Comité Réseau des Universités

CRU

Fédération du CRU pour la propagation d'identités et d'attributs

ou

« Comment partager des ressources web entre établissements d'enseignement supérieur »

La fédération du CRU – Montpellier, 13 avril 2005

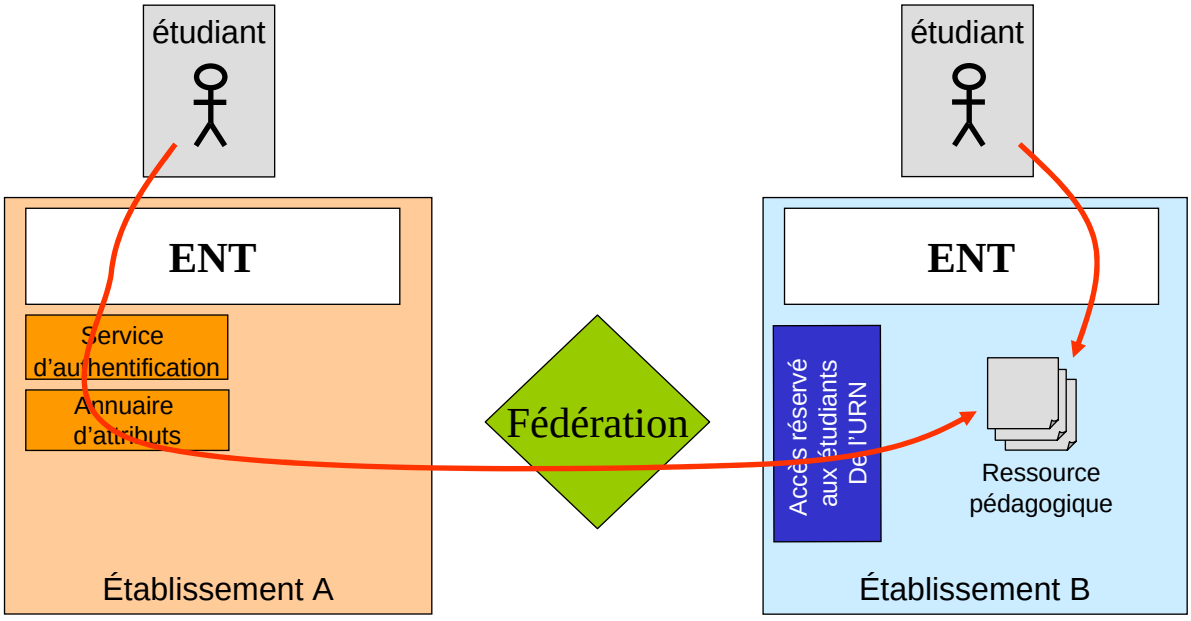
Comité Réseau des Universités

Plan de la présentation

1. **Problématique : délégation de l'authentification**
2. Architecture pour une authentification distribuée
3. Shibboleth, le produit retenu par le CRU
4. La fédération du CRU

Comité Réseau des Universités

Le contexte inter-établissement



Comité Réseau des Universités

Terminologie

- Ressource web = cours en ligne, application, documents (doc. Numérisé, thèse,…)
- Etablissement d'origine = établissement où est enregistré l'utilisateur
- Attributs utilisateur = données concernant l'utilisateur (établissement, formation suivie, identifiant, adresse email,…)

Comité Réseau des Universités

La problématique

- **« Ouvrir l'accès à certaines ressources web à des personnes extérieures à l'établissement »**
- Besoin émergeant dans le contexte des UNR pour l'accès à des ressources pédagogiques
- Pose des problèmes de deux types:
  1. Gestion des identités
  2. Gestion du contrôle d'accès

=> Chacun fait avec des solutions de fortune…

Comité Réseau des Universités

Les solutions simples

1. Accès public, pas de contrôle d'accès
   (Pas toujours adapté…)
2. Pas d'accès du tout, faute de pouvoir contrôler qui accède à la ressource
   (Dommage…)
3. Compte invité partagé par plusieurs utilisateurs
   (Niveau de sécurité très bas)
4. Dupliquer le contenu de la ressource au niveau de chaque établissement
   (Plus de contrôle du fournisseur de contenu)

