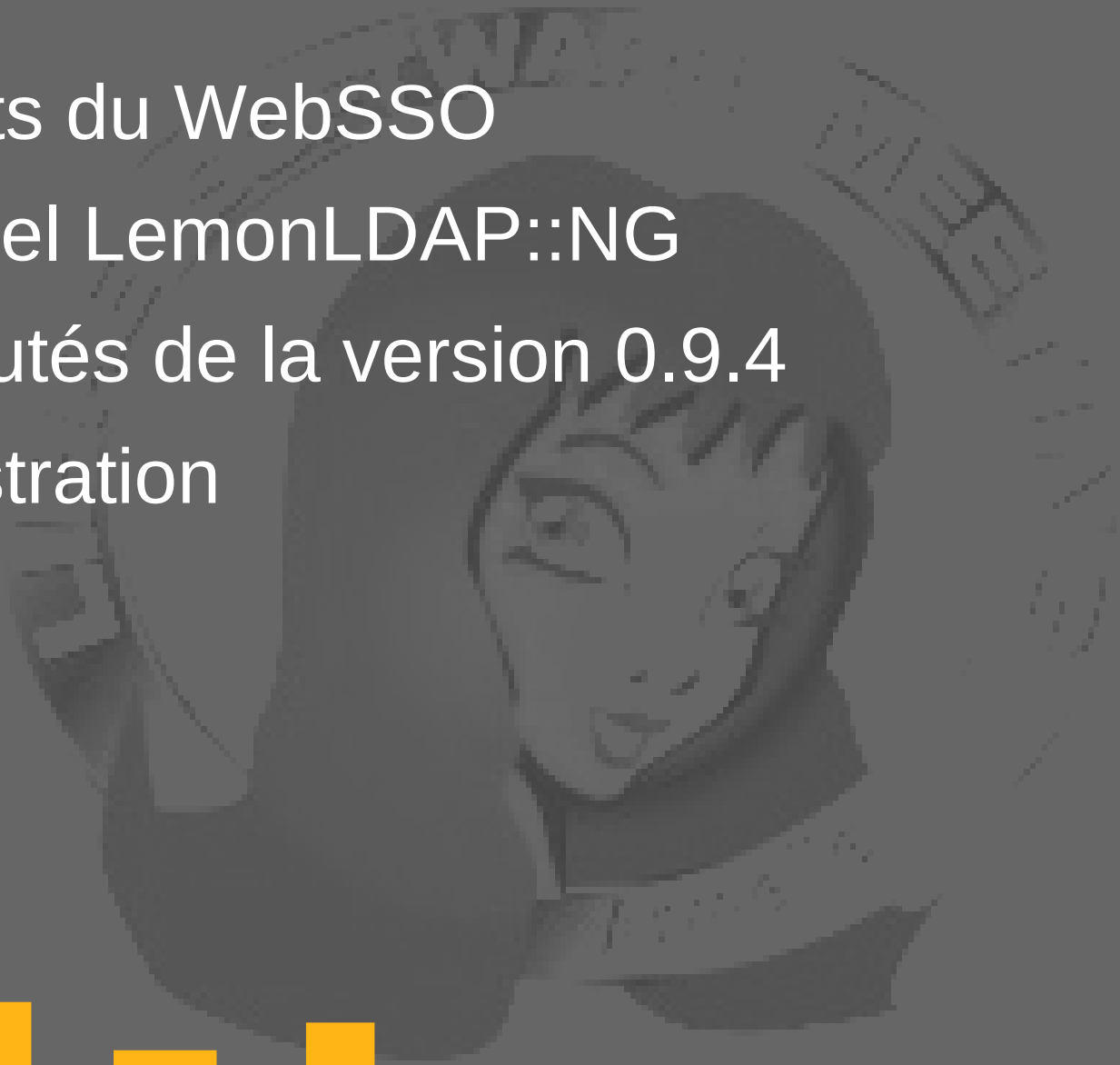
Rencontres Mondiales du Logiciel Libre 2009

