Application de la fédération d’identités pour l’authentification réseau

Philippe.Arnould@univ-pau.fr

Anthony.Hinsinger@univ-pau.fr

Plan

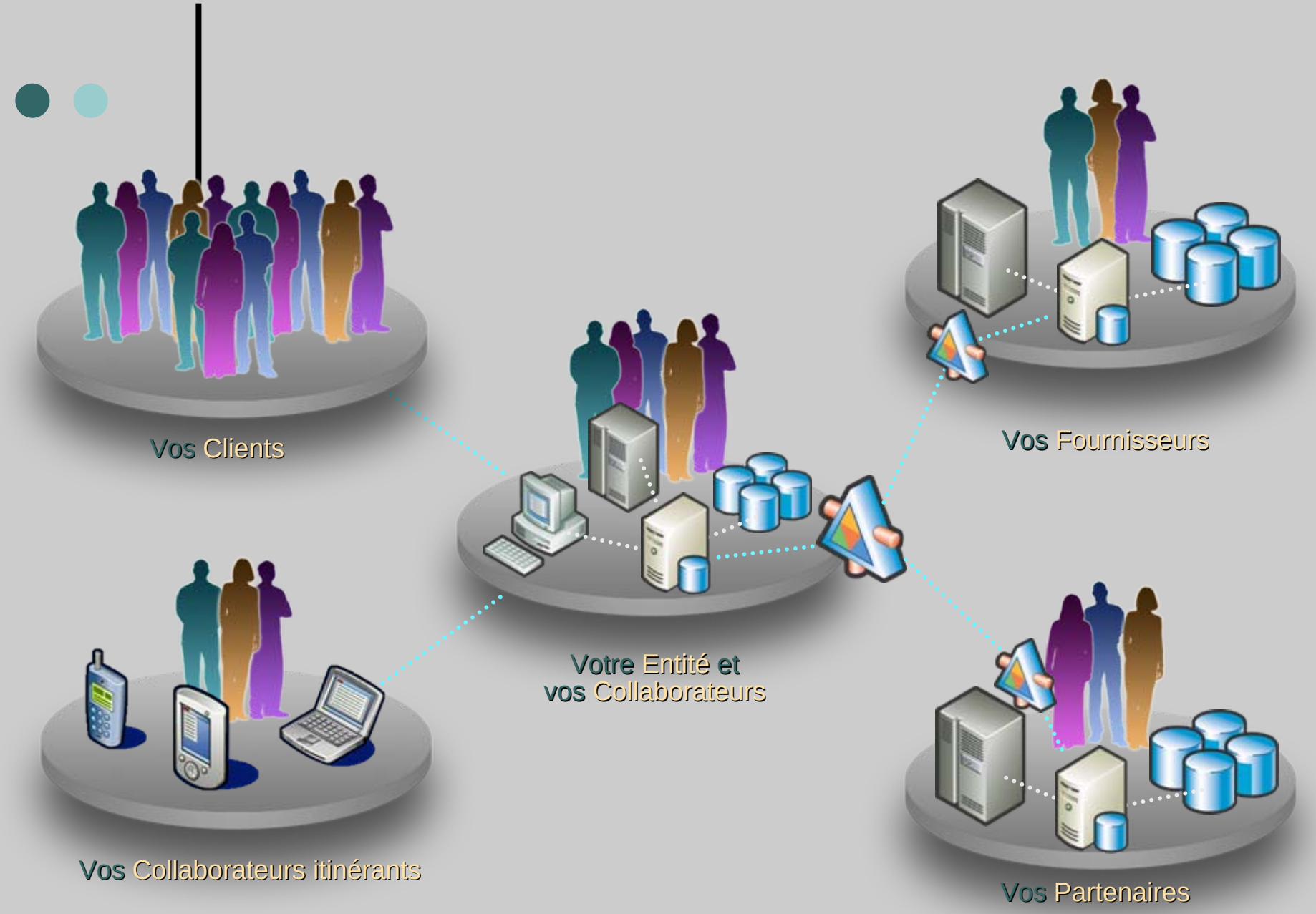
- Fédération d’identités
- Problématique de de l’authentification réseau
- Chilibboleth : utilisation de Shibboleth pour l’authentification et la gestion d’attributs
- Conclusion

Pourquoi authentification réseau

- 60 bornes wifi installées
- Sites multi-établissements
- Simplicité de mise en œuvre des postes clients
  - Authentification basée sur le login et mot de passe des utilisateurs (étudiants, personnels) stockées dans un annuaire.
  - Solution « portail captif »
- Mise en œuvre d'un ENT (ACO) avec un SSO
- Comment ne pas multiplier les saisies :
  - Utilisation du mécanisme de fédération d'identité en liaison avec le SSO:
    - Cookie permet de ne pas se re-authentifier sur le portail
    - Mécanisme d'authentification des utilisateurs extérieurs

Fédération d’identités

- Déploiement des services web
- Nécessité interconnecter les référentiels authentification
- Entreprises, établissements publics


Vos Clients
Votre Entité et
vos Collaborateurs
Vos Fournisseurs
Vos Collaborateurs itinérants
Vos Partenaires

Fédération d’identités

- La fédération d’identité répond au besoin d’interconnecter les systèmes authentification en utilisant :
  - la délégation de l’authentification
  - la propagation d’attributs utilisateur

Fédération d’identités

- La délégation d’authentification
  - consiste à utiliser le service d’authentification proposé par l’établissement de rattachement de l’utilisateur
  - En utilisant les mécanismes standard du web : redirection http, javascript et cookies
  - Ce qui permet de pouvoir fournir un service sans avoir à gérer les comptes utilisateurs.

Fédération d’identités

- Propagation d’attributs:
  - Cela permet après authentification à récupérer certains attributs relatifs à l’utilisateur à partir de l’établissement d’origine:
    - Nom, prénom, email
    - Catégorie d’utilisateurs, rôles,…

Fédération d’identités

- Exemples d’utilisation
  - Accès aux périodiques en ligne
  - Gestion d’un intranet entre plusieurs établissement
  - Authentification réseau…

Fédération d’identités

- Solutions techniques
  - Accès par compte générique, par IP, certificats, méta annuaire -> difficile à gérer
  - SAML : Security Assertion Markup Language
    - Standard OASIS
    - Permet de transmettre sous la forme d’un document xml qu’un utilisateur à été correctement authentifié par tel établissement
  - SAML sert de support à deux autres normes
    - Shibboleth
    - Liberty Alliance

Fédération d'identités
Exemple SAML

```
<saml:Assertion
        MajorVersion="1"
        MinorVersion="0"
        AssertionID="128.9.167.32.12345678"
        Issuer="Comite Reseau des Universites"
        IssueInstant="2002-03-21T10:02:00Z">
        <saml:Conditions
                NotBefore="2002-03-21T10:02:00Z"
                NotAfter="2002-03-21T10:07:00Z" />
                <saml:AuthenticationStatement
                AuthenticationMethod="password"
                AuthenticationInstant="2002-03-21T10:02:00Z">
        <saml:Subject>
        <saml:NameIdentifier
                SecurityDomain="www.cru.fr"
                Name="dupont" />
                </saml:Subject>
        </saml:AuthenticationStatement>
</saml:Assertion>
```

Fédération d’identités
Exemple SAML

Authentification SAML

- SAML ne sert pas à authentifier l’utilisateur mais à communiquer le fait qu’il a été correctement authentifié.
- L’assertion contient ici des informations sur la date et le mode d’authentification, et possède une durée de validité limitée.