Comité Réseau des Universités

CRU

Les solutions lourdes

1. Contrôle par adresses IP

   (Inapplicable à des utilisateurs nomades)

2. Enregistrement local des utilisateurs

   (Difficile à gérer)

3. Mise en place d'un meta-annuaire pour l'authentification

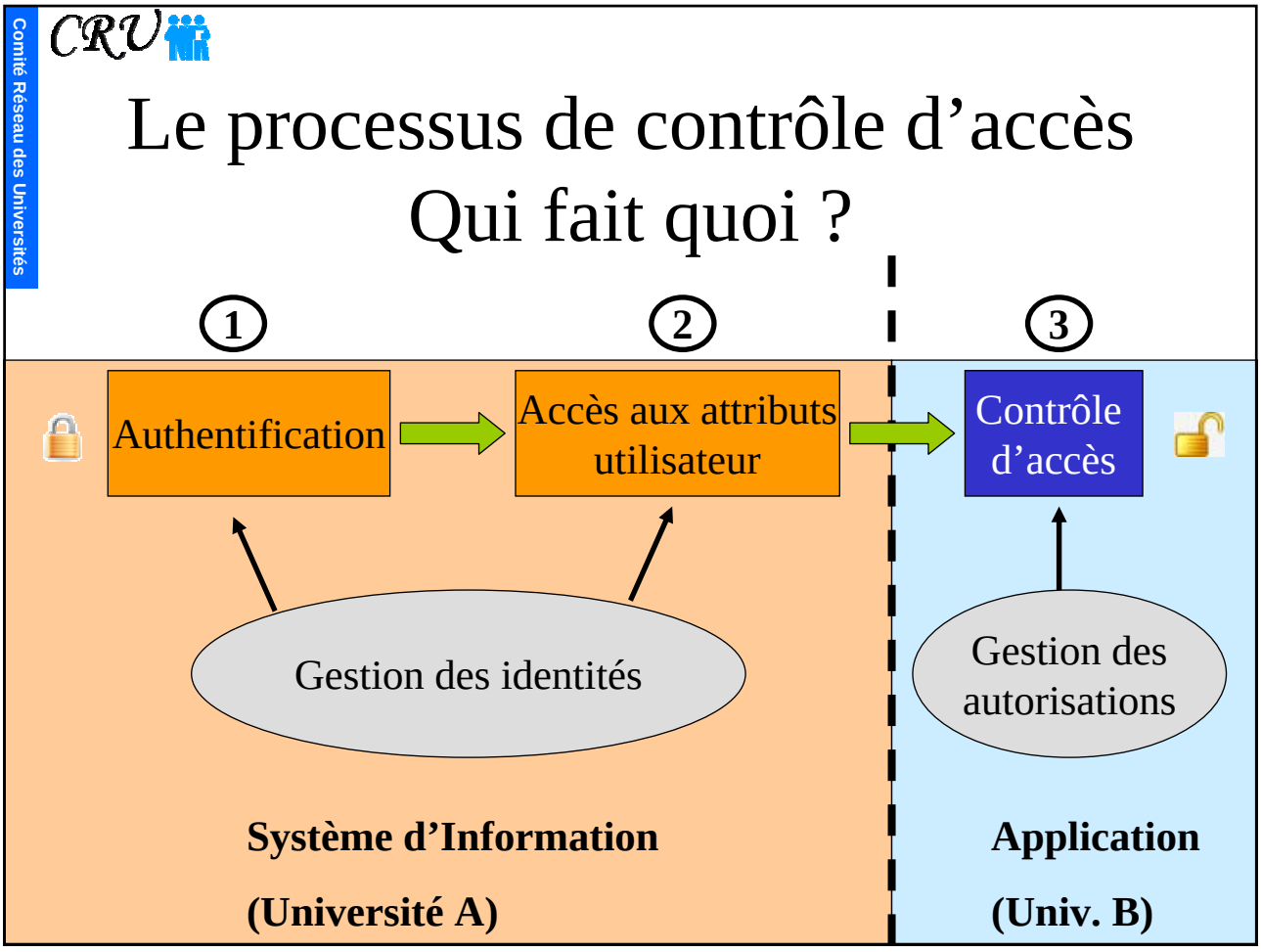
   (Multiplication des meta-annuaires, au gré des partenariats)

Comité Réseau des Universités

CRU

Qui fait quoi ?