Présentation du WebSSO LemonLDAP::NG

Clément OUDOT

Menu du jour



Concepts du WebSSO

Le logiciel LemonLDAP::NG

Nouveautés de la version 0.9.4

Démonstration

Définition du WebSSO

SSO signifie « Single Sign On », qui peut se traduire en français par « authentification unique »

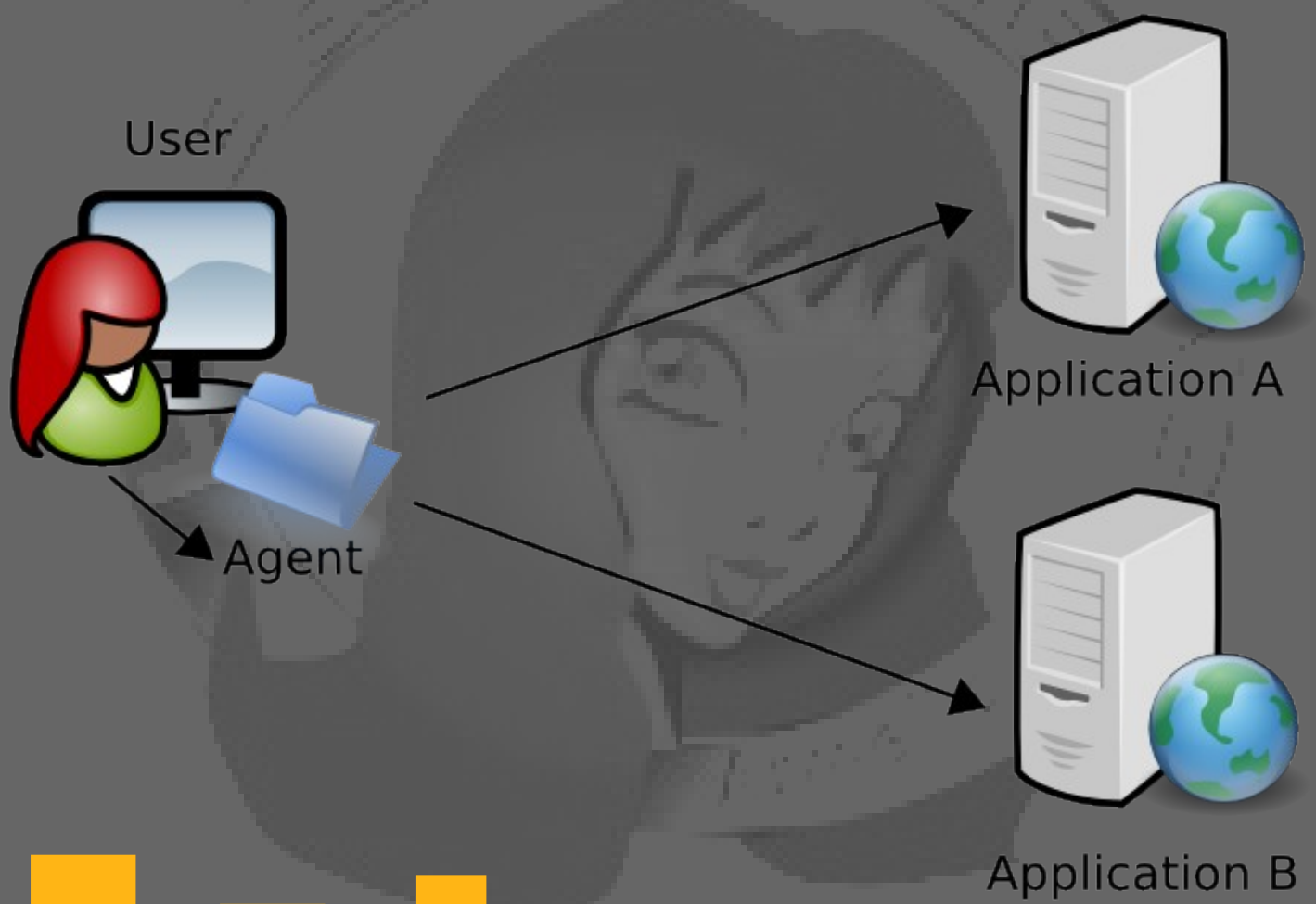
Le SSO est souvent accompagné de certaines fonctionnalités :

