

SSO

CAS

Xavier.Marty@univ-tlse1.fr

Université Toulouse 1 Sciences Sociales

CAPITOUL - 18/10/2007

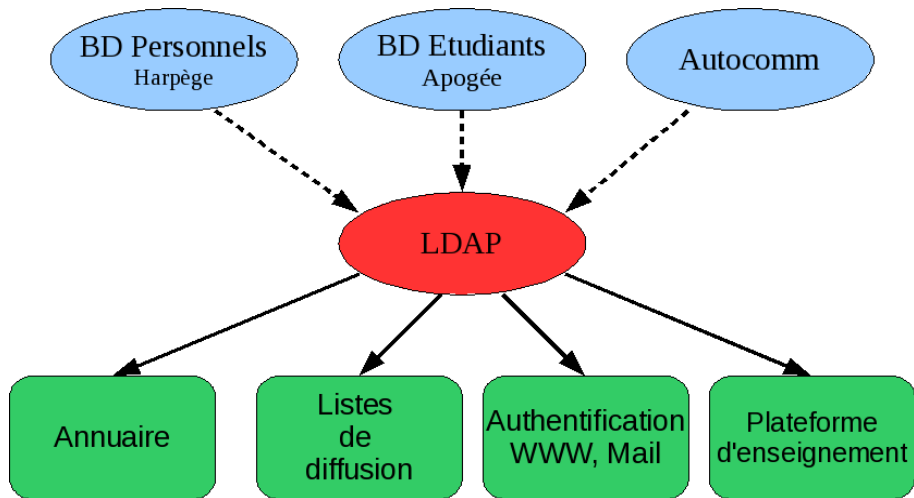


Plan

- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?
- 2 Principe de fonctionnement de CAS
 - Authentification
 - Accès d'un utilisateur
 - Fonctionnement simple
- 3 Mise en oeuvre à l'UT1
 - Installation de CAS
 - Utilisation d'applications compatibles CAS
 - Modifications des applications
 - Exemple
- 4 Conclusion
 - Bilan
 - Liens

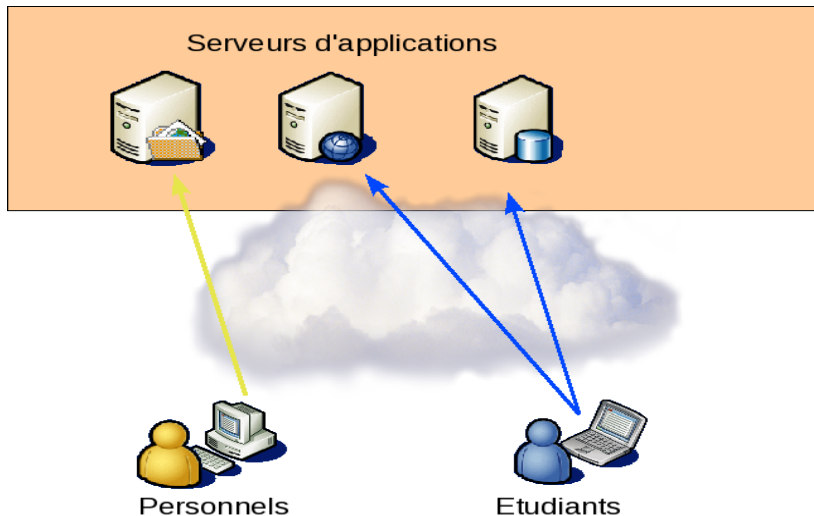
Un Système d'Information

Où en sommes nous ?



