Plan

- Présentation du logiciel Sympa
- Architecture
- La gestion des hôtes virtuels
- Listes avec inclusion des abonnés
- **Les modules d'authentification**

- Les Scénarios d'autorisation
- Le format TT2
- Les familles de listes
- Retour d'expérience de la gendarmerie, listes automatiques
- Le serveur SOAP
- Les mises à jour
- Conclusions

Les différentes interfaces

- Mail
  - A priori confiance dans le champ From:
  - Possibilité de challenge MD5
  - Support S/MIME
- Web
  - Authentification native sympa (mot de passe)
  - Utilisation de certificats x.509
  - Nombreuses autres méthodes implémentées
- SOAP
  - Authentification de l'utilisateur

  OU
  - authentification de l'application cliente

L'authentification native de sympa

- Utilisée pour l'accès à l'interface web (et SOAP)
- Couple email + mot de passe
- Gestion actuelle des mots de passe :
  - Mdp initial puis personnalisé par l'utilisateur
  - Crypté (réversible) dans la base de données
  - Possibilité de rappel du mot de passe

- Dans le futur :
  - Stockage d'une empreinte MD5
  - Plus de rappel du mot de passe

Gestion des sessions

- Login :
  1. Authentification
  2. Cookie de session positionné
- Cookie = md5(email+secret serveur)
- Logout = suppression du cookie

- Dans le futur, table des sessions côté serveur
  - Plus de gestion du secret serveur
  - Permet le Single Logout

Les modes d'authentification
(interfaces web et SOAP)

- Native Sympa
- LDAP
- CAS
- Generic SSO (convient pour Shibboleth, LemonLDAP,…)

- Paramétrage dans le fichier **auth.conf**

Le ficher auth.conf

- Auth.conf par défaut

  user_table

  regexp .*
- Configurable pour chaque virtual host
  - /home/sympa/etc/auth.conf
  - /home/sympa/etc/myvhost/auth.conf
- Définit :
  - les modes d'authentification utilisés
  - la séquence (+expressions régulières)

Exemple d'un auth.conf

```
cas
base_url https://sso-cas.cru.fr
auth_service_name cas-cru
ldap_host ldap.cru.fr:389
ldap_get_email_by_uid_filter (uid=[uid])
ldap_suffix dc=cru,dc=fr
ldap_scope sub
ldap_email_attribute mail

ldap
regexp univ-x\.fr
host ldap.univ-x.fr:389
suffix dc=univ-rennes1,dc=fr
get_dn_by_uid_filter (uid=[sender])
get_dn_by_email_filter (|(mail=[sender])(mailalternateaddress=[sender]))
email_attribute mail

user_table
negative_regexp ((univ-rennes1)|(univ-nancy2))\.fr
```

Mixer les modes d'authentification

L'authentification LDAP

1. Utilisateur saisit email/uid + mot de passe
2. Interrogation LDAP
   - get_dn_by_email ou get_dn_by_uid
3. Vérification du mot de passe
   - bind LDAP avec DN utilisateur + mot de passe

Paramétrage LDAP

- host, bind_dn, bind_password, timeout
- use_ssl, ssl_version, ssl_ciphers
- suffix, scope
- get_dn_by_uid_filter,
  get_dn_by_email_filter
- email_attribute, alternative_email_attribute
- authentication_info_url
- regexp, negative_regexp

L'authentification CAS

- Rappel CAS
  - Service de Single Sign-On
  - Déployé dans de nombreuses universités
  - Utilise le mécanisme des redirections HTTP
  - CAS ne véhicule qu'un identifiant utilisateur
  - Fonctionnement en mode proxy

L'authentification CAS dans Sympa

- Configuration de 1 ou +eurs serveurs CAS
  - Menu déroulant pour sélectionner le serveur
- Le serveur CAS ne fournit pas l'adresse email
  - Sympa interroge un serveur LDAP
- Paramètre non_blocking_redirection
  - Permet une authentification transparente
- Utilisation du mode proxy (pour SOAP)
  1. Uportal fournit un proxy ticket
  2. Sympa valide le proxy ticket auprès du serveur CAS

Exemple de configuration

```
cas
base_url https://sso-cas.cru.fr
non_blocking_redirection on
auth_service_name cas-cru
ldap_host ldap.cru.fr:389
ldap_get_email_by_uid_filter (uid=[uid])
ldap_timeout 7
ldap_suffix dc=cru,dc=fr
ldap_scope sub
ldap_email_attribute mail
```