- Authentification et gestion des attributs
  - Lourd à gérer au niveau de la ressource
  - L'établissement d'origine le fait déjà (référentiel LDAP, service de Single Sign-On)
- Gestion du contrôle d'accès
  - Valeur ajoutée pour l'organisme fournissant la ressource
  - L'établissement d'origine de l'utilisateur n'est pas habilité à le faire


Comité Réseau des Universités
CRU
Le processus de contrôle d'accès
Qui fait quoi ?
1
2
3
Authentification
Accès aux attributs utilisateur
Contrôle d'accès
Gestion des identités
Gestion des autorisations
Système d'Information
(Université A)
Application
(Univ. B)

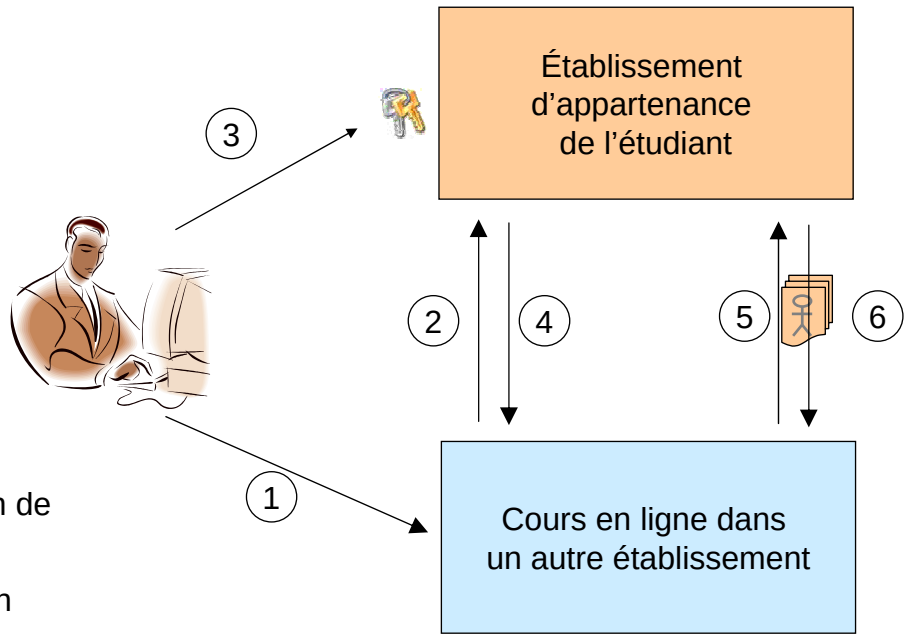
Comité Réseau des Universités

Plan de la présentation

1. Problématique : délégation de l'authentification
2. **Architecture pour une authentification distribuée**
3. Shibboleth, le produit retenu par le CRU
4. La fédération du CRU

Comité Réseau des Universités

Scénario d'utilisation d'une fédération



- 2 et 4 : délégation de l'authentification
- 3 : authentification
- 5 et 6 : propagation d'attributs utilisateur

