

*REAUMUR / ACO
TIC/PRES Université de Bordeaux*



Shibboleth sur REAUMUR

Journée Fédération du CRU – Paris, 25 Janvier 2007

Laurent FACQ - facq@u-bordeaux.fr

www.reaumur.net

REseau Aquitain des Utilisateurs des Milieux Universitaire et de Recherche

Version du 24/01/2007 20:50:51



Plan de la présentation

Format: Retour d'expérience chronologique

- contexte de réalisation
- première mise en place (portail captif)
- extensions et évolutions
- bilan



Contexte 2005

- REAUMUR
 - Service réseau inter-universitaire (7 personnes)
 - Mission : gérer le réseau régional Aquitain Nord & campus inter-u Bordelais
 - Partenaires : Établissements Enseignement Supérieur & Recherche (Universités, Écoles, EPST, ...)
- Mission ACO (Aquitaine Campus Ouvert) du Pôle Universitaire de Bordeaux
 - Mission : Développer l'usage des TIC en Aquitaine, mise en place d'ENT (Environnement Numérique de Travail), mutualisation des compétences et moyens techniques

Mi-2005 – La genèse

- Nouveau projet (ACO) confié à REAUMUR : déployer une infrastructure sans-fil inter-établissements
 - contraintes : accès universel, simple, authentifié
 - => portail captif (NoCatAuth)
 - => authentification « Web »
 - => être capable d'authentifier « tout le monde »
 - => être capable d'inter-opérer avec les annuaires existants
 - => le plus transparent possible pour les établissements
- Par ailleurs : Serveurs CAS (Central Authentication Service) en cours d'installation dans les universités (ENT)
- **==> Choix d'une authentification inter-établissement**



Choix d'une authentification inter-établissements (1/2)

- **Choix 1 : 100% maison ?**
 - mécanisme d'authentification au cas par cas
- **Avantages**
 - + Maîtrise totale
 - + Simple ?
 - + Prêt à temps (rentrée 2005) ?
- **Inconvénients**
 - Développement spécifique
 - Difficile à réutiliser ailleurs
 - Manipulation des mots de passe en clair
(formulaire web -> serveur d'authentification)



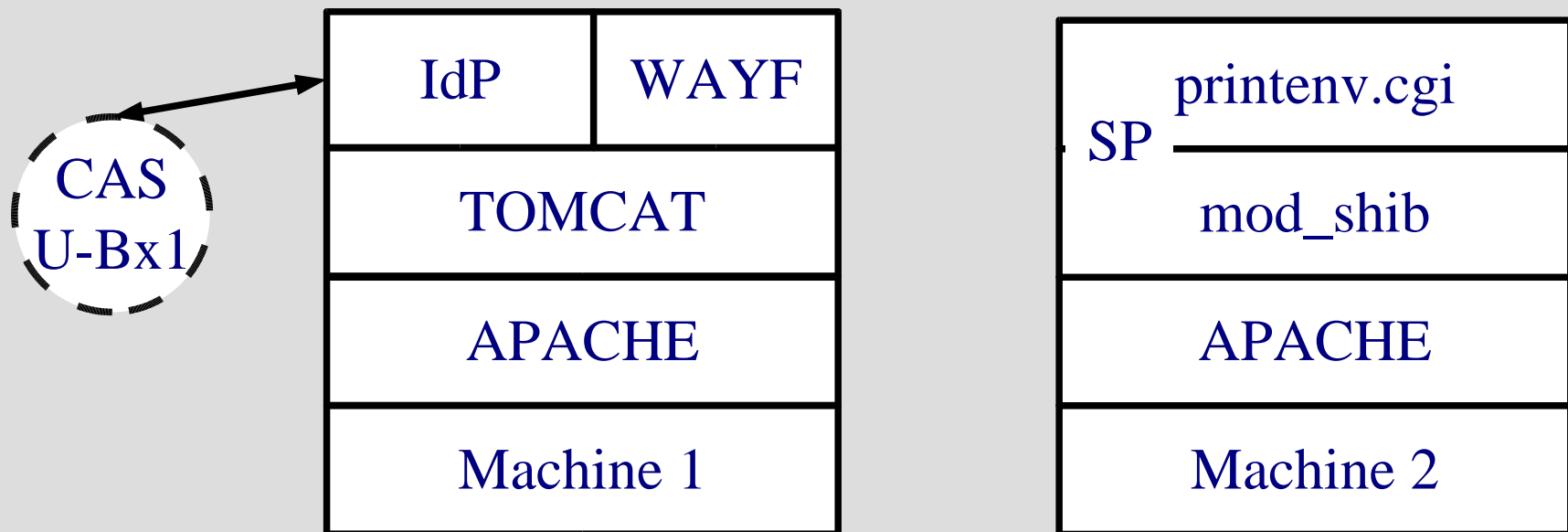
Choix d'une authentification inter-établissements (2/2)