Politique de mot de passe centralisée

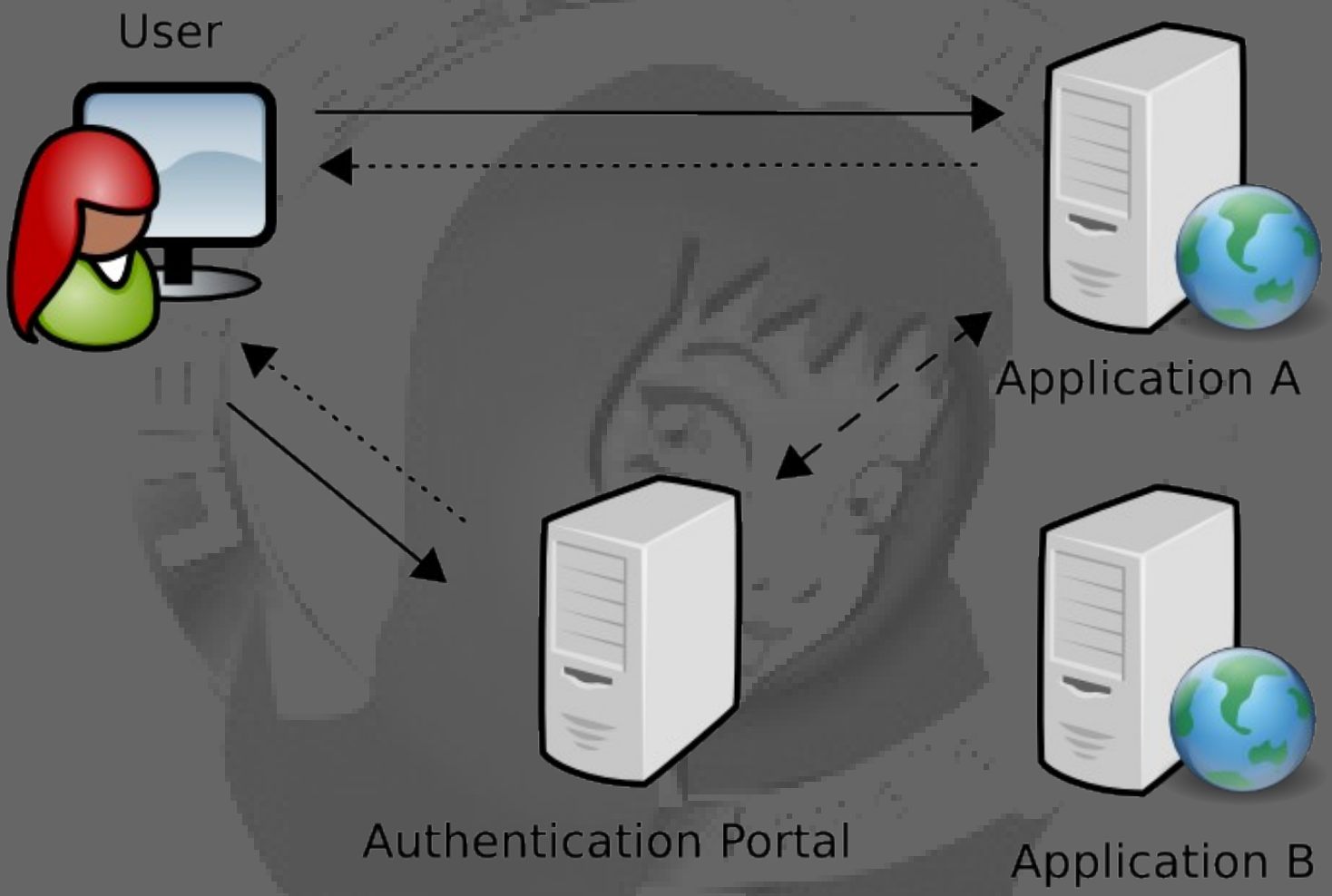
Transmission transparente des informations de session aux applications