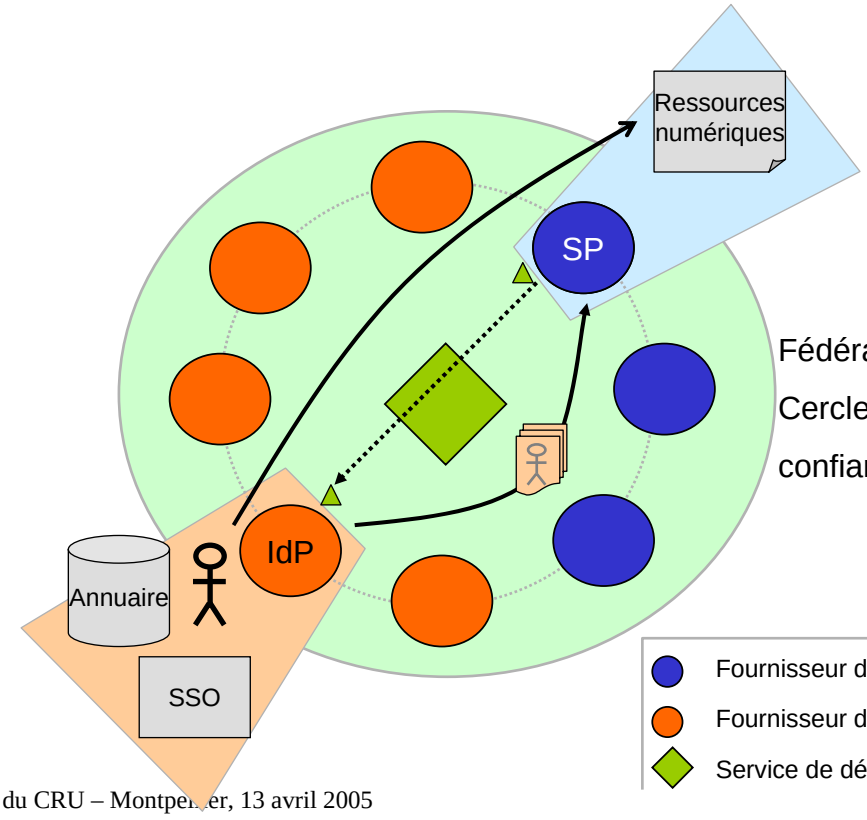
Comité Réseau des Universités

Un aperçu…

- Demo

Comité Réseau des Universités

Structure d'une fédération



Fédération = Cercle de confiance

- Fournisseur de service (SP)
- Fournisseur d'identité (IdP)
- Service de découverte des IdP

Comité Réseau des Universités

CRU

Services rendus par une fédération

- premier service, la **délégation de l'authentification** : quelque soit la ressource numérique à laquelle il essaye d'accéder, un étudiant s'authentifie toujours dans l'ENT de son établissement
- deuxième service, la **propagation d'attributs** : une ressource numérique peut interroger l'établissement d'appartenance de l'étudiant pour obtenir certains de ses attributs, afin d'autoriser ou non son accès
- troisième service, **SSO inter-établissement** : un utilisateur ne s'authentifie qu'une seule fois par session pour l'ensemble des ressources de la fédération

Comité Réseau des Universités

CRU

Intérêts d'une fédération

- Permet de gérer la délégation d'authentification entre :
  - N fournisseurs de services
  - et M fournisseurs d'identités
- La fédération évite la multiplication des relations bilatérale, tout en les permettant
- L'architecture est distribuée donc s'adapte à une échelle nationale

Comité Réseau des Universités

Les bases techniques

- Repose sur le standard SAML pour l'échange d'assertions (authentification, attributs,…)
- Fonctionnement et techniques identiques aux SSO web (redirections, gestion des sessions)
- Une brique centrale : le service de découverte (« Where Are You From »)
- Intégration avec les SI d'établissements :
  - Prolongation (pas remplacement) des systèmes existants (SSO, LDAP…)

Comité Réseau des Universités

CRU

Plan de la présentation

1. Problématique : délégation de l'authentification
2. Architecture pour une authentification distribuée
3. **Shibboleth, le produit retenu par le CRU**
4. La fédération du CRU

Comité Réseau des Universités

Shibboleth

http://shibboleth.internet2.edu

- Développé par Internet2, contexte enseignement / recherche au USA
- Application « open-source », basée sur OpenSAML
- Répond aux besoins d'interconnexion des SSO/LDAP des établissements, sans changer l'existant
- Shibboleth certifié par le gouvernement américain (E-Authentication).

