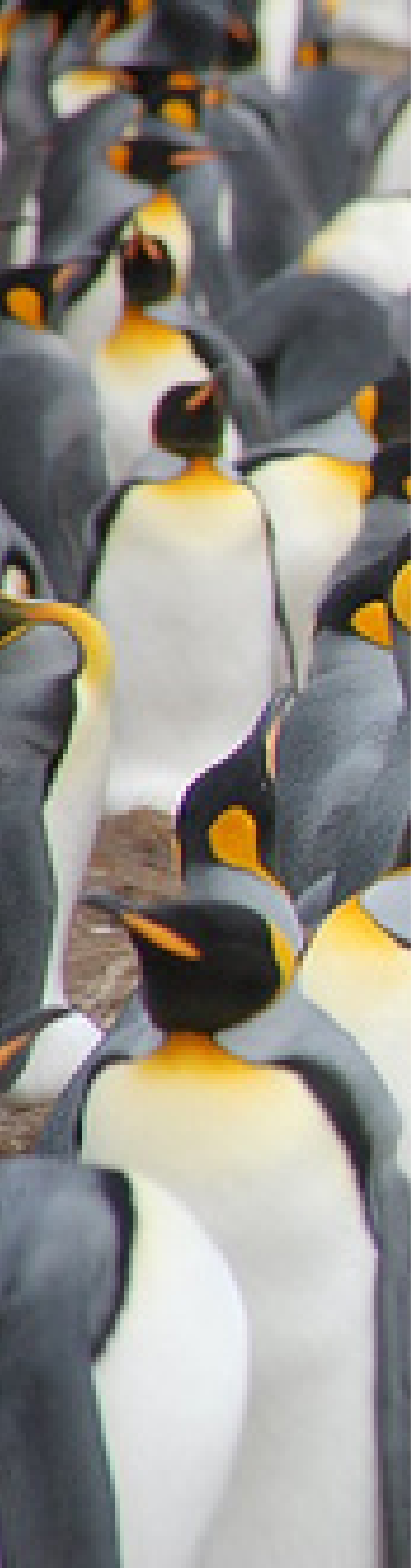


LINAGORA

Support de SAML2 dans LemonLDAP::NG

Clément OUDOT

Mercredi 7 juillet 2010

LemonLDAP::NG

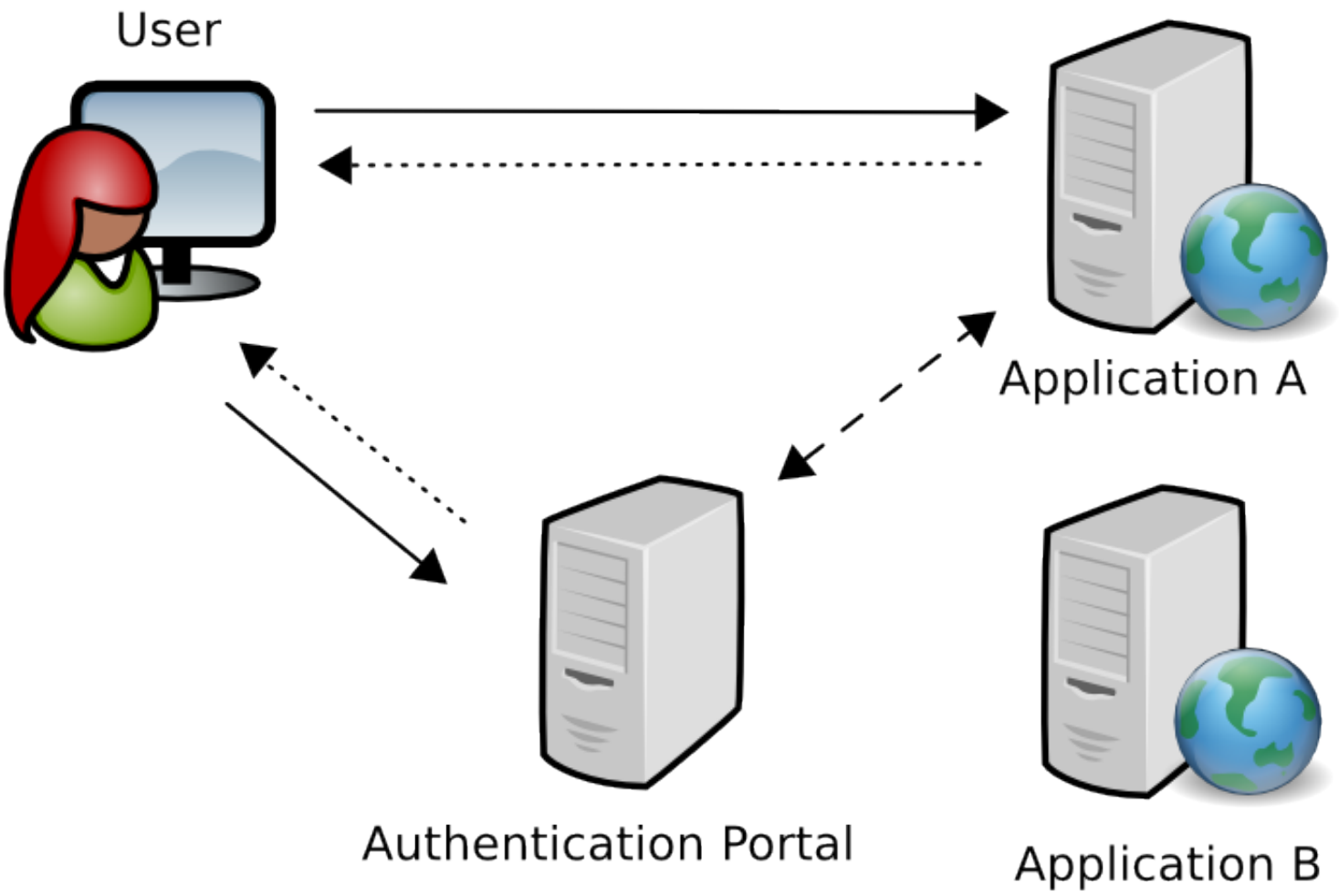
SOMMAIRE

- Enjeux et usages du SSO
- Présentation de LemonLDAP::NG
- SAML2 et la fédération d'identités
- Support SAML2 dans LemonLDAP::NG
- Démonstration

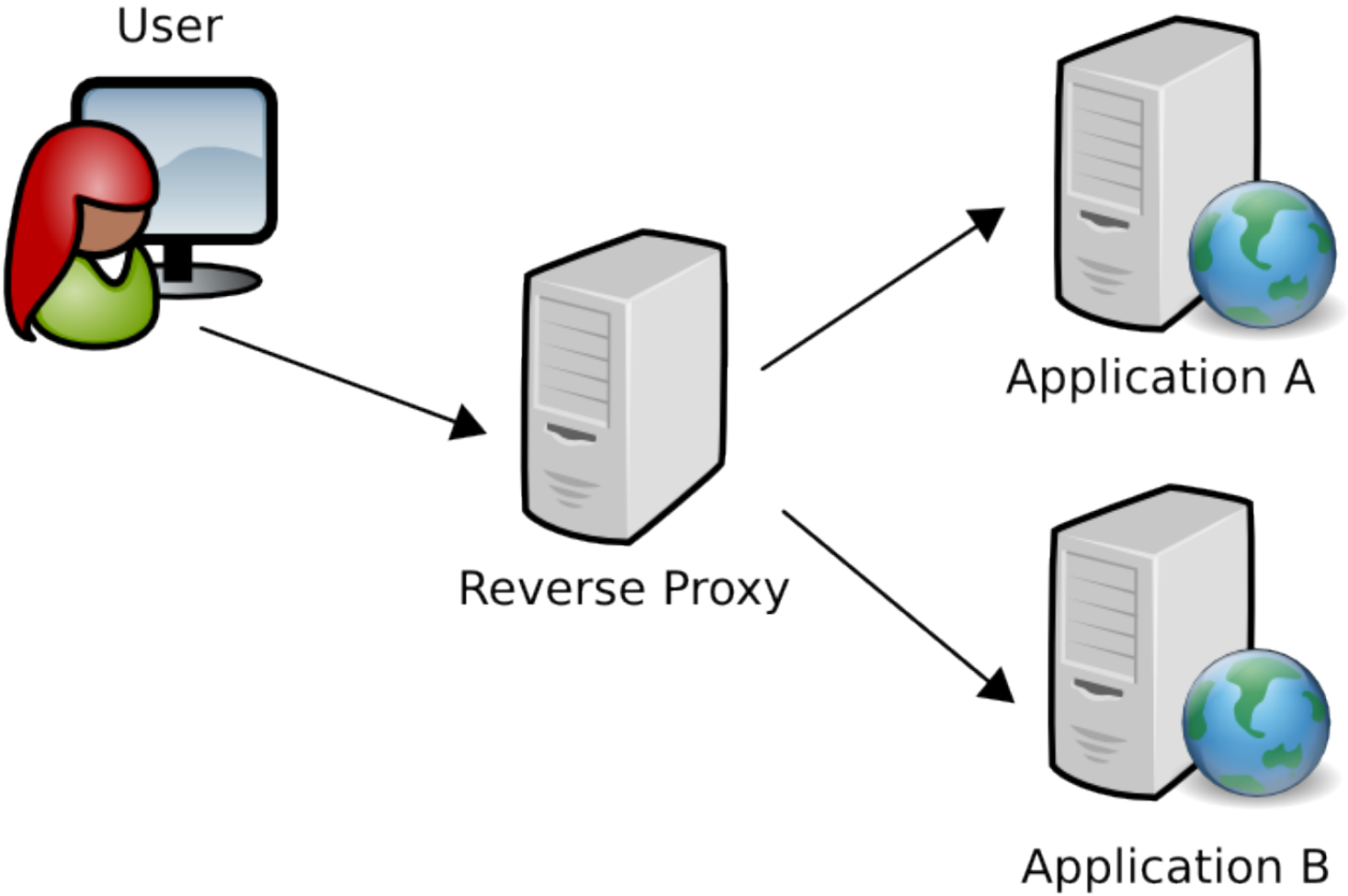
Le WebSSO

- SSO signifie « Single Sign On », qui peut se traduire en français par « authentification unique »
- Le WebSSO se consacre à l'authentification unique pour les applications Web, c'est-à-dire des applications client-serveur dont le client est un navigateur Web (IE, Firefox, etc.)
- Le principe de base est d'intercepter les requêtes entre le client et le serveur, et indiquer au serveur que le client est bien authentifié
- Techniquement, cela repose essentiellement sur la gestion d'une session SSO stockée au niveau du serveur WebSSO et liée à un cookie dans le navigateur de l'utilisateur
- Deux architectures complémentaires existent :
  - WebSSO par délégation
  - WebSSO par mandataire inverse