Gestion des profils applicatifs, c'est-à-dire qui accède à quoi

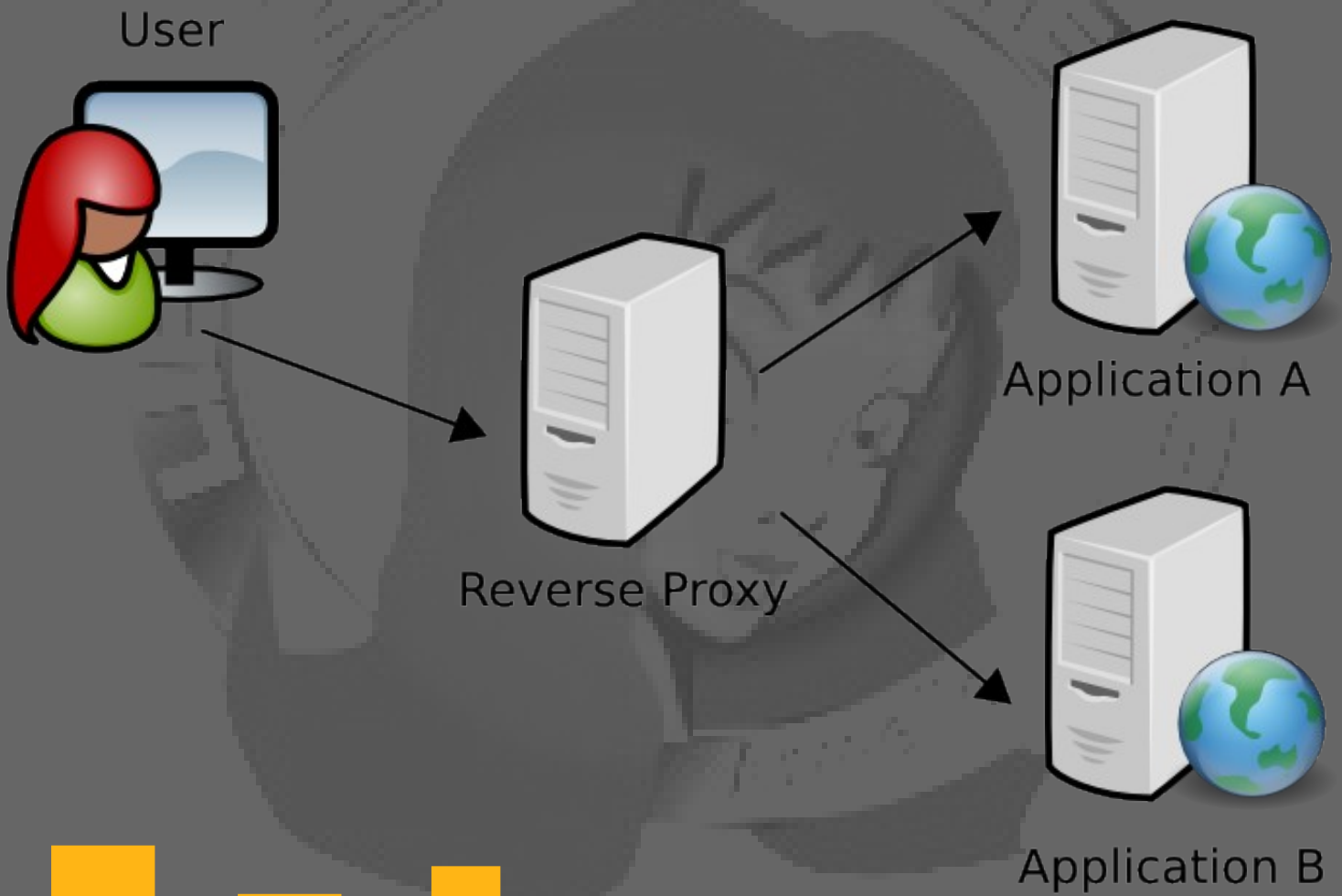
SSO par agent



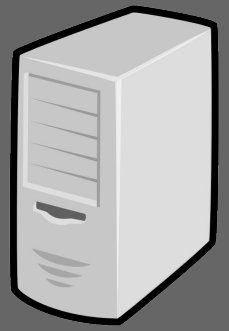
SSO par délégation



SSO par mandataire inverse



Le protocole HTTP



```
GET http://lemonldap.ow2.org HTTP/1.1
Accept: text/html
User-Agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.7.6)
```

```
HTTP/1.1 200 OK
Date: Thu, 13 Mar 2008 15:05:29 GMT