identifiant CAS

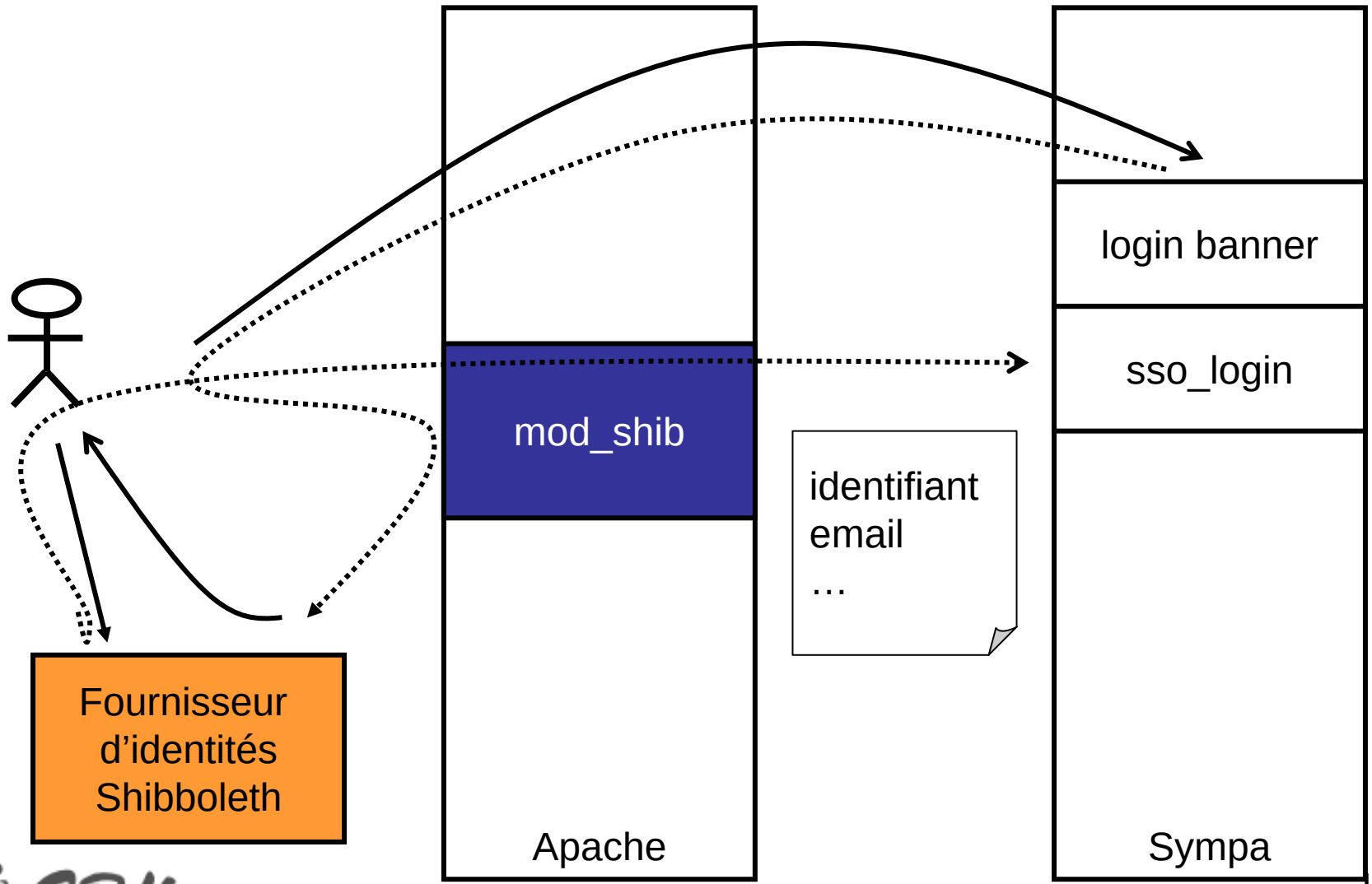
L'authentification Shibboleth

- Rappel sur Shibboleth :
  - Système de fédération d'identités
  - Transmet des attributs utilisateur
  - Brique « fournisseur de services » :
    - Module d'authentification pour Apache
    - Installé en frontal de l'interface web de Sympa
    - Fournit les attributs via des champs d'entête HTTP
    - Attributs utilisables par l'interface web de Sympa

Intégration Shibboleth dans Sympa

- Définition d'un connecteur générique (generic_sso)
  - Utilisable avec LemonLDAP, PAPI, Feide,…
- Pré-requis :
  - Contrôle d'accès en amont (Apache)
  - Activé sur une URL
    - /sympa/sso_login/mon_sso
  - Attributs (email) transmis via champ d'entête HTTP (= variable d'environnement)

Shibboleth / Sympa



Exemple de configuration Sympa (auth.conf)

```
generic_sso
service_name  Fédération du CRU
service_id  federation_cru
http_header_prefix   HTTP_SHIB
email_http_header HTTP_SHIB_EMAIL_ADDRESS
```

identifiant du service

Exemple de configuration Apache

```
<Location /sympa/sso_login/federation_cru>
  AuthType shibboleth
  require email
</Location>
```

Pour résumer… L'authentification

- Plusieurs modes d'authentification web :
  - Natif
  - LDAP
  - CAS
  - Shibboleth (generic_sso)
- Ils peuvent être mixés
  - Exemple : CAS ou LDAP ou natif