Comité Réseau des Universités

Le choix de Shibboleth

http://federation.cru.fr/pourquoi-shib.html

- Le CRU a évalué Shibboleth et une implémentation de Liberty Alliance (Lasso)
- Nos critères de choix :
  - Maturité de la solution Shibboleth (développement universitaire)
  - Solution adoptée dans plusieurs pays pour la communauté enseignement/recherche
  - Solution non intrusive (s'adapte à l'existant)
  - Pas de produit open-source conforme Liberty Alliance adapté à nos besoins
  - Perspective d'interopérabilité avec SAML 2.0
- Internet2 est membre de Liberty Alliance et participe aux travaux sur SAML (OASIS)

Comité Réseau des Universités

Les autres fédérations académiques

- aux USA, InCommon (http://incommonfederation.org)
- en Suisse, SWITCH AAI (http://www.switch.ch/aai/)
- en Grande-Bretagne (http://sdss.ac.uk/)
- en Norvège (http://www.feide.no/englishwww/doc.html)
- principales applications : cours en ligne, accès à des ressources bibliographiques

Comité Réseau des Universités

CRU

Fonctions au sein de la fédération

- fournisseur d'identité (IdP): établissement gérant des utilisateurs
- fournisseur de service (SP): entité qui propose une ressource en ligne (université, éditeur de contenu…)
- service de découverte : permet à l'utilisateur d'être orienté vers son établissement

- *un même établissement peut exercer à la fois la fonction de fournisseur d'identité et celui de fournisseurs de service<u>s</u>*

Comité Réseau des Universités

Intégration avec l'ENT

- Au niveau de la brique « fournisseur d'identités »
  - L'authentification est déléguée au serveur CAS
  - Extraction des attributs utilisateurs dans l'annuaire LDAP puis exportation
- Au niveau de la brique « fournisseur de services »
  - Récupération des éléments d'authentification et attributs utilisateur
  - L'application cible peut gérer elle-même le contrôle d'accès

Comité Réseau des Universités

Là où s'arrête la fédération

les outils de la fédération ne se substituent pas à un SSO et des référentiels d'attributs

Comité Réseau des Universités

Mise en place de Shibboleth brique « fournisseur d'identités »

- Installation :
  - Application Java (=> Tomcat)
  - Apache en frontal pour gérer la partie SSL (=> mod_jk)
- Configuration :
  - Intégration avec SSO et annuaire LDAP
    - Connecteurs JDBC (SQL) et JNDI (LDAP) disponibles
  - Définition des sites de confiance
  - Définition des attributs à délivrer, en fonction des sites / applications
  - Possibilité d'appartenance à plusieurs fédérations

Comité Réseau des Universités

Exemple : connecteur avec les référentiels d'attributs utilisateurs

```
<AttributeResolver>
        <!– L'adresse email est extraite de l'annuaire LDAP -->
        <SimpleAttributeDefinition id="urn:mace:dir:attribute-def:mail">
                <DataConnectorDependency requires="supann"/>
        </SimpleAttributeDefinition>

        <!– L'élément pédagogique provient de la base apogée -->
        <SimpleAttributeDefinition id="urn:mace:cru.fr:attribute-def:elementPedagogique">
                <DataConnectorDependency requires="apogee"/>
        </SimpleAttributeDefinition>

        <JNDIDirectoryDataConnector id="supann">
                <Search filter="cn=%PRINCIPAL%">
                        <Controls searchScope="SUBTREE_SCOPE" returningObjects="false" />
                </Search>
                <Property name="java.naming.factory.initial" value="com.sun.jndi.ldap.LdapCtxFactory" />
                <Property name="java.naming.provider.url" value="ldap://ldap.univ-test.fr/dc=univ-test,dc=fr" />
                <Property name="java.naming.security.principal" value="cn=etu,dc=univ-test,dc=fr" />
                <Property name="java.naming.security.credentials" value="passwd" />
        </JNDIDirectoryDataConnector>

        <JDBCDataConnector id="apogee" minResultSet="1" maxResultSet="1"
                dbURL="jdbc:oracle:apogee:user/passwd@dbhost.univ-test.fr"
                dbDriver="oracle.jdbc.driver.OracleDriver""
                maxActive="10"     maxIdle="5">
                <Query>SELECT IND_CONTRAT_ELP.COD_ELP
                FROM APOGEE.IND_CONTRAT_ELP IND_CONTRAT_ELP, APOGEE.INDIVIDU INDIVIDU
                WHERE INDIVIDU.COD_IND = IND_CONTRAT_ELP.COD_IND AND INDIVIDU.COD_ETU = ?</Query>
        </JDBCDataConnector>
</AttributeResolver>
```