Server: Apache
Content-Length: 264
Content-Type: text/html; charset=iso-8859-1

<?xml version="1.0" encoding="iso-8859-1" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="fr" xml:lang="fr" dir="ltr">
<head>
<title>LemonLDAP::NG Homepage</title>

....
</html>
```

Présentation de LemonLDAP::NG

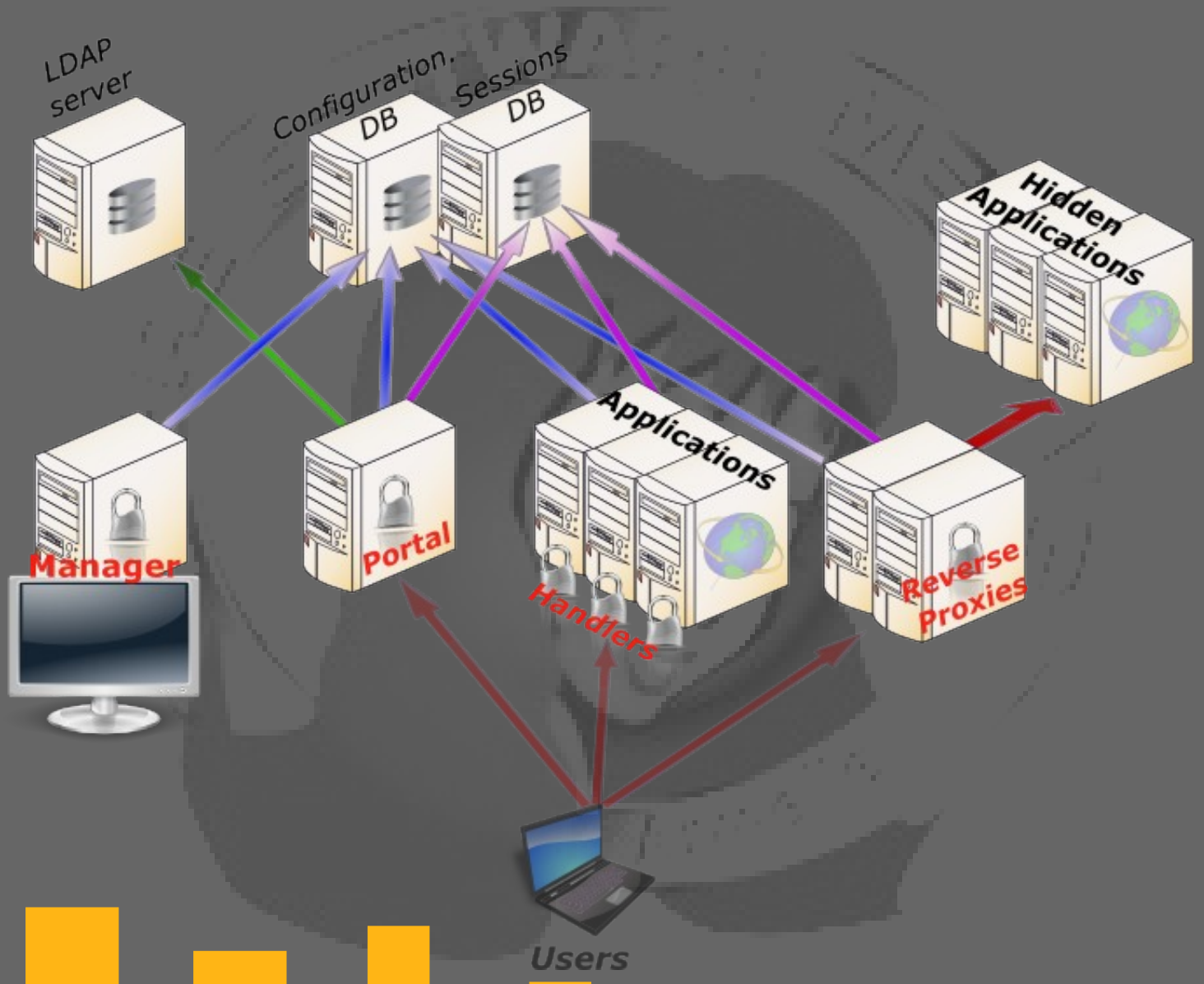
LemonLDAP::NG est un logiciel libre (licence GPL) hébergé chez OW2 : http://lemonldap.ow2.org