- **Choix 2 : Fédération d'identité Shibboleth ?**
 - Conçue pour répondre à ce besoin
- Avantages
 - + « Standard » de la Communauté (CRU + Univ. d'Europe)
 - + Single Sign On
 - + Supporte « toutes » les authentifications (modules Apache)
 - + Facilement réutilisable pour d'autres projets
 - + Stable
- Inconvénients
 - Complexité
 - Aucune expérience Java/Tomcat
- **⇒ On se donne 15 jours pour tester shibboleth**

Première mise en place de Shibboleth

Objectif : une maquette

- 1 stagiaire (Mathieu GELI – ENSEIRB) + 1 titulaire à ~50%
- Objectifs :
 - Tests avec la fédération pilote du CRU
 - Maquette autonome :



IdP = Identity Provider
Fournisseur d'identité

SP = Service Provider
Fournisseur de Service



Première mise en place de Shibboleth

Premier Bilan

- ~2 semaines d'installation, configuration & **compréhension**
 - => l'authentification fonctionne
 - TOMCAT : très simple à installer
 - Déploiement d'application java = copie d'un fichier
- Problème : il manque le login (problème d'attribut)
- + ~2 semaines de débogage !! (problème de certificat)
 - => occasion d'approfondir nos connaissances et de se familiariser avec les logs
 - => du temps gagné en prévision de la résolution des futurs problèmes en phase d'exploitation
- Conclusion : ça marche, on continue !



« Shibbolethisation » du portail captif (1/2)

modification de l'authentification

- Problématique :
passer d'une authentification par formulaire « login »
spécifique à l'application (NoCatAuth)
à
une authentification générique par module Apache (mod_shib)
- Première modification :
 - protéger l'URL de « login » par Shibboleth (Apache)
 - modification du script « login » pour utiliser les variables fournies par mod_shib (REMOTE_USER & HTTP_SHIB_ORIGIN_SITE) et court-circuiter le formulaire
- Authentification ok, mais perte de l'affichage des informations spécifiques sur l'utilisation du service

« Shibbolethisation » du portail captif (2/2)

ré-insertion d'une page d'infos

- Version originale :

Je veux www....

capture

Bienvenu sur ...
... Aide – Infos ...

Login :
Passwd :

redirection

Page www....

- Avec shibboleth :

Je veux www....

capture

WAYF
Quel Etablissement ?

IdP/Serveur CAS
Login :
Passwd :

redirection

Page www....

Bienvenu...
Aide
Infos
Se connecter

- Problème : Plus d'espace pour informer l'usager (spécifique au portail captif)
- Deuxième modification : Ré-Insertion d'une page d'information... (en conservant les paramètres de capture : adresse mac, page demandée, ...)



Création de fournisseurs d'identité (IdP) par clonage

- Besoin : un fournisseur d'identité par établissement
- Contexte : tout sur le même serveur
- Solution : on duplique le premier IdP mis en place sur CAS
 - copie des arborescences java & configuration
 - procéder aux substitutions ad-hoc
- Durée : moins d'une heure par IdP



Extensions & Évolutions

- Autres Fournisseurs d'identité
- Shibbolethisation d'applications



Fournisseurs d'identité basés sur des modules d'authentification d'Apache (1.3)

- Objectif : intégrer des entités sans CAS
- Encore plus simple :
 - il suffit de protéger l'URL « SSO » avec le module choisi
 - le module doit remplir la variable REMOTE_USER
- Testé et en production avec :
 - Radius (mod_auth_radius)
 - POP (module mod_auth_pop)
 - LDAP (AD) (module auth_ldap modifié)
 - AuthType Basic
- Problème : comptes de test de certaines sources (POP)
 - Si nécessaire : liste noire au niveau des applications en coopération avec l'entité



Comment authentifier les usagers de passage ?

- Objectif : comptes temporaires pour les personnes de passage (congrès, formations, invités)
- Annuaire d'établissements inadaptés
- Solution rapide : un IdP de plus !
 - basé sur un fichier htaccess (format login:passwd)
 - génération de login/passwd à partir de listes de personnes
- En cours : automatisation de la gestion de l'IdP
 - Délégation aux organisateurs d'évènements (congrès, formations)
 - Parrainage pour les invités

Et les certificats X509 ?