Fédération d’identités

- Shibboleth :
  - Développé depuis 2001 par internet2
  - Désigne à la fois une norme et le produit open source
  - C’est une extension de SAML en introduisant:
    - La délégation d’authentification
    - La propagation d’attributs

Fédération d’identités

- Liberty Alliance
  - Consortium d’entreprise fondé en 2001
  - Produit plusieurs spécifications :
    - ID-FF : Identity Fédération framework :
      - federation comptes,
      - Délégation authentification, propagation en fin de session
    - ID-WSF : Identity-based Web services :
      - Propagation d’attributs
  - Nombreux produits propriétaires et open source l’utilisent

Fédération d’identités

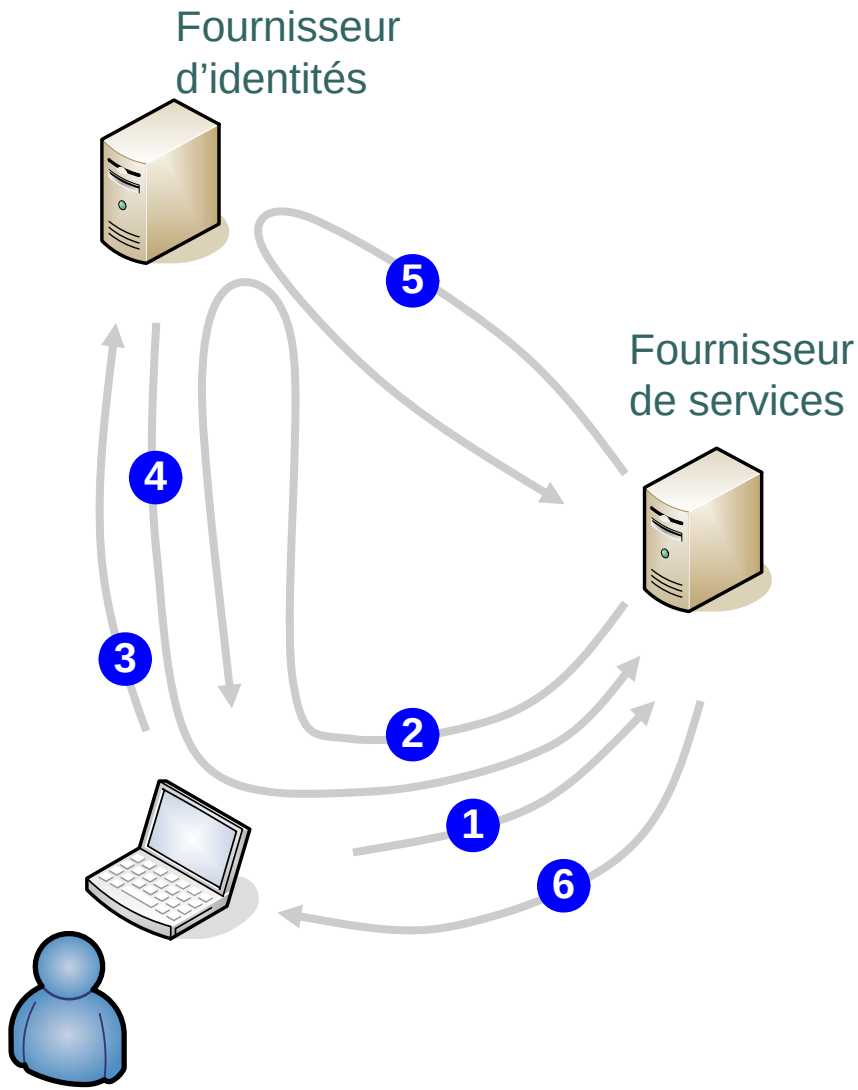
- Choix des universités
  - Shibboleth
- Choix de Agence pour le développement de l'administration électronique (ADAE):
  - Liberty Alliance

Shibboleth

- Architecture
  - Navigateur : User agent
  - Fournisseur de services Service Provider
    - Entité proposant des ressources web dans un contexte SAML
    - Noté SP
  - Fournisseur d’identité Identity Provider
    - Entité authentifiant les utilisateurs et fournissant les attributs
    - Noté IdP
  - WAYF Where Are You From ?
    - Orienter l’utilisateur vers son fournisseur d’identité (IdP).

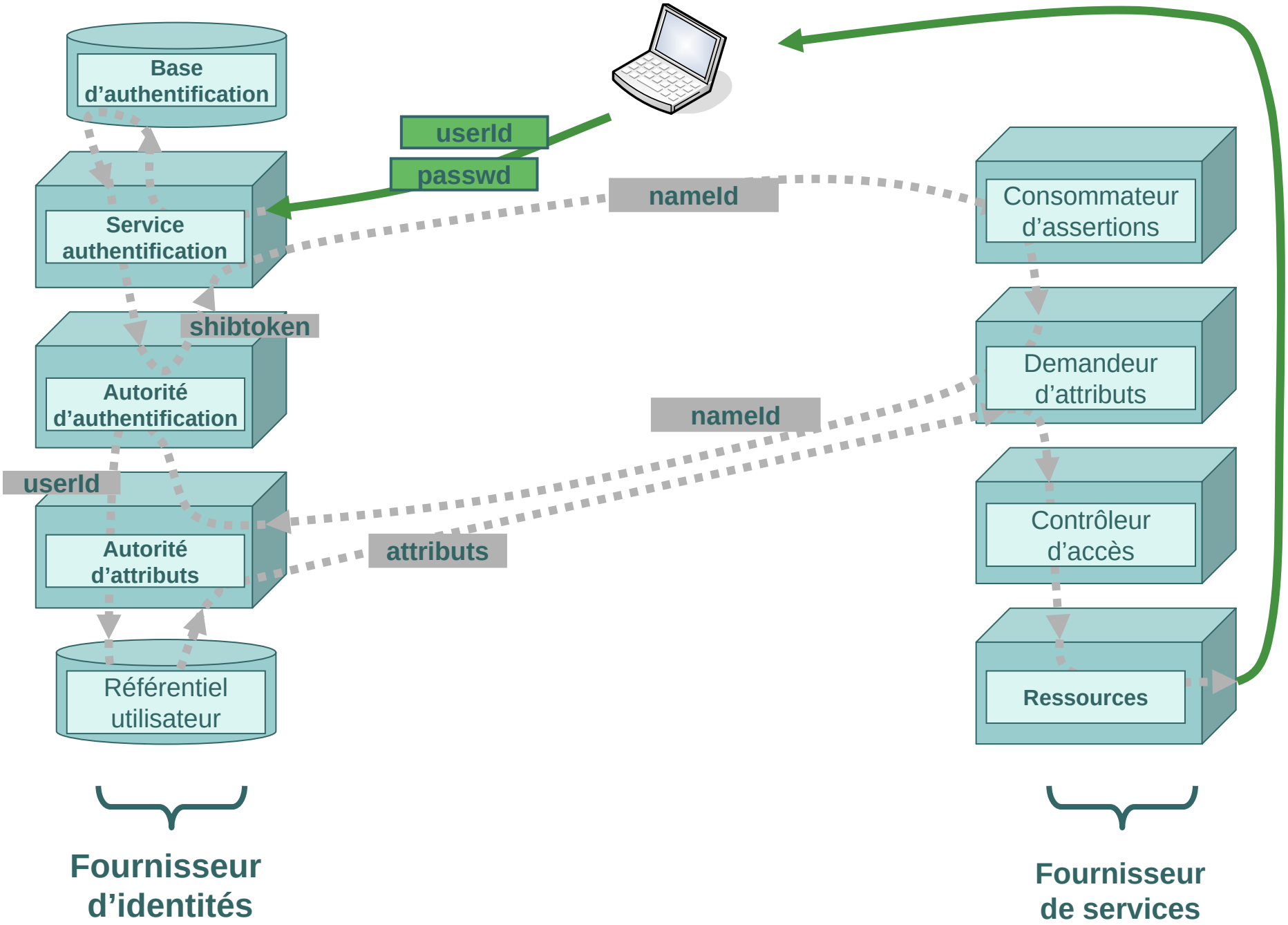
Shibboleth

1. L'utilisateur UA effectue une requête http vers le fournisseur de services
2. Le SP, sans information d'authentification, redirige vers l'IdP de l''utilisateur
3. Sans SSO, la réponse de IdP est une demande d'authentification, l'utilisateur fournit **userID** et **passwd**
4. Une fois authentifié, l'IdP alors le navigateur Vers le SP, accompagné d'une assertion SAML signée contenant un identifiant **nameId**
5. Récupération des attributs en utilisant **nameId**
6. Le SP peut alors faire le contrôle d'accès en utilisant éventuellement les attributs



