Attributs utilisateurs pour la fédération d'identités

Olivier Salaün - CRU

tutoJRES 11

Annuaires : mise en oeuvre de SupAnn 2008

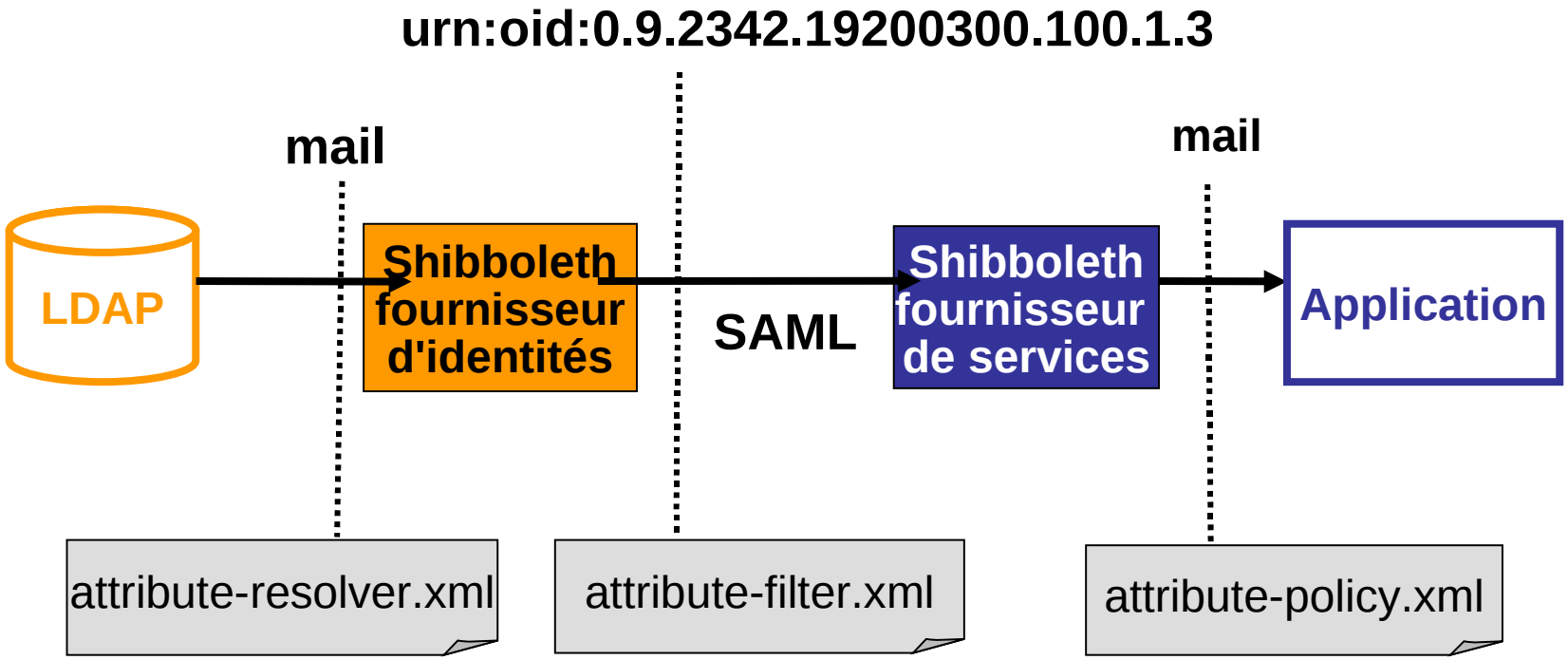
1 avril 2009

Fédération d'identités et SupAnn

1. Branchement Shibboleth et annuaire
   - Voyage d'un attribut dans la fédération
   - Les connecteurs Shibboleth
   - Nouvelles contraintes sur les annuaires
   - La fédération Education-Recherche
2. SAML et attributs
   - Les assertions SAML
   - Les attributs qualifiés
   - Les attributs composites
   - Les attributs calculés

