pseudonimo (es. EdupersonTargetedID)

  -> Generato dall'Idp per i VO Services di una VO usando l'Affiliation descriptor presente nei metadati

Warning: garantisce maggior riservatezza anche se risulta essere condiviso tra i VO Services di una data VO

Affiliation Descriptor (SAML 2.0)

La VO viene descritta mediante **Affiliation Descriptor** nei metadati condivisi tra Idp (Home), VO Services e VO Platform. Questo meccanismo consente ad un Idp di generare un persistent identifier riferito ad un gruppo di SP (i VO Services) e non solo a un singolo SP.

```
<EntityDescriptor entityID="http://vo.idem.garr.it/cts">
<AffiliationDescriptor affiliationOwnerID="http://vo.idem.garr.it/vop">
<AffiliateMember>http://vo.idem.garr.it/vop</AffiliateMember>
<AffiliateMember>https://aai.caspur.it/GARR-AAI-fed/</AffiliateMember>
<AffiliateMember>http://vconf.garr.it/econfportal/www-aai</AffiliateMember>
</AffiliationDescriptor>
</EntityDescriptor>
```

From…Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0

An entity might alternatively represent an affiliation of other entities, such as an affiliation of service providers. The <AffiliationDescriptor> is provided for this purpose.

Warning! Ritardo nella propagazione dei metadati -> ritardo nella fruizione della VO

Authentication Request from VO Service

La Authentication Request proveniente da un SP associato ad un VO service deve contenere il riferimento alla VO (Entity ID dell'affiliation descriptor) e non allo specifico SP.

```
<samlp:AuthnRequest ID="12345" Version="2.0“ IssueInstant="2010-12-02T1200Z">
<saml:Issuer>https://sp.example.com/SAML2</saml:Issuer>
<samlp:NameIDPolicy SPNameQualifier="http://vo.idem.garr.it/cts "/>
</samlp:AuthnRequest>
```

OASIS

From… Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0
3.4.1 Element <AuthnRequest>
<NameIDPolicy> [Optional]
Specifies constraints on the name identifier to be used to represent the requested subject.
SPNameQualifier [Optional]
Optionally specifies that the assertion subject's identifier be returned (or created) in the namespace of a service provider other than the requester, **or in the namespace of an affiliation group of service providers.**

SPNameQualifier – single VO

Occorre fare in modo che l'SP quando si presenta all'home idp dell'utente indichi per quale affiliazione (VO) viene attivato il servizio. Nel caso di appartenenza a singola VO è sufficiente settare l'attributo "**SPNameQualifier**" nel **Session initiator handler** definito in shibboleth2.xml

```
<SessionInitiator type="SAML2" acsByIndex="false" acsIndex="1"
template="bindingTemplate.html"
SPNameQualifier="https://vo.idem.garr.it/cts"
NameIDFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" />
```

https://spaces.internet2.edu/display/SHIB2/NativeSPSessionInitiator

SPNameQualifier (URI) (Version 2.3 and Above)
If set, causes the authentication request to carry a saml:NameIDPolicy with an SPNameQualifier containing the provided value. If the receiving IdP can not fulfill this requirement, it will return an error response (if correctly implemented)

SPNameQualifier multiple VOs

VO Service solution:

Se un VO Service è acceduto da membri di diverse VOs, cioè se il VO service è affiliato a diverse VOs, occorre far esprimere l'utente chiedendo per quale VO intende presentarsi. In questo caso occorre fare in modo che ci sia una pagina nel VO Service per esprimere la scelta.

SPNameQualifier non viene impostato in shbboleth2.xml ma deve essere impostato "al volo" accedendo ad un SessionInitiator esistente e aggiungendeo SPNameQualifier al suo URL.
e.g. /Shibboleth.sso/DS?SPNameQualifier=https://vo.idem.garr.it/cts

Warning! Necessaria personalizzazione a livello del VO Service -> da manutenere

VO Platform solution:

In alternativa la VOPlatform dovrà fornire un portale che l'utente deve visitare prima di utilizzare ogni servizio allo scopo di far esprimere all'utente la scelta di VO

Home org IdP (Require Affiliation descriptor support)