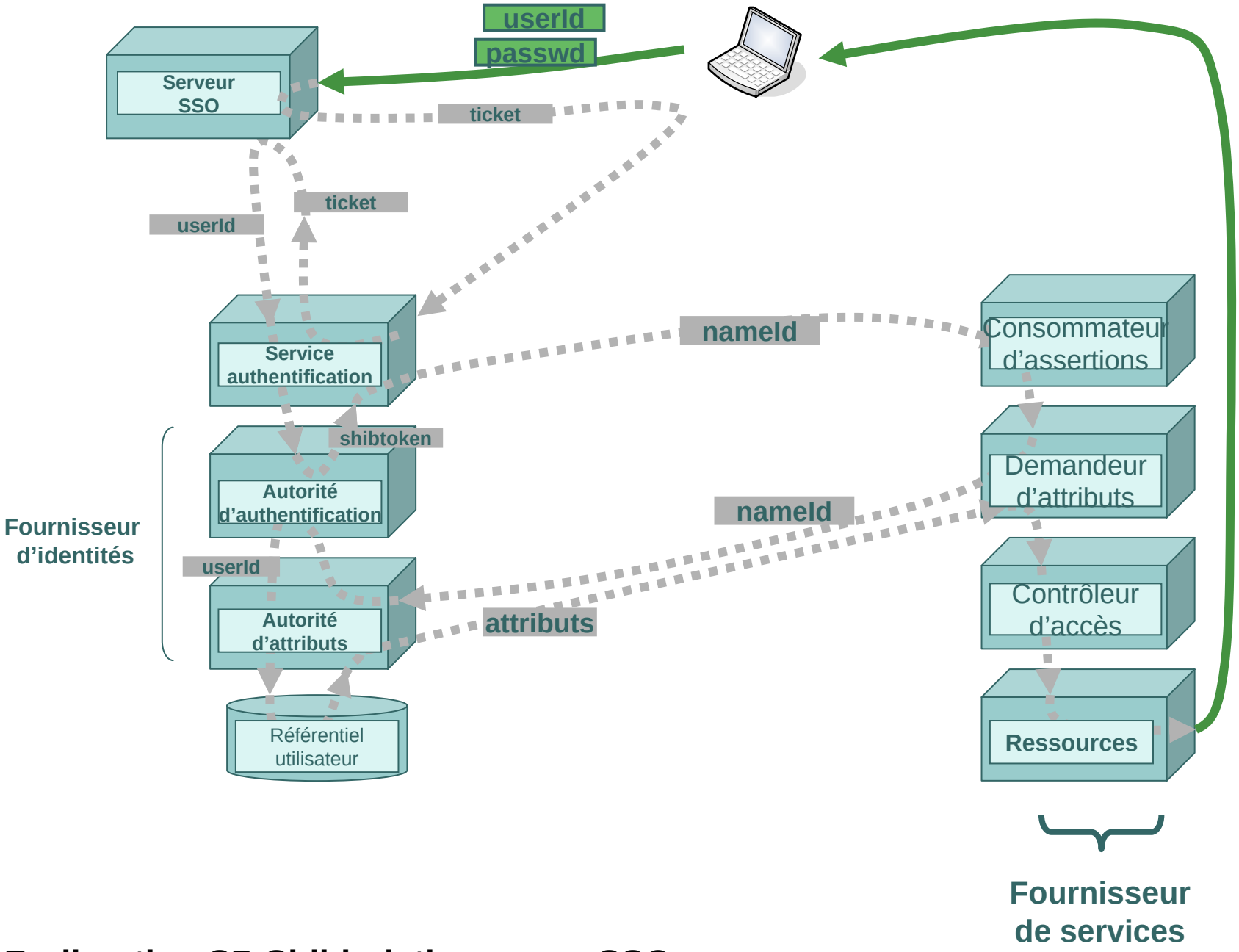
Architecture de Shibboleth

- Fournisseur de services
  - Le consommateur d’assertions
  - Le demandeur d’attributs
  - Le contrôleur d’accès
- Fournisseur d’identités
  - Service authentification
  - Autorité d’authentification
  - Autorité d’attributs

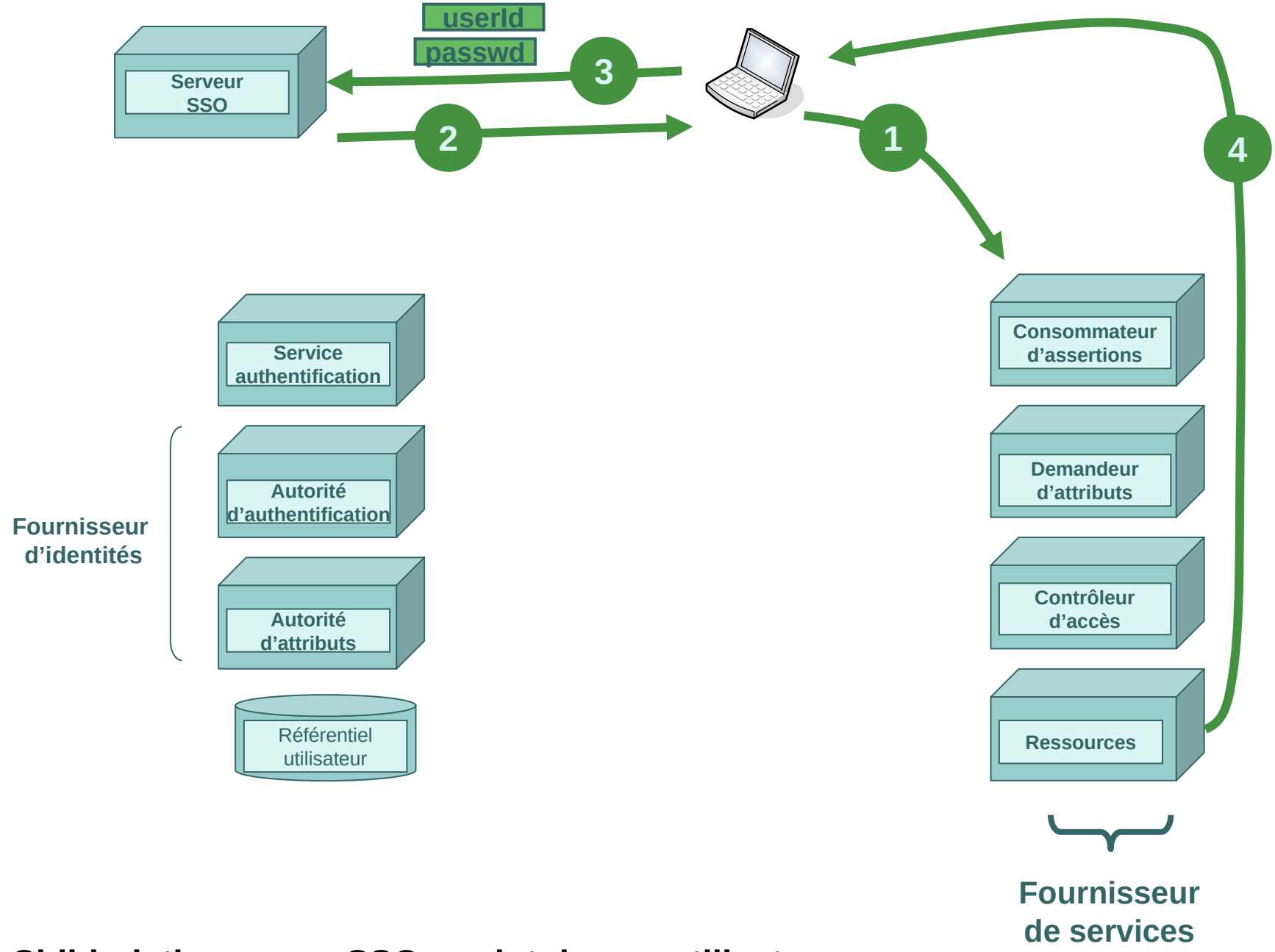

Base d'authentification
Service authentification
Autorité d'authentification
Autorité d'attributs
Référentiel utilisateur
userId
passwd
nameId
shibtoken
userId
nameId
attributs
Consommateur d'assertions
Demandeur d'attributs
Contrôleur d'accès
Ressources
Fournisseur d'identités
Fournisseur de services