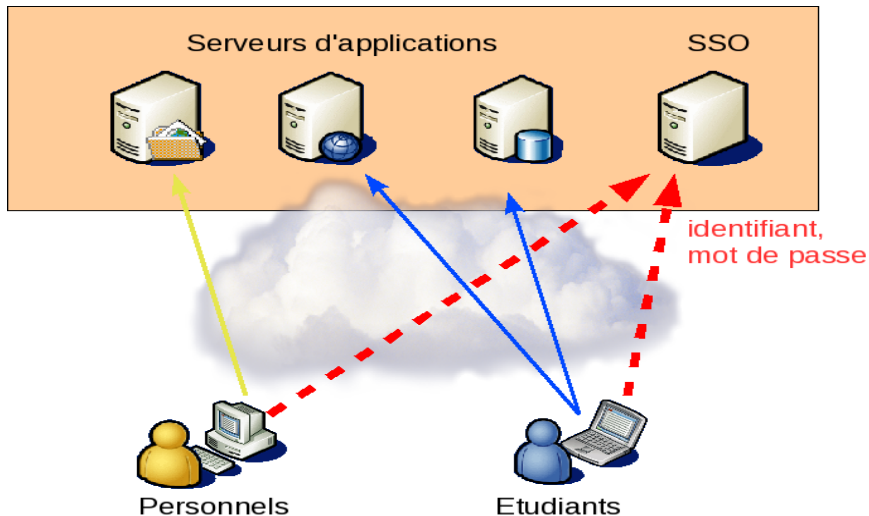
Un Système d'Information

A quoi voulons nous arriver ?



Un Système d'Information

A quoi voulons nous arriver ?



- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?

- 2 Principe de fonctionnement de CAS
 - Authentification
 - Accès d'un utilisateur
 - Fonctionnement simple

- 3 Mise en oeuvre à l'UT1
 - Installation de CAS
 - Utilisation d'applications compatibles CAS
 - Modifications des applications
 - Exemple

- 4 Conclusion
 - Bilan
 - Liens

Une authentification unique pour quoi ?

- Courrier électronique
- Agenda
- Documents partagés
- Listes de diffusion
- Intranet
- Forums
- Plate-forme de télé-enseignement
- ...

Plan

- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?

- 2 Principe de fonctionnement de CAS
 - Authentification
 - Accès d'un utilisateur
 - Fonctionnement simple

- 3 Mise en oeuvre à l'UT1
 - Installation de CAS
 - Utilisation d'applications compatibles CAS
 - Modifications des applications
 - Exemple

- 4 Conclusion
 - Bilan
 - Liens

Pourquoi avons nous choisi CAS ?

1/3

- Pour la centralisation de l'authentification (sur un serveur)
- Pour les applications webs essentiellement
- Pour les utilisateurs
 - ▶ L'utilisation est simple
 - ▶ Leurs identifiants est unique pour l'ensemble des services
- Pour la sécurité
 - ▶ Le mot de passe peut être plus fort
 - ▶ Le trafic est en https
 - ▶ La page web est donc de confiance
 - ▶ La communication se fait entre client et serveur cas uniquement
 - ▶ La ré-authentification est transparente via cookie privé et protégé
 - ▶ L'application tierce ne connaît pas le mot de passe
 - ▶ L'application reçoit un ticket

Pourquoi avons nous choisi CAS ?

2/3

Le ticket

- ne contient aucune information personnelle
- ne peut être rejoué
- a une durée de vie limitée
- n'est utilisable que par l'application qui le demande

Pourquoi avons nous choisi CAS ?

3/3

- Portabilité (bibliothèques clientes)
 - ▶ Java, Perl, JSP, ASP, PHP, PL/SQL, modules Apache et PAM
 - ▶ Adaptation aisée des applications
- Pérennité
 - ▶ Développé par l'Université de Yale
 - ▶ En production dans les Universités
- Plateforme J2EE
 - ▶ Code léger (un millier de lignes de code)
- Open Source
- Intégration uPortal

Plan

- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?
- 2 **Principe de fonctionnement de CAS**
 - **Authentification**
 - Accès d'un utilisateur
 - Fonctionnement simple
- 3 Mise en oeuvre à l'UT1
 - Installation de CAS
 - Utilisation d'applications compatibles CAS
 - Modifications des applications
 - Exemple
- 4 Conclusion
 - Bilan
 - Liens

- Apache
 - ▶ mod_cas : authentication de page statique
- Perl
 - ▶ pam_cas : authentication de service non webs

Authentication

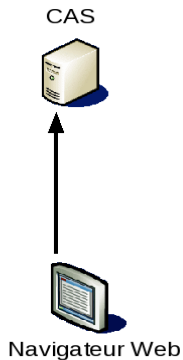
Mode d'authentification

- Annuaire LDAP
- Base de données
- Certificat X509
- Domaine Kerberos
- Domaine NIS
- Domaine Windows NT