Transfert des attributs en SAML

- Principe de la fédération d'identités
  - Authentifier un utilisateur d'un autre organisme
  - Véhiculer une identité « riche »



Connecteurs d'un fournisseur d'identités Shibboleth

- Variété connecteurs de données Shibboleth
  - JDBC, JNDI (LDAP),
  - Mapping des valeurs : 1->1 ou N->1
  - Script : langage ECMAScript
- On peut les associer
  - Définition de dépendances
- Permet de masquer des spécificités locales

Fédération d'identités et contraintes sur les annuaires

- Ressources fédérées
  - Reposent sur un service d'authentification extérieur
  - Attributs utilisateurs utilisables pour contrôle d'accès
- Contraintes sur les fournisseurs d'identités
  - Niveau authentification
  - Informations à jour (anciens utilisateurs)
  - Nommage des attributs
  - Format des attributs
  - Sémantique des attributs

La fédération Education-Recherche https://federation.renater.fr

- Suite de la fédération du CRU
  - Ouvert aux EPST notamment
  - En cours de migration
- Cadre technique / référentiel attributs
  - SupAnn 2008 + attributs spécifiques fédération
  - Voir https://federation.renater.fr/technique/attributs
- Besoin de chaque ressource fédérée
  - Déclaration des attributs requis/optionnels
  - Chaque organisme configure sa brique Shibboleth IdP

SAML et les attributs utilisateurs

```
<saml:AttributeStatement>

  <saml:Attribute FriendlyName="eduPersonScopedAffiliation"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">

    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">student@renater.fr</
saml:AttributeValue>

  </saml:Attribute>

  <saml:Attribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Jean
Dupont</saml:AttributeValue>

  </saml:Attribute>

  <saml:Attribute FriendlyName="supannEtuInscription" Name="urn:oid:1.3.6.1.4.1.7135.1.2.1.30"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">[etab={UAI}0131843H][anneeinsc=2007][regimeinsc={SISE}10]
[sectdisc={SISE}04][typedip={SISE}YA][cursusann=D3][affect=56R17][diplome={SISE}2001099]
[etape={UAI:0131843H}B8EFAI-B8EFA3]</saml:AttributeValue>

  </saml:Attribute>
```

Les attributs qualifiés

- Exemple eduPersonScopedAffiliation
  - student@univ-x.fr
- Deux attributs de ce type
  - EPScopedAffiliation, EPPrincipalName
- Principe
  - On ajoute le domaine DNS à un attribut
  - Un fournisseur d'identités déclare les domaines qu'il gère dans la fédération
  - Un fournisseur de services vérifie la validité du domaine

Les attributs composites

- Nouveauté de SupAnn 2008
- Principe
  - Corréler plusieurs attributs
- Exemple de SupannRoleEntite
  - [role=supannRoleGenerique] [type=supannTypeEntite][code=supannCodeEntite]
- Indispensable pour la fédération d'identités
  - Les attributs SAML ne sont pas structurés
  - On perd la corrélation, si attribut multivalué
  - Attribut composite évite erreur d'interprétation

Les attributs « calculés » par Shibboleth

- Certains attributs utilisateurs sont/peuvent être calculés par la brique IdP Shibboleth :
  - NameID : identifiant de session SAML
  - EduPersonTargetedID : identifiant persistant, opaque et différent pour chaque application
    - Cet attribut est calculé pour chaque triplet (IdP, utilisateur, SP)
  - EduPersonEntitlement : définit des droits pour une ressource
    - Exemple : urn:mace:dir:entitlement:common-lib-terms

Quid des nouveaux besoins ?

- Attribut supannEtuInscription né du besoin d'une UNT (Université Numérique en Région)
  - Profil étudiant riche (discipline, diplôme, etc.)
- De nouveaux besoins plus ou moins locaux
- Plusieurs options
  - Attribut « maison » ?
  - Allocation de nouveaux OID ?
  - Remontée du besoin à SupAnn ?
  - Attribut stocké dans LDAP ou produit par Shibboleth ?