Shibboleth avec un SSO

- SSO Single Sign On
  - Authentifier une seule fois un utilisateur pour accéder à un ensemble d'applications.
- Avantages:
  - Session d'authentification partagée par toutes les applications web
  - Apport ergonomique :
    - un seul mot de passe
    - Saisi une seule fois
    - à un seul endroit
  - Portails
  - Sécurité
  - Gestion des comptes
  - Meilleure intégration avec le SI
- Kerberos, CAS,…



Redirection SP Shibboleth avec un SSO

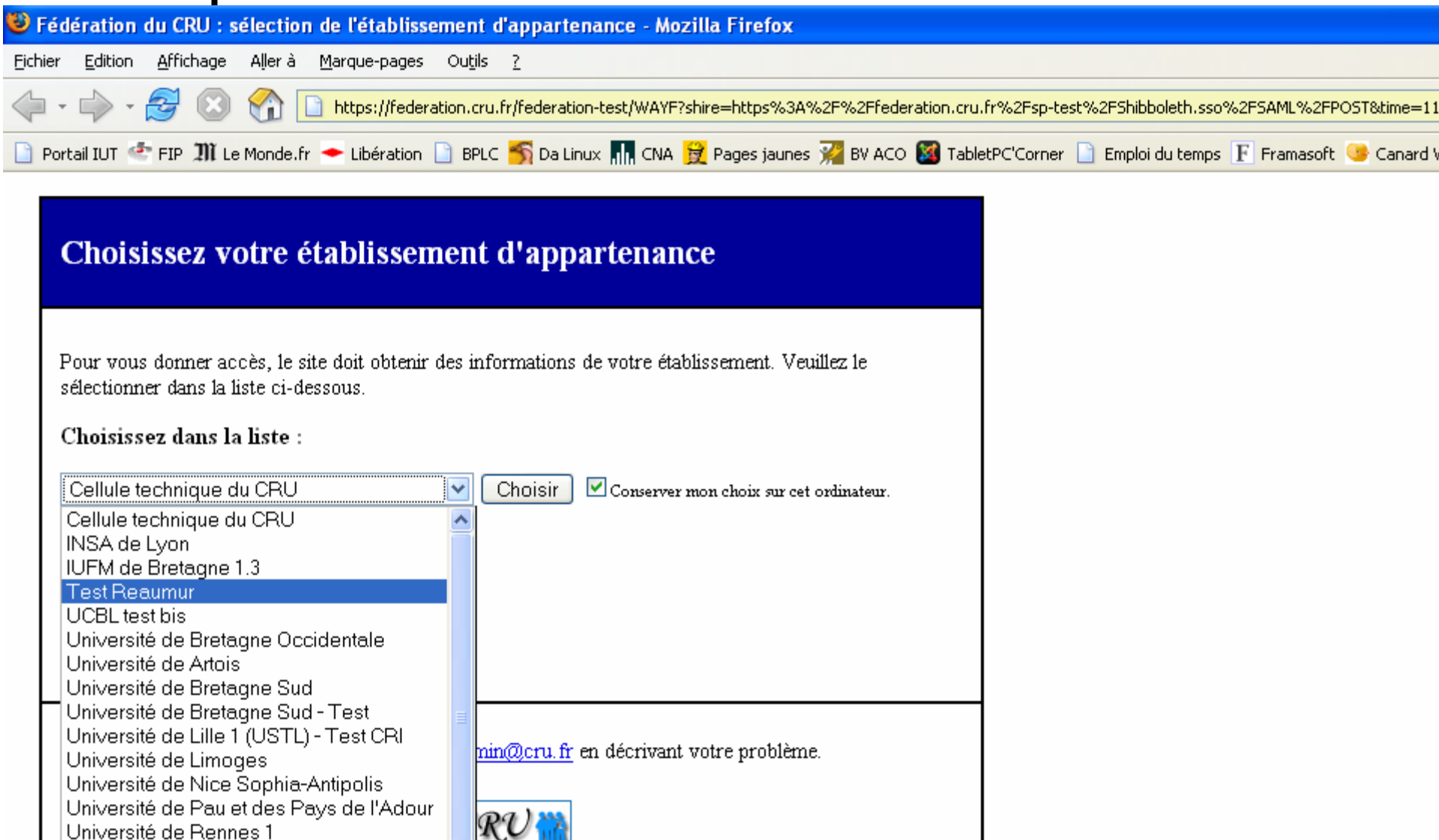


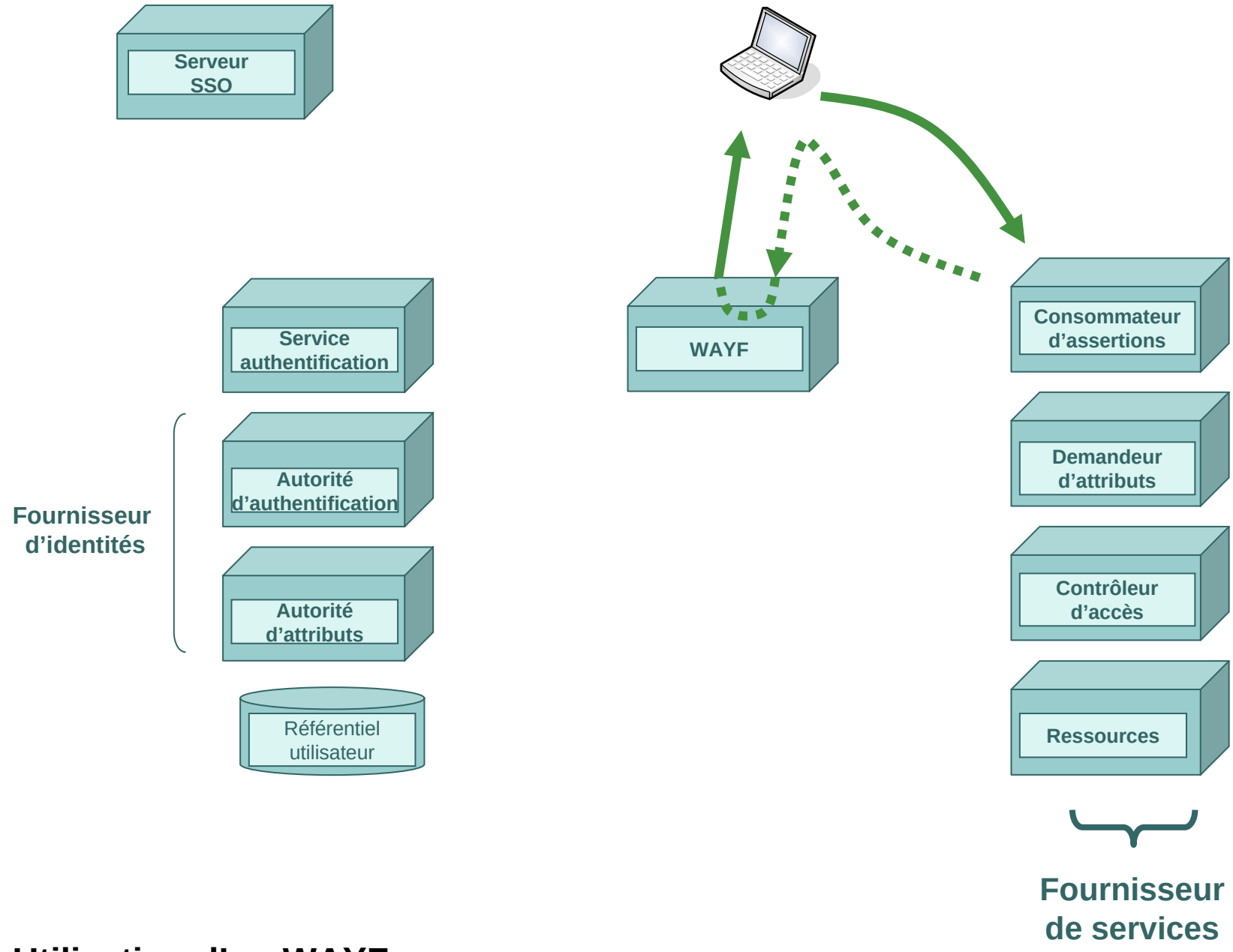
Shibboleth avec un SSO : point de vue utilisateur