Comité Réseau des Universités

Mise en place de Shibboleth brique « fournisseur de services »

- Installation :
  - Module pour Apache (RPM dispo.) et module pour IIS
  - ou application Java en version beta
- Configuration :
  - Définition de la fédération et sites de confiance
  - Définition des attributs requis
  - Le module peut gérer le contrôle d'accès :

    require affiliation student@univ-test.fr student@autreuniv-test.fr
  - Une seule instance peut suffire à plusieurs applications

Comité Réseau des Universités

Les applications déjà compatibles
http://shibboleth.internet2.edu/seas.html

- Applications :
  - Blackboard
  - Napster
  - Sympa
  - TWiki
  - WebCT
  - Zope4Edu
  - ...
- Fournisseurs de contenus :
  - Elsevier ScienceDirect
  - JSTOR (Journal Storage)
  - OCLC (Online Computer Library Center)

Comité Réseau des Universités

Exemple d'intégration avec le serveur de listes *Sympa*

- Cohabitation de *Shibboleth* avec le service d'authentification natif de *Sympa*
- Utilisation du module pour *Apache mod_shib*, protégeant une sous-URL de l'interface web de Sympa
- En plus de l'adresse email de l'utilisateur, *Sympa* a accès à d'autres attributs qu'il peut exploiter pour gérer le contrôle d'accès.
  - Exemple d'usage : montrer une catégorie de liste, uniquement à des étudiants suivant une formation associée

Comité Réseau des Universités

Evolution de Shibboleth

- Shibboleth 1.2.1 (décembre 2004)
  - Version utilisée pour la fédération du CRU
- Shibboleth 2.0 (prévu fin 2005)
  - Version majeure, basée sur SAML 2.0, donc *a priori* inter-opérable avec Liberty Alliance

Comité Réseau des Universités

Plan de la présentation

1. Problématique : délégation de l'authentification
2. Architecture pour une authentification distribuée
3. Shibboleth, le produit retenu par le CRU
4. **La fédération du CRU**

Comité Réseau des Universités

CRU

La fédération du CRU

- le Comité Réseau des Universités opère une fédération pour les établissements d'enseignement supérieur
- Nos activités dans le cadre de la fédération :
  - mise en place d'un *cercle de confiance* regroupant des établissements volontaires,
  - définition des relations de confiance,
  - assistance technique aux établissements,
  - gestion du *service de découverte*

Comité Réseau des Universités

Gestion de la confiance au sein de la fédération

- Gestion d'une **liste des sites de confiance** partagée au sein de la fédération (+ relations bilatérales)
- Gestion locale de la **politique de délivrance des attributs utilisateurs**, configuré en fonction du site interlocuteur

- ces 2 éléments sont paramétrables au niveau de chaque brique (SP, IdP)

Comité Réseau des Universités

Exemple : liste des sites de confiance

```
<!--  Extrait de cru-sites.xml -- >
<SiteGroup Name="urn:mace:cru.fr:federation" xmlns="urn:mace:shibboleth:1.0">
      <OriginSite Name="urn:mace:cru.fr:federation:univ-test.cru.fr" >
            <Alias>Université de test</Alias>
            <Contact Type="technical" Name="Admin fédération" Email="federation-admin@cru.fr"/>
            <HandleService Location="https://federation.cru.fr/univ-test/HS" Name="federation.cru.fr"/>
            <AttributeAuthority Location="https://federation.cru.fr/univ-test/AA" Name="federation.cru.fr"/>
            <Domain>federation.cru.fr</Domain>
      </OriginSite>

      <OriginSite Name="urn:mace:cru.fr:federation:idp.cru.fr" ErrorURL="http://www.cru.fr/ciboulette/error.html">
            <Alias>Comité Réseau des Universités</Alias>
            <Contact Type="technical" Name="Admin fédération" Email="federation-admin@cru.fr"/>
            <HandleService Location="https://www.cru.fr/ciboulette/HS" Name="www.cru.fr"/>
            <AttributeAuthority Location="https://www.cru.fr/ciboulette/AA" Name="www.cru.fr"/>
            <Domain>www.cru.fr</Domain>
      </OriginSite>

      <DestinationSite Name="https://federation.cru.fr/sp-test">
            <Alias>Service Provider de test</Alias>
            <Contact Type="technical" Name="Admin fédération" Email="federation-admin@cru.fr"/>
            <AssertionConsumerServiceURL Location="https://federation.cru.fr/Shibboleth.shire"/>
            <AttributeRequester Name="federation.cru.fr"/>
      </DestinationSite>
</SiteGroup>
```