Il supporto ad Affiliation descriptor introdotto in Shibboleth IdP 2.2 è un prerequisito necessario per l'utilizzo di uno shared-id

```
<samlp:Response Destination="..." ID="..." InResponseTo="..." IssueInstant="..." Version="2.0">
  <saml:Issuer>https://idp.polimi.it/idp/shibboleth</saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:Assertion Version="2.0" ID="..." IssueInstant="...">
    <saml:Issuer>https://idp.polimi.it/idp/shibboleth</saml:Issuer>

    <!-- the shared identifier -->
     <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
E8042FB4-4D5B-48C3-8E14-8EDD852790DD
        </saml:NameID>
     </saml:Subject>
    <saml:AuthnStatement AuthnInstant="..." SessionIndex="..." />
  </saml:Assertion>
</samlp:Response>
```

Quando la richiesta arriva l'Idp Shib 2.2 **verificherà la coerenza tra il name qualifier dato nell'authn request e l'affiliation descriptor presente nei metadati per assicurarsi che l'SP richiedente appartenga all'affiliation dichiarata**. Se tutto ok la richiesta verrà processata come sempre ma lo store ID plugin userà l'affiliation entity ID come target dell'ID invece dell'SP's entity ID.

Simple Attribute Aggregation

Grazie al supporto introdotto da Shib 2.2 per **l'attribute aggregation**, il VO Service, oltre all'Home-Idp dell'utente, può interrogare altri IdPs (Attribute Authority) usando eduPersonTargtedID come NameIdentifier. Ad es:

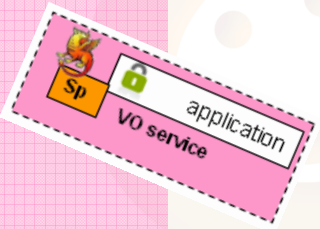
```
Shibboleth2.xml:
<AttributeResolver type="Chaining">
<!-- Use a standard SAML query if no attributes
are supplied during SSO. -->
<AttributeResolver type="Query"/>
<!-- Uses eduPersonTargetedID
from IdP to query as NameID -->
<AttributeResolver
type="SimpleAggregation"
attributeId="eduPersonTargetedID"
format="urn:mace:dir:attribute-def:eduPersonTargtedID">
<Entity>https://vo.idem.garr.it/idp/shibboleth</Entity>
<Entity>https://vo-idp.switch.ch/idp/shibboleth</Entity>
</AttributeResolver>
</AttributeResolver>
```

https://spaces.internet2.edu/display/SHIB2/NativeSPAttributeResolver

Riassumendo…
requisiti per i VO components (Shib based)

VO Service SP:

- Opzione 1 (ePPN come Shared ID) -> Shibboleth 2.2 or newer (implementa simple attribute aggregation)
- Opzione 2 (persistentID as Shared ID) -> Shibboleth 2.3 or newer (implementa il session initiator attribute "SPNameQualifier")

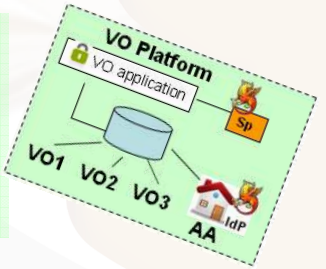


Home Organisation User IdP:

- Opzione 1: Any existing user IdP (including Simple SAML PHP)
- Opzione 2: Shibboleth 2.2 or newer (implementa affiliation descriptor extension)

VO Platform IdP:

- Opzione 1-2: Shibboleth 2.0 or newer (deve supportare Attribute queries)