Utilisation d’un WAYF

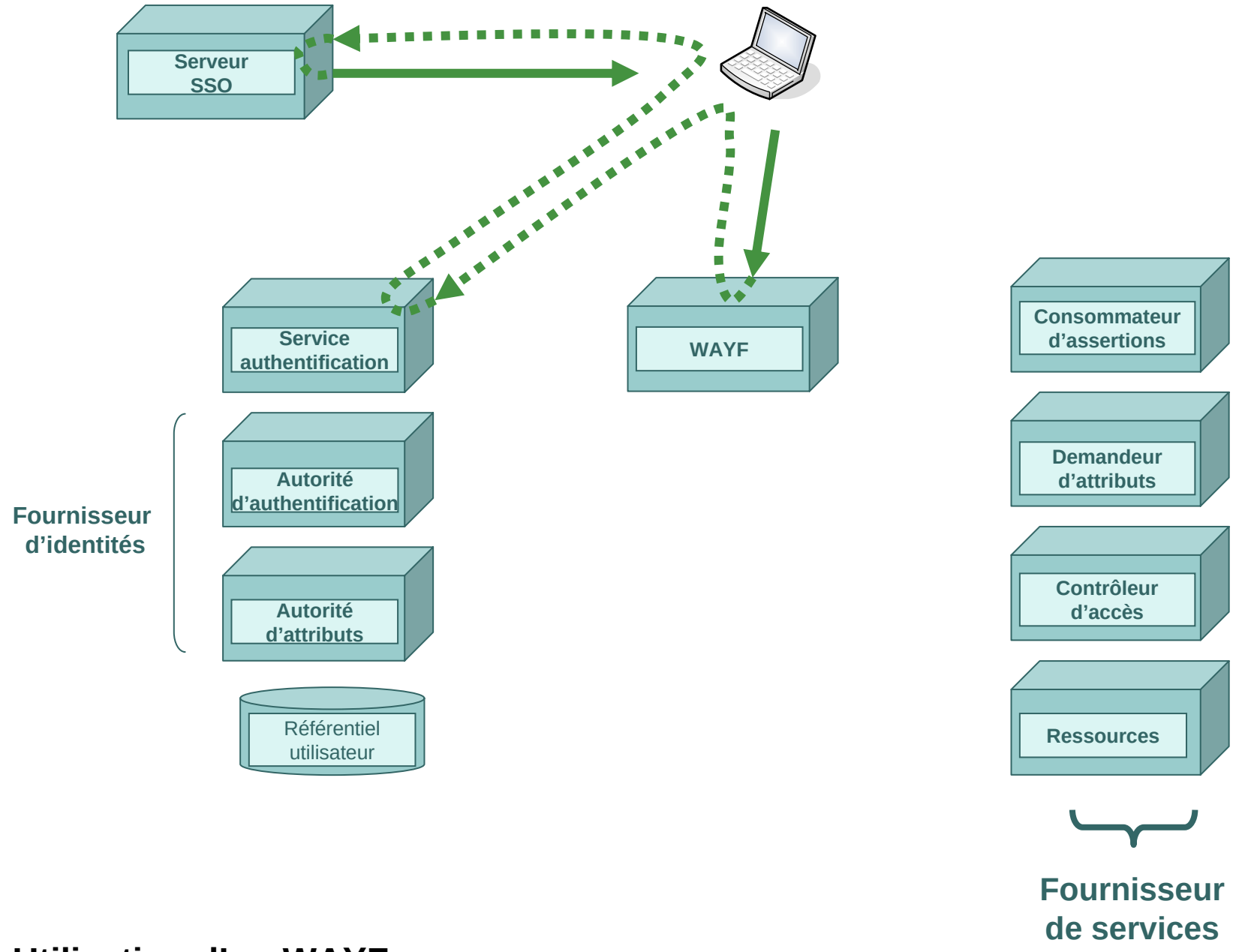
- Where Are You From ?
- Rôle :
  - Orienter les utilisateurs pour sélectionner leur fournisseur d’identité.

Utilisation d'un WAYF

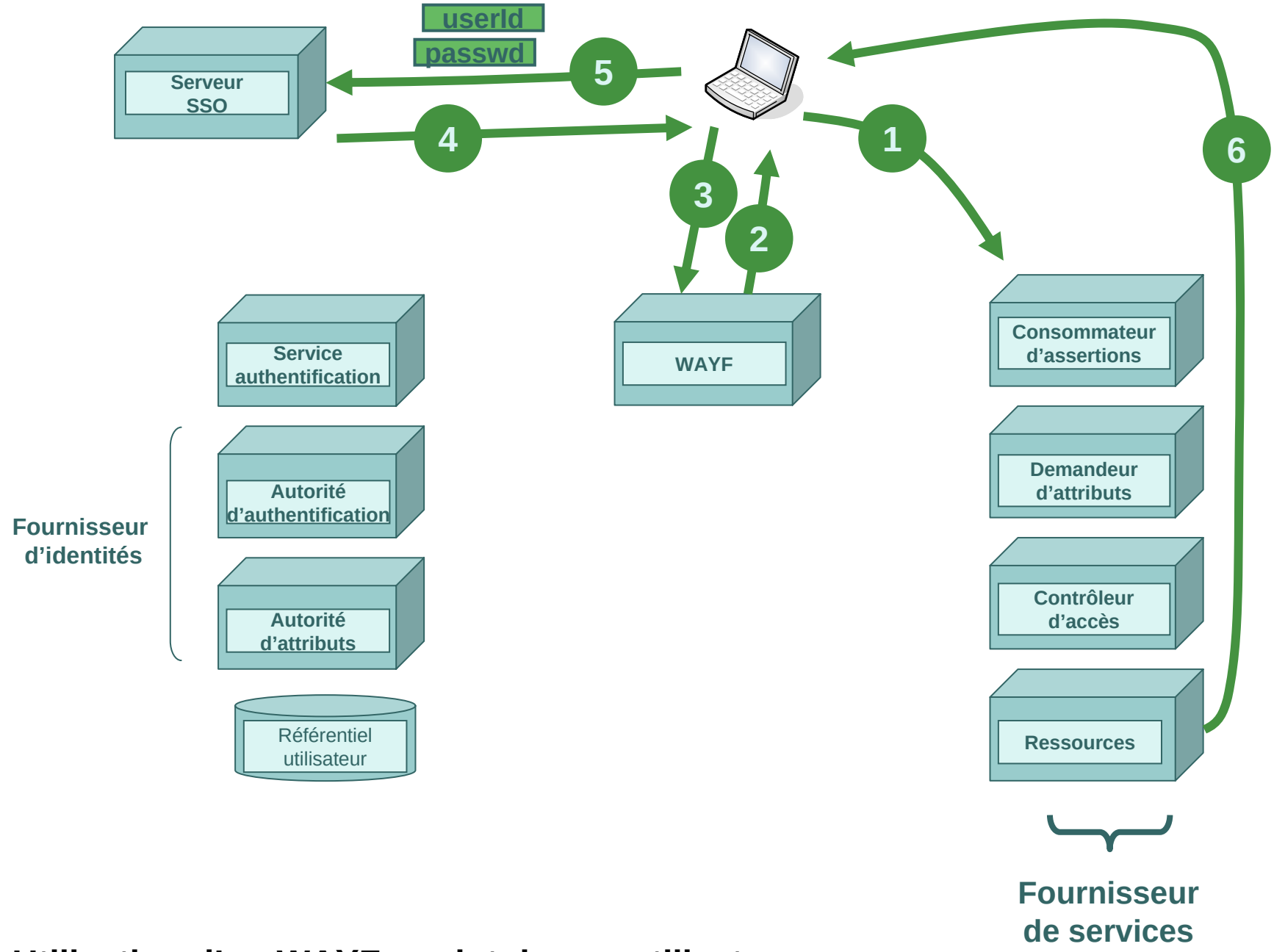




Utilisation d'un WAYF



Utilisation d'un WAYF



Utilisation d'un WAYF : point de vue utilisateur

Utilisation de Shibboleth dans les universités françaises

- Fédération du comité réseau des universités :
  - http://federation.cru.fr/
  - Signature convention entre le CRU et l'université.
  - partage de 15 attributs à la communauté