Développé à l'origine par Xavier GUIMARD pour les besoins de la Gendarmerie Nationale

Produit basé sur Apache et mod_perl, entièrement écrit en Perl (moteur et interfaces)

Fournit un portail d'accès dynamique et une interface d'administration

Architecture



Principe

L'implémentation par défaut utilise un annuaire LDAP pour :

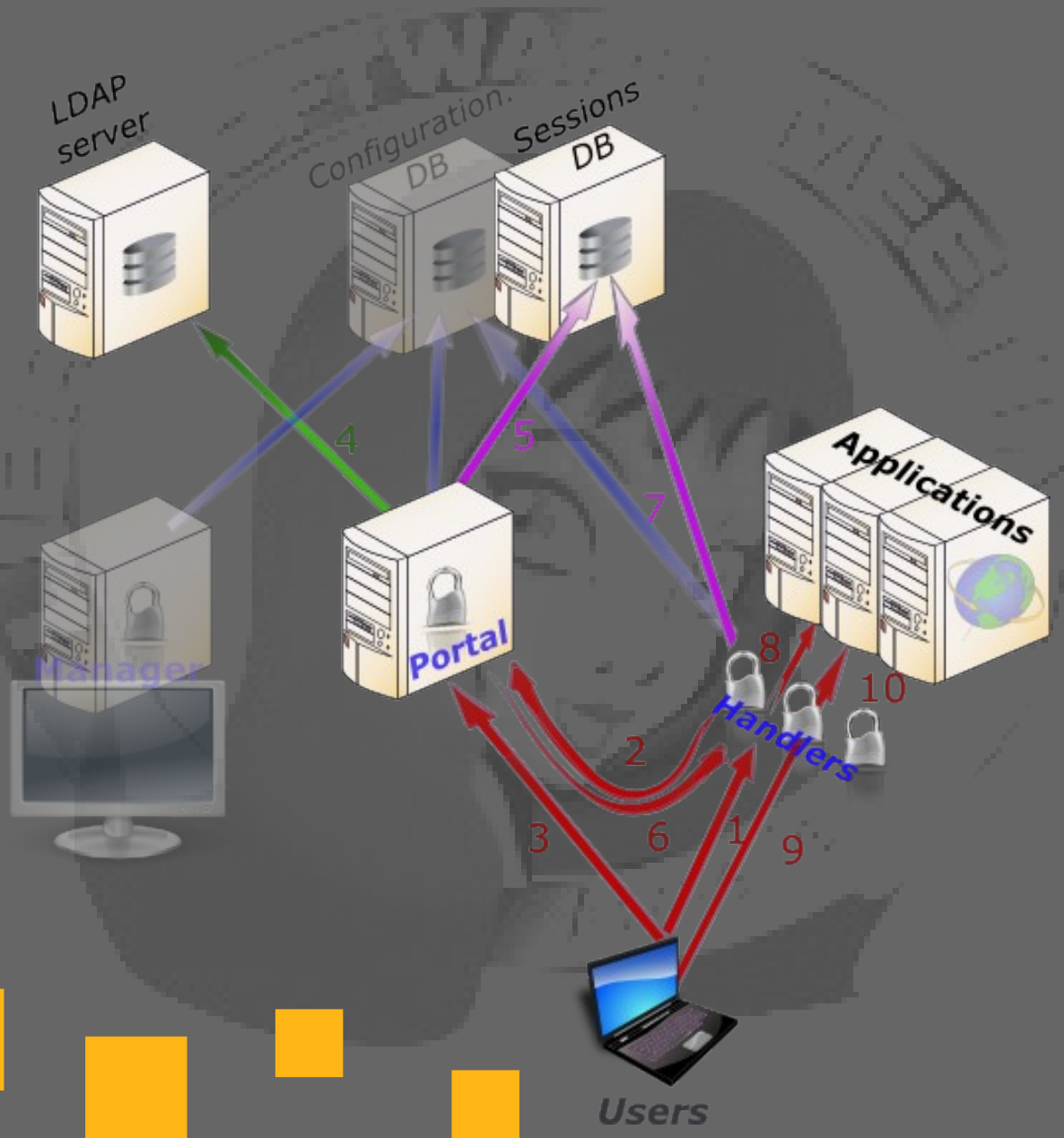
authentifier l'utilisateur (vérification du mot de passe)