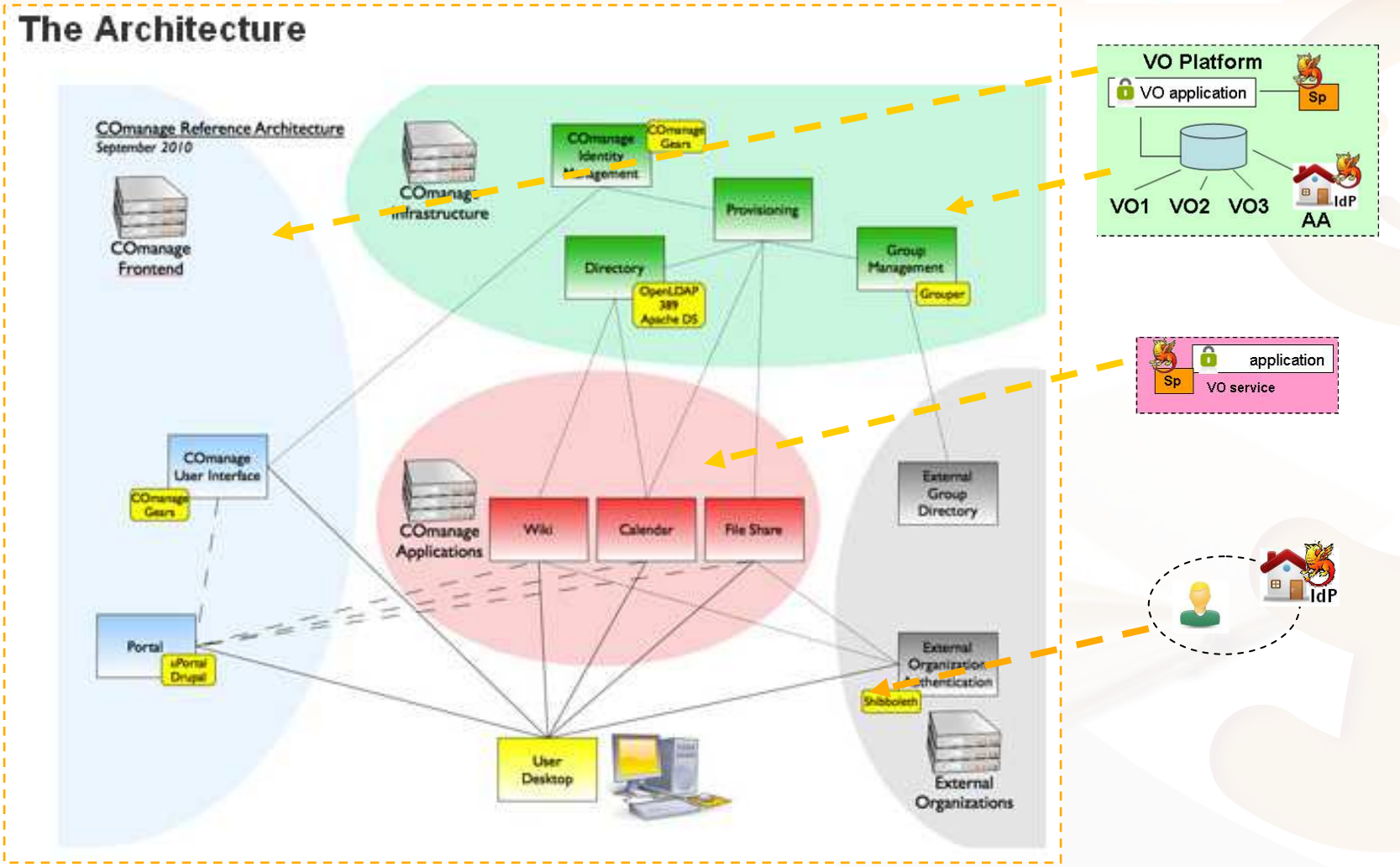


Altre collaboration platform

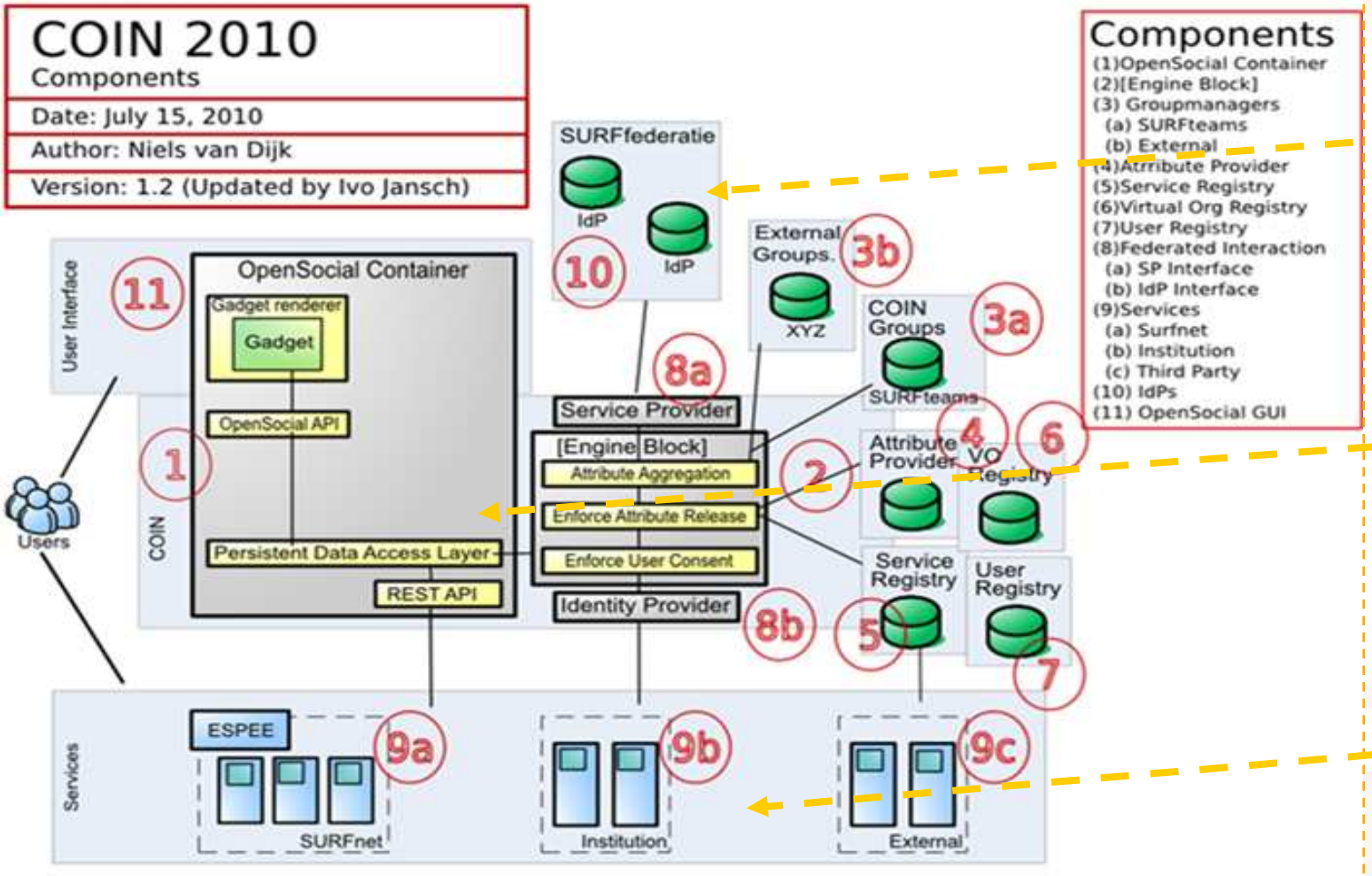
COIN (Surf Net)
https://gui.dev.coin.surf.net/coin/
https://projectcoin.surfnet.nl/

COmanage (Internet2)
http://www.internet2.edu/comanage/

COmanage: Collaborative Organization Management



Coin


COIN 2010
Components
Date: July 15, 2010
Author: Niels van Dijk
Version: 1.2 (Updated by Ivo Jansch)
Components
(1)OpenSocial Container
(2)[Engine Block]
(3) Groupmanagers
(a) SURFteams
(b) External
(4)Attribute Provider
(5)Service Registry
(6)Virtual Org Registry
(7)User Registry
(8)Federated Interaction
(a) SP Interface
(b) IdP Interface
(9)Services
(a) Surfnet
(b) Institution
(c) Third Party
(10) IdPs
(11) OpenSocial GUI
SURFfederatie
IdP
IdP
10
External Groups.
XYZ
3b
COIN Groups
SURFteams
3a
8a
Service Provider
[Engine Block]
Attribute Aggregation
Enforce Attribute Release
Enforce User Consent
Identity Provider
8b
Attribute Provider
4
VO Registry
6
2
Service Registry
5
User Registry
7
User Interface
11
OpenSocial Container
Gadget renderer
Gadget
OpenSocial API
1
COIN
Persistent Data Access Layer
REST API
Users
Services
ESPEE
9a
SURFnet
9b
Institution
9c
External
IdP
VO Platform
VO application
Sp
VO1
VO2
VO3
IdP
AA
application
Sp
VO service

Ringraziamenti

Lukas Hämmerle (SWITCH)
Status update on the SWITCH VO Pilot (Eurocamp - Vienna 23 Novembre 2010)

Niels van Dijk (Surf Net)
The COIN Project (Eurocamp - Vienna 23 Novembre 2010)