Fédération pilote du CRU

service de propagation d'identités et d'attributs

Publication de l'article JRES sur la fédération d'identités

- Fédération pilote

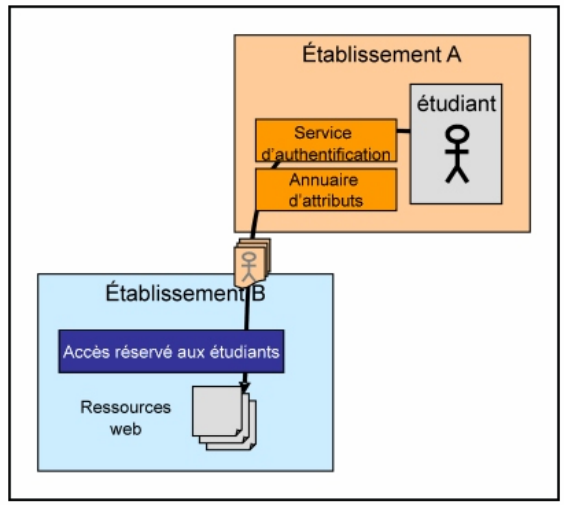
- Fédération de test

- Documentations
- Glossaire
- FAQ
- Démo

- Comment participer ?
- Annonces / contact

- Les attributs propageables au sein de la fédération pilote

L'objectif de ce service est de faciliter le partage de ressources numériques en ligne entre établissements d'enseignement supérieur en interconnectant leurs services d'authentification. Il devient possible d'ouvrir l'accès à une ressource numérique (pédagogique, scientifique, bibliothéquaire, etc.) à une population identifiée, sans devoir gérer localement l'enregistrement des utilisateurs. Exemple d'usage : une université B ouvre l'accès à un cours en ligne de pharmacologie, mais uniquement aux étudiants de cette discipline appartenant aux universités françaises, voire uniquement aux étudiants inscrits dans une université participant à l'Université Numérique en Région. Un étudiant en pharmacologie d'une université A pourra ainsi accéder au cours en ligne en s'authentifiant sur le site de son université et sans que l'université B doive l'enregistrer en tant qu'utilisateur.



- la fédération, un cercle de confiance
- principes de la propagation d'identités et d'attributs
- le service proposé par le CRU
- Shibboleth, le produit utilisé pour gérer la fédération

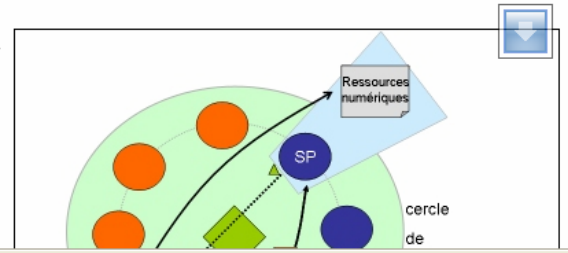
La fédération, un cercle de confiance

La fédération concrétise, pour un groupement d'établissements d'enseignement supérieur, l'interconnexion de leurs services d'authentification et l'utilisation d'un ensemble commun d'attributs utilisateurs. Un établissement qui gère un ensemble d'utilisateurs est appelé fournisseur d'identités. Un fournisseur de services est une entité - établissement, adminstration, société privée - qui propose une ressource numérique en ligne au sein de la fédération. Techniquement, les relations de confiance entre les membres d'une fédération reposent sur des certificats éléctroniques et des méta données partagées. La confiance peut en outre s'établir administrativement entre les participants de la fédération, de façon plus ou moins formelle (contrat, convention, charte, etc.).

Un même établissement peut participer à plusieurs fédérations et gérer des partenariats de manière bilatérale. Exemple : appartenance à la fédération nationale, à la fédération de l'UNR, partenariat avec des universités européennes. Un même établissement peut également jouer à la fois le rôle de fournisseur d'identités et de fournisseur de services.

Principes de la propagation d'identités et d'attributs

L'objectif de la propagation d'identités est double : déléguer l'authentification à l'établissement d'origine de l'utilisateur et obtenir certains attributs de l'utilisateurs (pour gérer le contrôle d'accès ou personnaliser les contenus).



La délégation de l'authentification réutilise les techniques de Single Sign-On web (redirection, cookies...). Lors de l'accès initial à une ressource numérique, l'utilisateur est redirigé vers le service de découverte de la fédération, d'où il sélectionne son établissement d'origine ; il est ensuite renvoyé vers son fournisseur d'identités. Le prérequis pour le fournisseur d'identités est de disposer d'un service d'authentification globale (pas forcément d'un SSO).

attribut	signification	exemple	URN	pour un fournisseur de service[1]	origine
givenName	prénom	Jérôme	urn:mace:dir:attribute-def:givenName	HTTP_SHIB_INETORGPERSON_GIVENNAME	inetOrgPerson
sn	nom	Dupond	urn:mace:dir:attribute-def:sn	HTTP_SHIB_PERSON_SURNAME	inetOrgPerson
cn	nom puis prénom sans accents	Dupond Jerome	urn:mace:dir:attribute-def:cn	HTTP_SHIB_PERSON_CN	inetOrgPerson
displayName	prénom puis nom avec accents	Jérôme Dupond	urn:mace:dir:attribute-def:displayName	HTTP_SHIB_INETORGPERSON_DISPLAYNAME	inetOrgPerson
mail	adresse de courrier électronique canonique	jerome.dupond@univ-xxx.fr	urn:mace:dir:attribute-def:mail	HTTP_SHIB_INETORGPERSON_MAIL	inetOrgPerson
preferredLanguage	langue usuelle	fr	urn:mace:dir:attribute-def:preferredLanguage	HTTP_SHIB_INETORGPERSON_PREFLANG	inetOrgPerson
postalAddress	adresse postale	1 rue Duchemin 12345 Lebled	urn:mace:dir:attribute-def:postalAddress	HTTP_SHIB_INETORGPERSON_POSTALADDRESS	inetOrgPerson
telephoneNumber	numéro de téléphone fixe	0123456789	urn:mace:dir:attribute-def:telephoneNumber	HTTP_SHIB_PERSON_TELEPHONENUMBER	inetOrgPerson
eduPersonPrincipalName	identifiant institutionnel inter établissements unique	jerome.dupond@univ-xxx.fr	urn:mace:dir:attribute-def:eduPersonPrincipalName	REMOTE_USER	eduPerson
eduPersonAffiliation	catégorie d'usager	staff	urn:mace:dir:attribute-def:eduPersonAffiliation	HTTP_SHIB_EP_UNSCOPEDAFFILIATION	eduPerson
eduPersonPrimaryAffiliation	catégorie principale d'usager	student	urn:mace:dir:attribute-def:eduPersonPrimaryAffiliation	HTTP_SHIB_EP_PRIMARYAFFILIATION	eduPerson
eduPersonScopedAffiliation	catégorie principale d'usager et organisme de de rattachement administratif	employee@univ-xxx.fr	urn:mace:dir:attribute-def:eduPersonScopedAffiliation	HTTP_SHIB_EP_AFFILIATION	eduPerson
supannOrganisme	organisme de rattachement administratif	{EES} 1234567N	urn:mace:cru.fr:attribute-def:supannOrganisme	HTTP_SHIB_SUPANN_SUPANNORGANISME	SUPANN
supannRole	sert à constituer des groupes de personnes transverses aux établissements	DIRECTEUR-IUT	urn:mace:cru.fr:attribute-def:supannRole	HTTP_SHIB_SUPANN_SUPANNROLE	SUPANN
supannAffectation	définit le(s) service(s) d'affectation pour les employés ou l'(es) entité(s) de formation pour les étudiants	Direction	urn:mace:cru.fr:attribute-def:supannAffectation	HTTP_SHIB_SUPANN_SUPANNAFFECTATION	SUPANN

L'attribut eduPersonTargetedID est un identifiant utilisateur unique, opaque et persistant partagé entre un fournisseur d'identités et un fournisseur de services. Il permet à un fournisseur de services d'avoir un identifiant anonyme pour un utilisateur. Un fournisseur d'identités choisit s'il diffuse cet attribut ou non. *eduPersonTargetedID* est construit automatiquement par Shibboleth, il est donc inutile de le renseigner dans un annuaire d'établissement. Son URN est *urn:mace:dir:attribute-def:eduPersonTargetedID*. Cette documentation propose une implémentation alternative qui améliore les propriétés de eduPersonTargetedID>

1 : indique le nom de la variable d'environnement par laquelle un fournisseur de service récupère la valeur de l'attribut. Ce nom correspond aux *headers* définis dans le fichier de configuration AAP.xml, préfixés par 'HTTP_', transformés en majuscule et avec les '-' passés en '_'.