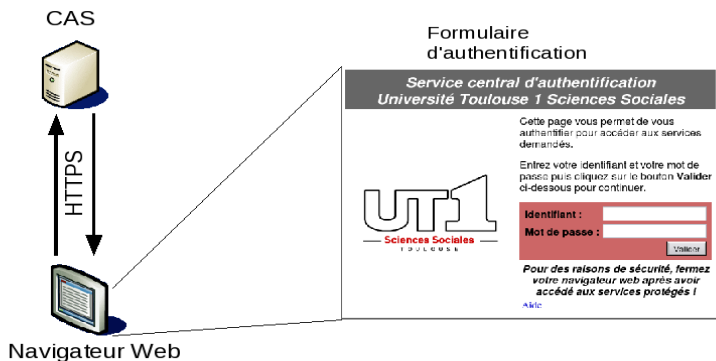
Plan

- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?
- 2 **Principe de fonctionnement de CAS**
 - Authentification
 - **Accès d'un utilisateur**
 - Fonctionnement simple
- 3 Mise en oeuvre à l'UT1
 - Installation de CAS
 - Utilisation d'applications compatibles CAS
 - Modifications des applications
 - Exemple
- 4 Conclusion
 - Bilan
 - Liens

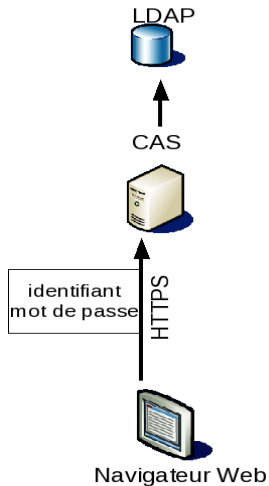
Accès d'un utilisateur



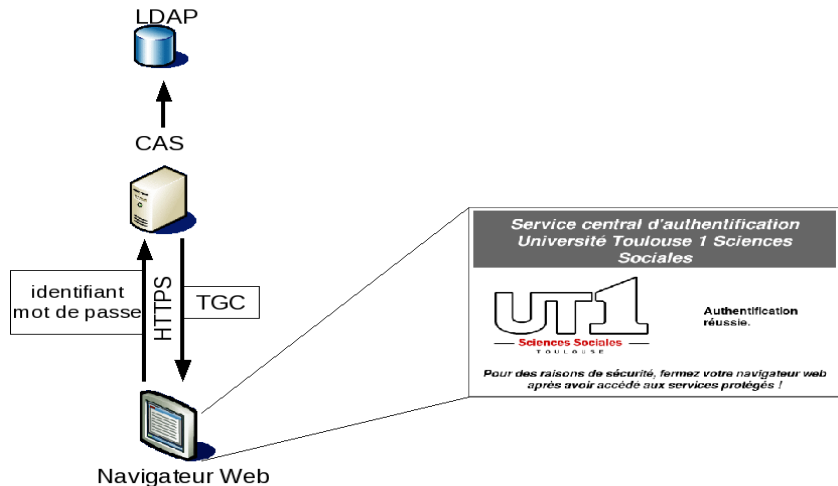
Accès d'un utilisateur



Accès d'un utilisateur



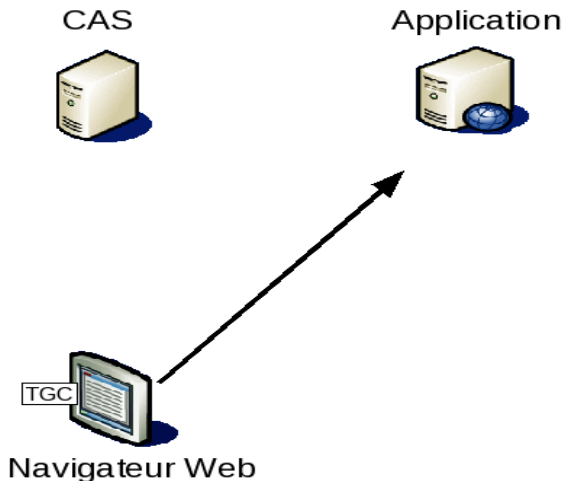
Accès d'un utilisateur



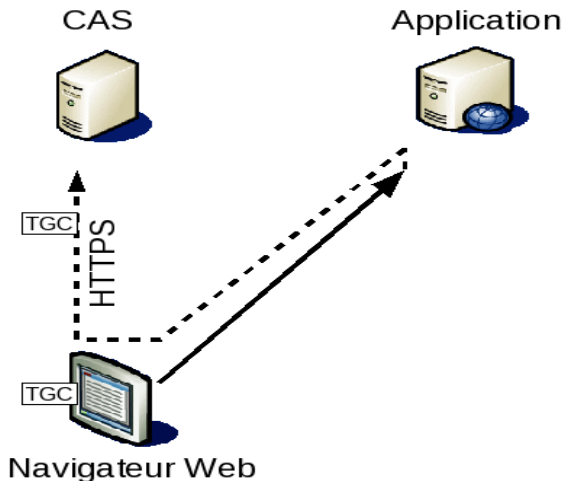
Plan

- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?
- 2 **Principe de fonctionnement de CAS**
 - Authentification
 - Accès d'un utilisateur
 - **Fonctionnement simple**
- 3 Mise en oeuvre à l'UT1
 - Installation de CAS
 - Utilisation d'applications compatibles CAS