La

Comité Réseau des Universités

Exemple : politique de délivrance des attributs utilisateurs

```
<!– extrait de arp.site.xml -- >
<AttributeReleasePolicy xmlns="urn:mace:shibboleth:arp:1.0" >
      <Description>Exemple de politique</Description>
      <Rule>
            <Target>
                  <AnyTarget/>
            </Target>
            <Attribute name="urn:mace:dir:attribute-def:mail">
                  <AnyValue release="permit"/>
            </Attribute>
            <Attribute name="urn:mace:dir:attribute-def:eduPersonPrincipalName">
                  <AnyValue release="permit"/>
            </Attribute>
            <Attribute name="urn:mace:cru.fr:attribute-def:supannOrganisme">
                  <AnyValue release="permit"/>
            </Attribute>
            <Attribute name="urn:mace:cru.fr:attribute-def:supannRole">
                  <AnyValue release="permit"/>
            </Attribute>
      </Rule>
</AttributeReleasePolicy>
```

La

Comité Réseau des Universités

CRU

Participation à plusieurs fédérations

Un *fournisseur d'identités* peut s'intégrer dans plusieurs fédération, et également gérer des relations bilatérales

- Pour chaque contexte, on peut définir :
  - La liste des sites de confiance
  - Une politique de délivrance des attributs
  - Le référentiel pour les attributs utilisateurs

Comité Réseau des Universités

L'importance du nommage dans le cadre de la fédération

- Outre l'usage de certificats X.509, on base en grande partie la confiance sur :
  1. Les identifiants des sites (ProviderId)
  2. Les identifiants des attributs et leur sémantique
- Le CRU gère un service de nommage qui fournit des URN uniques dans l'espace de nommage :
  - Exemples :
    - urn:mace:cru.fr:federation:univ-test.fr
    - urn:mace:cru.fr:attribute-def:supannRole

Comité Réseau des Universités

CRU

Nécessité d'un jeu commun d'attributs

- les partenaires s'échangent des attributs utilisateurs
- il faut donc une nomenclature commun des attributs pour les échanger dans le cadre de la fédération
- un IdP et un SP peuvent définir une correspondance entre cette nomenclature et leur nomenclature interne

Comité Réseau des Universités

Un jeu d'attributs communs

http://federation.cru.fr/attributs.html

- Des attributs hérités de *eduPerson* :
  - mail, eduPersonPrincipalName, eduPersonAffiliation,
- Des attributs hérités de *supAnn* :
  - supannOrganisme, supannRole, supannAffectation
- Des attributs fournit par *Shibboleth* :
  - eduPersonTargetedID, originSite, authenticationMethod
- Des informations pédagogiques à définir (SISE, Eurydice) :
  - Cours, formation, étape,…

Comité Réseau des Universités

Etat d'avancement du projet

http://federation.cru.fr

- Documentation de l'architecture
- Documentation pour la mise en œuvre (SP et IdP)
- Définition des meta-données (sites.xml, trust.xml, attributs)
- Service de découverte de la fédération
- Services de test (découverte + SP) pour aide à la mise en place
- Réflexion concernant l'interopérabilité avec d'autres fédérations (contexte Terena)

Comité Réseau des Universités

Formalisation des relations de confiance ?