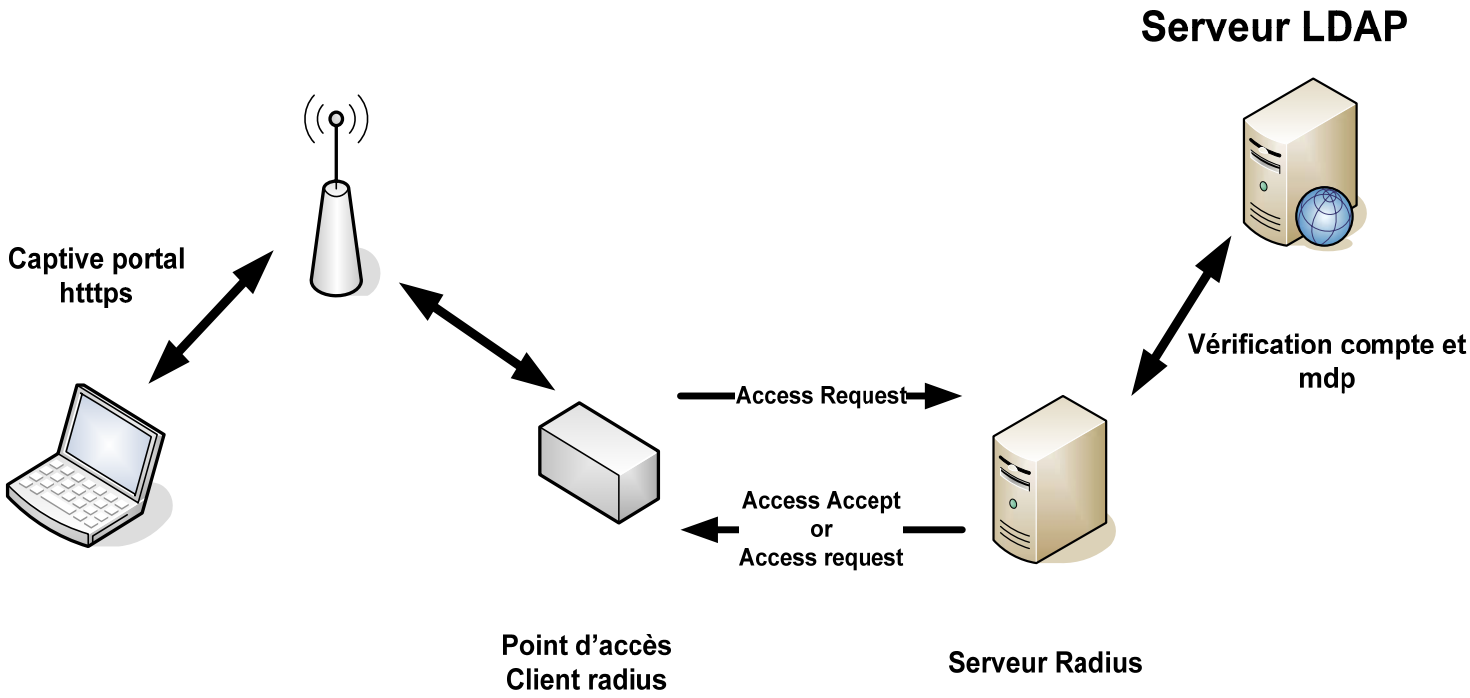
Authentification réseau

- Notre problématique concerne l'authentification des utilisateurs des différentes établissements aquitains pour utiliser le réseau wifi
- Première version utilisation d'un portail captif avec le protocole radius.
- Deuxième version : utilisation de Shibboleth et des attributs associés

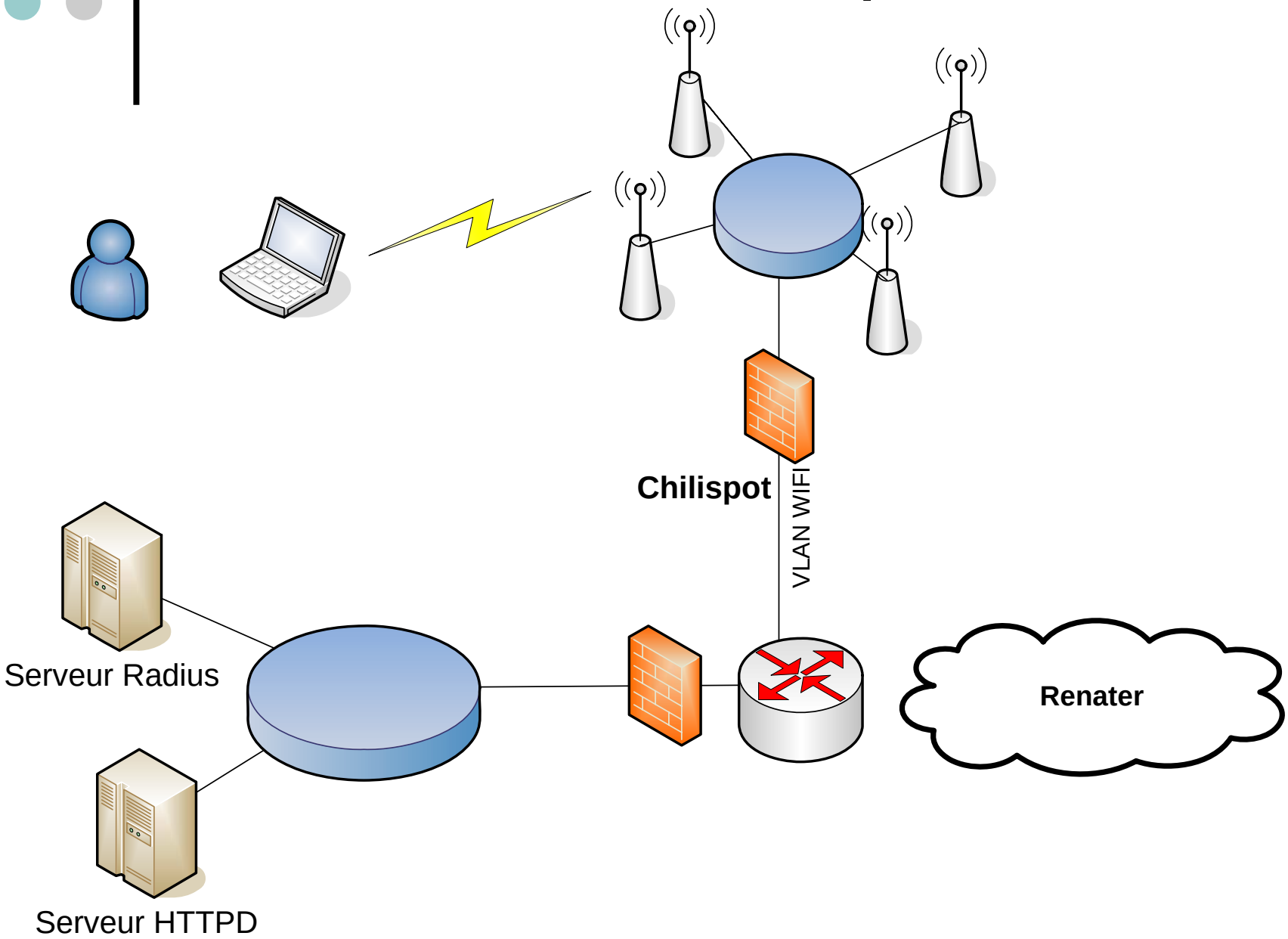
Portail captif version 1

- Chilispot
- Serveur Radius : Freeradius
- Le tout intégré sur un système embarqué Soekris avec une carte compact flash de 256 Mo.