 - Modifications des applications
 - Exemple
- 4 Conclusion
 - Bilan
 - Liens

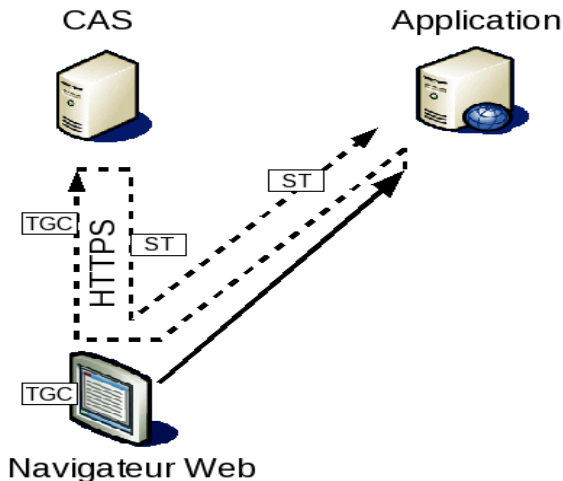
Fonctionnement simple



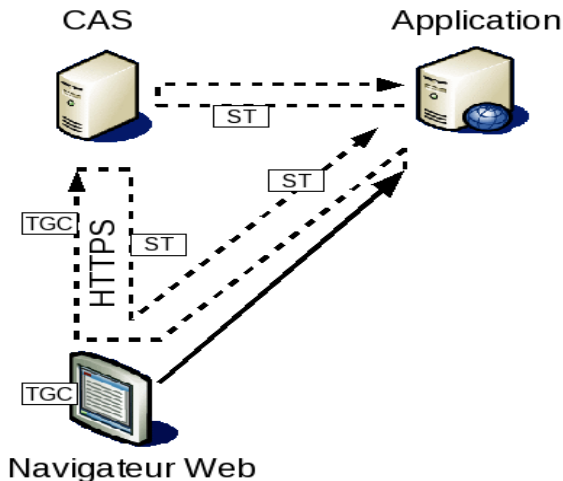
Fonctionnement simple



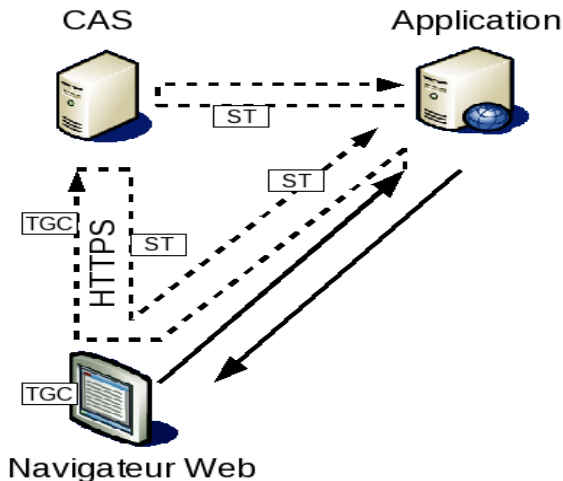
Fonctionnement simple



Fonctionnement simple



Fonctionnement simple



Plan

- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?
- 2 Principe de fonctionnement de CAS
 - Authentification
 - Accès d'un utilisateur
 - Fonctionnement simple
- 3 **Mise en oeuvre à l'UT1**
 - **Installation de CAS**
 - Utilisation d'applications compatibles CAS
 - Modifications des applications
 - Exemple
- 4 Conclusion
 - Bilan
 - Liens

Installation de CAS

- Installation

- ▶ Simple, bien documentée
- ▶ Package esup-cas-quickstart qui intègre le serveur tomcat

- Configuration

- ▶ Fichier properties qui contient le paramétrage et le mode d'authentification
- ▶ Création d'une keystore contenant les certificats