- Problème :
 - nos applications existantes authentifient sur la base de certificats utilisateurs (CRU et CNRS)
- Solution actuelle : 2 URL pour le même service
 - URL Principal : `https://server/service`
 - Authentification X509 optionnelle (SSLVerifyClient optional)
 - Absence de certificat client => affichage d'un lien 'login shibboleth'
 - URL Shibboleth : `https://server/shibauth/service`
 - protégé par Shibboleth
 - lien symbolique sur le répertoire du service
 - Inconvénients :
 - L'application doit traiter les 2 cas (X509/Shib)
 - « SSLVerifyClient optional » déconseillé (pb sur certains navigateurs)

Et les certificats X509 ?

- Autre solution possible : 100% Shibboleth (non testée)
 - IdP basé sur certificats
 - Utilise le filtre « ClientCertTrustFilter »
 - Avantages :
 - simplicité maximale au niveau application
 - plus de cas particulier
 - Inconvénients :
 - si un seul IdP X509 : casse la règle « un IdP par établissement » (pas pratique pour les statistiques)
 - Solution : constituer des IdP par Autorité de Certification d'établissement ou exploitant le champ Subject, ...

Shibbolethisation d'applications

- Développements locaux : simple
 - Ex: applications pour nos correspondants techniques
Application de gestion de la sécurité, « looking-glass »,...
- Open Source :
 - basé sur une module d'authentification apache : simple
 - formulaire login/password : à priori faisable facilement
 - testé sur :
 - NoCatAuth (perl),
 - MediaWiki (php)
- Applications web « fermées » ???
 - code source inaccessible
 - logiciels embarqués

Shibbolethisation d'applications fermées

- Une solution : un proxy http (CGI) shibbolethisé



- Principe :
 - accès au proxy contrôlé par shibboleth
 - substitutions au vol en fonction de l'utilisateur (simple pour les applications sans état)
 - dans la requête (get/post)
 - dans la réponse
 - => ajout/suppression de liens..
 - => contrôle fin des droits utilisateurs
 - attributs utilisateurs stockés dans une base externe si besoin
- Inconvénients :
 - cas par cas à re-valider à chaque mise à jour de l'application

Shibbolethisation d'applications fermées

- Utilisation de CGIProxy (Perl) shibbolethisé
 - instances dédiées par application
- Applications traitées de cette façon :
 - interface de gestion de visioconférence d'un pont propriétaire (codian)
 - Pb : API XML insuffisante
 - => création de comptes locaux sur l'équipement en bijection avec comptes shibboleth
 - métrologie netmet (en cours)
 - Pb : pas de notion de comptes/droits
 - => un administrateur de site ne voit que les infos qui le concerne



Bilan

Shibboleth en exploitation

- En production depuis Septembre 2005 (V1.2.1 -> V1.3)
- Stable & peu gourmand
 - Charge machine très faible
 - ~ 1500 authentications par jour = 6000 requêtes SSO&AA
- Plus gros problèmes : dus aux certificats des serveurs CAS
 - se traduit par un message d'erreur dans le navigateur du client...
 - Expiration de certificat
 - Solution : l'établissement met à jour son certificat
 - Changement d'AC (CRU -> Cybertrust)
 - Solution : mise à jour du java.keystore
- Par précaution :
Activer le maximum de logs même en production !



Périmètre & Particularités

- Fournisseurs d'identités : 10 (7 CAS, 1POP, 1Radius, 1 htpasswd)
Universités Bordeaux 1,2,3,IV, ENSEIRB, > 50 000 usagers
IUFM-Aquitaine, UPPA
- IdP non gérés par les établissements
- Activation des Attributs : non (test ok)
- Intégration CRU : non (100% compatible)
- Fournisseurs de service gérés par REAUMUR : 6
- Fournisseur de service géré par des tiers : 0



Évolutions

- Haute Disponibilité
- A la demande des établissements :
 - activation des attributs
 - intégration des IdP dans Fédération CRU
- Statistiques
- Apache 1.3 -> Apache2
- IPv6

Conclusion

- Première mise en place non triviale....
 - Beaucoup de concepts nouveaux
- ... mais énorme gain de temps par la suite
 - ouverture & souplesse
- ==> une bonne opération !

Le mécanisme de fédération est vraiment
la bonne solution
dans un environnement multi-établissements.

Merci au CRU !



Fin

Questions ?