Portail captif version 1



Architecture Chilispot



Fonctionnement Chilispot

1. L’utilisateur se connecte via un navigateur à un site.
2. chillispot intercepte la requête http et retourne un « http code redirect 302» vers le serveur httpd du formulaire (ssl) de saisie login et mot de passe.
3. L’utilisateur valide le formulaire, le cgi chiffre le mot de passe avec une clef secrète connue de lui et de chillispot avec en plus un « challenge » valable 2 mn

Fonctionnement Chilispot

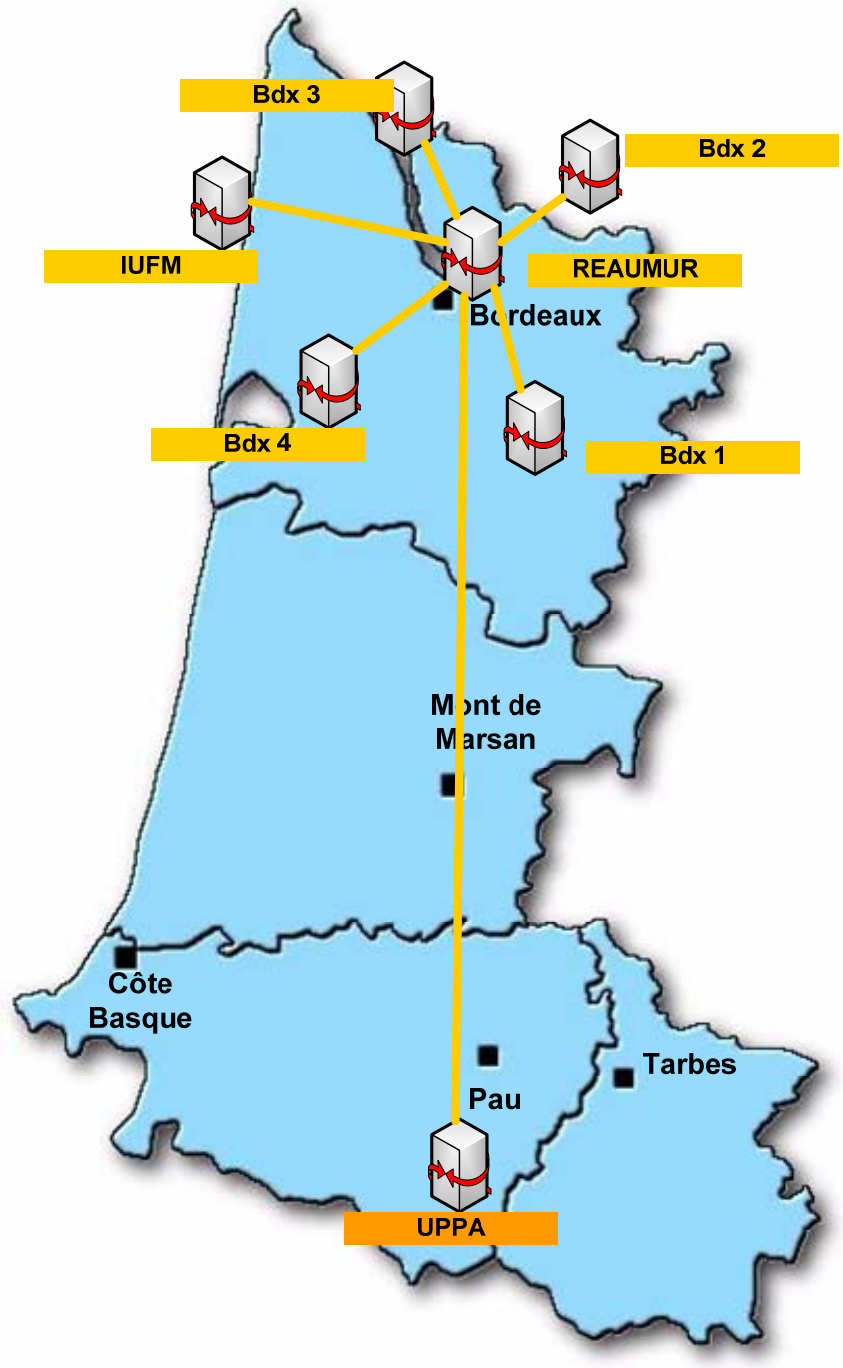
4. Le cgi renvoie un code « http redirect 302 » au navigateur du client avec le login et mot de passe chiffré vers le chillispot au port 3128.
5. Chillispot déchiffre le mot de passe et fait une requête radius « Acces-Request »
6. Si ok Radius renvoie un « acces accept »
7. Chillispot ouvre le réseau au (IP, @mac)
8. Chillispot renvoie un code « http redirect 302 » vers un serveur www mis en paramètre dans sa configuration.

Chilispot

- Avantages:
  - Simplicité de configuration des clients
  - Utilisation du proxy-radius pour plusieurs établissements (EDUROAM)
- Inconvénients
  - Pas de SSO
  - Le mot de passe est enregistré puis encrypté pour être envoyé sur des serveurs de la hiérarchie du proxy.

Chilispot Proxy-Radius

- Authentification par login@nom-établissement
- On n'accède plus aux annuaires LDAP des établissement mais uniquement à un serveur ProxyRadius central géré par Reaumur -> sécurité accrue
- Convention uniquement entre Reaumur et l'établissement



Chilibboleth

- Utilisation de chillispot avec Shibboleth
- Pourquoi ?
  - Captive portal
  - Utilisation du SSO des établissements
  - L’utilisateur s’authentifie sur son serveur d’appartenance.
- Pas de modification du code de chillispot

Chillibboleth

1. L’utilisateur se connecte via un navigateur à un site.
2. chillispot intercepte la requête http et retourne un « http code redirect 302» vers un cgi sur le serveur httpd où est installé une extension « mod-shib » qui propose le WAYF (autorisation des @ du WAYF et des SSO des établissements dans la configuration du chilispot)

Chillibboleth

3. Après authentification par shibboleth, le script cgi
   - récupère les attributs shibboleth normalisés Nom, prénom, statut,…
   - Encrypte l'attribut (statut) utile dans une variable que l'on passe dans le champ mot de passe utile au serveur radius.
4. Le cgi renvoie un code « http redirect 302 » au navigateur du client avec le login et les attributs chiffrés dans le champ mdp vers chillispot au port 3128

Chillibboleth

5. Chillispot fait alors une requête radius « Acces-Request » avec les attributs chiffrés dans le champ mot de passe
6. Le serveur radius (Freeradius) déchiffre les attributs et renvoie un « Acces-Accept » avec l'attribut chillispot adéquat :
    1. Pour les étudiants, on limite la bande passante en download à 1 Mbits donc si étudiant Freeradius renvoie l'attribut **WISPr-Bandwidth-Max-Down** avec la valeur 1048 576 b/s
4. Chillispot ouvre le réseau au (IP, @mac)
5. Chillispot renvoie un code « http redirect 302 » vers un serveur www mis en paramètre dans sa configuration

Conclusions

- Utilisation plus fines des attributs :
  - Logs, portail,…
- Utilisation du SSO de l'université renforcée ➔ portail plus utilisé
- Méthode applicable à d'autres portails captifs utilisant le protocole radius,

Références

- Shibboleth :
  - http://shibboleth.internet2.edu/
  - http://federation.cru.fr/doc/
- Chillispot :
  - http://chillispot.org
- Freeradius :
  - http://www.freeradius.org/