Plan

- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?
- 2 Principe de fonctionnement de CAS
 - Authentification
 - Accès d'un utilisateur
 - Fonctionnement simple
- 3 **Mise en oeuvre à l'UT1**
 - Installation de CAS
 - **Utilisation d'applications compatibles CAS**
 - Modifications des applications
 - Exemple
- 4 Conclusion
 - Bilan
 - Liens

Utilisation d'applications compatibles CAS

- Utilisation d'applications du consortium eSUP
 - ▶ ENT eSUP
 - ▶ Horde IMP
- Autres applications
 - ▶ Moodle
 - ▶ Sympa
 - ▶ Filex
- Toute nouvelle application est cassifiée

Plan

- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?
- 2 Principe de fonctionnement de CAS
 - Authentification
 - Accès d'un utilisateur
 - Fonctionnement simple
- 3 **Mise en oeuvre à l'UT1**
 - Installation de CAS
 - Utilisation d'applications compatibles CAS
 - **Modifications des applications**
 - Exemple
- 4 Conclusion
 - Bilan
 - Liens

Modifications des applications

- Sites statiques
 - ▶ Modification htaccess
- Classification des applications
 - ▶ Wiki : adaptation authentication
 - ▶ Casier : htaccess + adaptation
 - ▶ Cyrus-Imapd : modification sasl
- CAS fait de l'authentification, pas de l'autorisation
- Les groupes doivent être gérés par l'application, ou alors, on gère des listes d'utilisateurs "require user".

Plan

- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?
- 2 Principe de fonctionnement de CAS
 - Authentification
 - Accès d'un utilisateur
 - Fonctionnement simple
- 3 **Mise en oeuvre à l'UT1**
 - Installation de CAS
 - Utilisation d'applications compatibles CAS
 - Modifications des applications
 - **Exemple**
- 4 Conclusion
 - Bilan
 - Liens

- Fichier : httpd.conf

```
LoadModule cas_module modules/mod_cas.so
<IfModule mod_cas.c>
CASLocalCacheInsecure On
CASLocalCacheFile /tmp/CAScache
CASTrustedCACert /<rep>/ssl/certs/cybertrust.txt
CASLoginURL https ://cas.univ.fr
CASHost cas.univ.fr
CASPort 443
CASValidate /validate
</IfModule>
```

- Fichier .htaccess

```
AuthType CAS
AuthName "Authentification cas"
Require valid-user
```

- Démo : <http://cri.univ-tlse1.fr/capitoul/>

- Fichier : pam_cas.conf

```
host cas.univ-tlse1.fr
port 443
uriValidate /proxyValidate
ssl on
trusted_ca /<rep>/ssl/certs/cachain-suresign.pem
proxy https ://horde.univ.fr/horde/casProxy.php
```

- Fichier : imap (/etc/pam.d)

```
auth sufficient /lib/security/pam_cas.so -simap ://imap.univ.fr -f/etc/pam_cas.conf
auth required pam_stack.so service=system-auth
account required pam_stack.so service=system-auth
```

Plan

- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?
- 2 Principe de fonctionnement de CAS
 - Authentification
 - Accès d'un utilisateur
 - Fonctionnement simple
- 3 Mise en oeuvre à l'UT1
 - Installation de CAS
 - Utilisation d'applications compatibles CAS
 - Modifications des applications
 - Exemple
- 4 **Conclusion**
 - **Bilan**
 - Liens

- :-)
 - ▶ Installation rapide
 - ▶ Utilisation simple pour les utilisateurs
 - ▶ Sécurisation élevée des authentifications
- :-(
 - ▶ Base d'utilisateur centralisé (pour UT1)
 - ▶ Classification parfois difficiles en fonction des applications

Plan

- 1 Pourquoi un SSO ?
 - Un Système d'Information
 - Une authentification unique pour quoi ?
 - Pourquoi avons nous choisi CAS ?
- 2 Principe de fonctionnement de CAS
 - Authentification
 - Accès d'un utilisateur
 - Fonctionnement simple
- 3 Mise en oeuvre à l'UT1
 - Installation de CAS
 - Utilisation d'applications compatibles CAS
 - Modifications des applications
 - Exemple
- 4 **Conclusion**
 - Bilan
 - **Liens**

- Remerciement : Pascal Aubry
- Liens :
 - ▶ <http://2003.jres.org>
 - ▶ <http://esup-portail.org>