effectuer un contrôle d'accès (selon les attributs LDAP de l'utilisateur)

approvisionner les applications (par transmission des attributs LDAP dans les en-têtes HTTP)

permettre à l'utilisateur de changer son mot de passe

Fonctionnement général



Gestion des sessions

- Utilisation de n'importe quel module Apache::Session pour le stockage (File, DBI, LDAP, Memcached, ...)
- Inscription du numéro de session dans un cookie temporaire (non écrit sur disque) avec le choix :
  - Cookie non-sécurisé
  - Cookie sécurisé (HTTPS uniquement)
  - Double cookie
- Durée de vie des sessions configurable

Règles d'accès

- Les règles d'accès sont des expressions Perl
- Elles peuvent être appliquées sur tout ou partie d'une application protégée (utilisation d'expressions régulières sur les URL)
- Tous les attributs exportés lors de l'authentification sont disponibles dans les règles
- Un système de macros permet de stocker des valeurs calculées en session

Règles d'accès

Accès pour tous les utilisateurs authentifiés :

Default => accept

Accès pour le groupe « admin » :

Default => $groups =~ /admin/

Accès aux mp3 pour l'utilisateur HADOPI :

^/*\.mp3 => $uid eq "HADOPI"

Interception du logout de l'application

^/logout.php => logout_sso

Hôtes virtuels

La distinction des applications est basée sur la notion d'hôtes virtuels

Les hôtes virtuels peuvent être répartis sur plusieurs serveurs Apache

Chaque hôte virtuel possède :