- contexte de sécurité : délégation d'authentification et diffusion d'attributs
- plusieurs degrés de formalisation de la confiance entre les participants :
  - charte de bonnes pratiques
  - convention
  - contrat…
- phase initiale de la fédération du CRU : aucun formalisme pour le moment

Comité Réseau des Universités

CRU

Comment participer…

- Pour un *fournisseur d'identités* :
  - Obtention d'un certificat du *CRU* pour le serveur
  - Installation de la brique shibboleth-origin
  - Enregistrement auprès du service de test pour valider l'installation auprès du *SP* de test
  - Configuration des connecteurs avec le SI + configuration de la politique de confiance
  - Enregistrement dans la fédération du *CRU*

Comité Réseau des Universités

Comment participer…

- Pour un *fournisseur de services* :
  - Obtention d'un certificat du *CRU* pour le serveur (options TLS requises incluses automatiquement)
  - Installation du module *shibboleth* pour *Apache* (ou *IIS*)
  - Enregistrement auprès du service de test pour valider l'installation auprès de l'*IdP* de test
  - Configuration de l'application pour exploiter les attributs utilisateurs (champs d'entête HTTP)
  - Enregistrement dans la fédération du *CRU*

Comité Réseau des Universités

Evaluation des besoins

http://federation.cru.fr/doc/questionnaires.html

- Le CRU a mis au point 2 questionnaires, utilisables par les établissements pour évaluer les besoins pour un *fournisseur d'identités* et un *fournisseur de services*

Merci de nous remonter les infos…

Comité Réseau des Universités

CRU

Questionnaire
fournisseur de services

1. Description de la ressource : pédagogique, bibliographique, autre...
2. Quel établissement gère cette ressource ?
3. Quel est le responsable chargé de cette ressource (interlocuteur 'chef du projet') ? (nom + email)
4. Quel est le responsable de la plate-forme technique hébergeant la ressource (interlocuteur 'technique') ? (nom + email)
5. Quelle est la population accédant à cette ressource (actuellement ou dans le futur) :
   - type de population (ex: étudiant, personnel, autres)
   - origine (ex: établissement, ville, région, national, international)
6. Y aurait-il un intérêt à ouvrir cette ressource à des populations plus ciblées ?
7. Comment est géré actuellement le contrôle d'accès ? (aucun, adresses IP, comptes invités)
8. Quelles sont les contraintes de sécurité pour l'accès à la ressource (par exemple existe-t-il plusieurs niveaux d'authentification) ?
9. S'il y a un contrôle d'accès, comment est-il administré : qui récupére les infos, qui les met à jour... ?
10. Pouvez-vous indiquer les informations concernant l'utilisateur nécessaires pour lui octroyer l'accès ? par ex. : niveau d'études, établissements d'origine...
11. Quelles sont les limites du système actuel ?
12. Quelles sont les évolutions envisagées ?

La

Comité Réseau des Universités

Questionnaire
fournisseur d'identités

1. Nom de l'entité ?
2. Quel est le responsable de la plate-forme technique hébergeant la ressource (interlocuteur 'technique') ? (nom + email)
3. Y a-t-il un annuaire LDAP réunissant tous les personnels et/ou étudiants ?
4. Dans quelle mesure est-il conforme SUPANN ?
5. Y a-t-il un identifiant unique pour chaque utilisateur ? Si oui lequel ?
6. Comment sont gérés les groupes et attributs des utilisateurs ?
7. Quelles sont les procédures administratives d'enregistrement et de mise à jour de l'annuaire ou du référentiel source (par ex. base Apogée) ?
8. Existe-il une base centrale d'authentification ?
9. Existe-il un service central d'authentification (SSO) ? Si oui lequel (indiquer l'URL du produit) ?
10. Quelles sont la ou les méthodes d'authentification (mot de passe, OTP, certificats...) ?

Comité Réseau des Universités

CRU

Implication des établissements dans le projet

- Projet pilote dans le contexte UNR Bretagne ; en cours de test
- Groupe de travail (Université de Nancy, ENS Lyon, Rennes 1,…)

Vous êtes les bienvenus (expression de besoins, déploiement, test,…)

Comité Réseau des Universités

Contacts

federation-admin@cru.fr

federation-groupe@cru.fr

http://federation.cru.fr