- Des règles d'accès
- Des en-têtes HTTP

Les en-têtes HTTP contiennent également des expressions Perl

Applications nativement compatibles

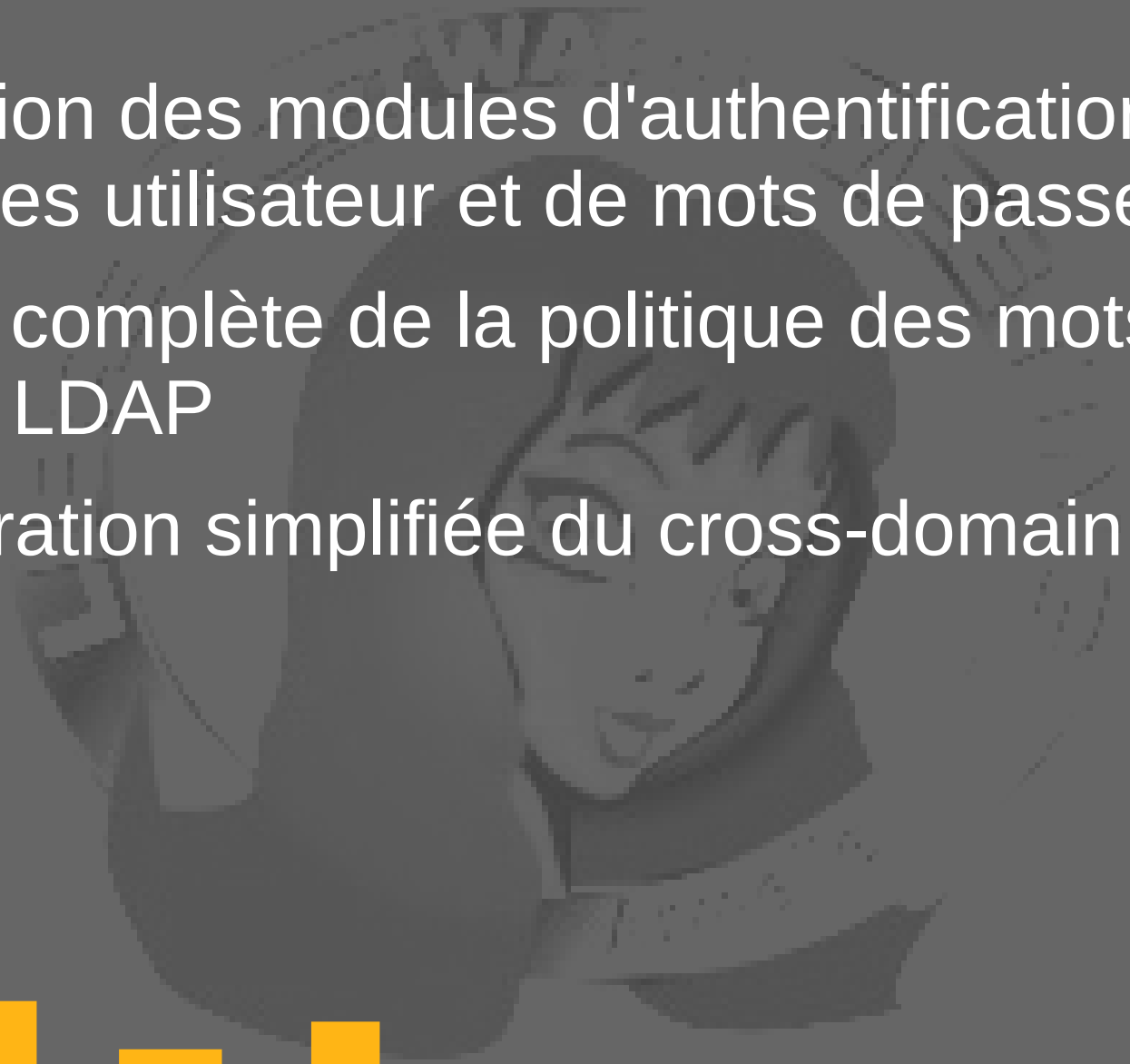
Autres applications compatibles

- Applications reposant sur la sécurité Apache (.htaccess) : Nagios, ...
- Applications reposant sur la sécurité Tomcat (users.xml) : Lutece, Probe, ...
- Applications utilisant HTTP Basic : Domino Web Access, Outlook Web Access, ...
- Applications compatibles SiteMinder

Nouveautés de la version 0.9.4

- Utilisation de LDAP possible pour le stockage de la configuration et des sessions
- Réécriture complète des fonctions SOAP : le portail est directement un point d'accès SOAP
- Système de notifications
- Nouvelles fonctions disponibles dans les règles d'accès pour vérifier les dates, les jours et les heures de connexion autorisés
- L'adresse du portail peut être dynamique

Nouveautés de la 0.9.4



- Séparation des modules d'authentification, de données utilisateur et de mots de passe
- Gestion complète de la politique des mots de passe LDAP
- Configuration simplifiée du cross-domain

Feuille de route

- Refonte de l'interface d'administration
- Validation du formulaire d'authentification pour les applications fermées
- Portefeuille de comptes pour les applications fermées
- Support SAML2 complet (fournisseur d'identités et fournisseur de service)

Démonstration