SSO par délégation



SSO par mandataire inverse



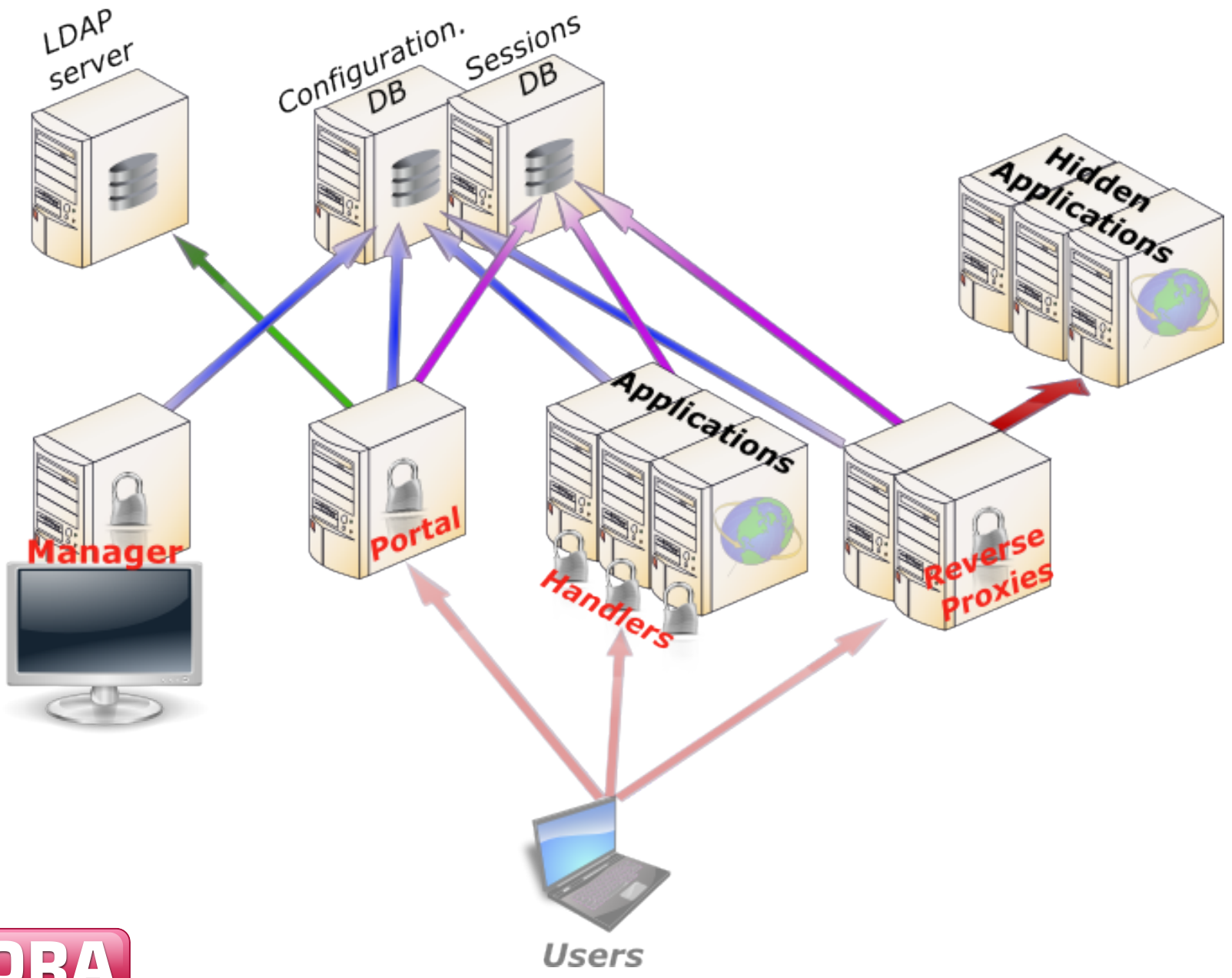
Autres fonctionnalités

- Le rôle standard du WebSSO est de propager l'authentification sur des applications Web
- En supplément, ces fonctionnalités sont souvent présentes dans les produits de WebSSO :
  - Contrôle d'accès aux applications (qui a accès à quoi)
  - Transfert d'informations complémentaires à l'identifiant de l'utilisateur (nom, mails, etc.)
  - Gestion du mot de passe (interface de changement de mot de passe, réinitialisation, etc.)

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

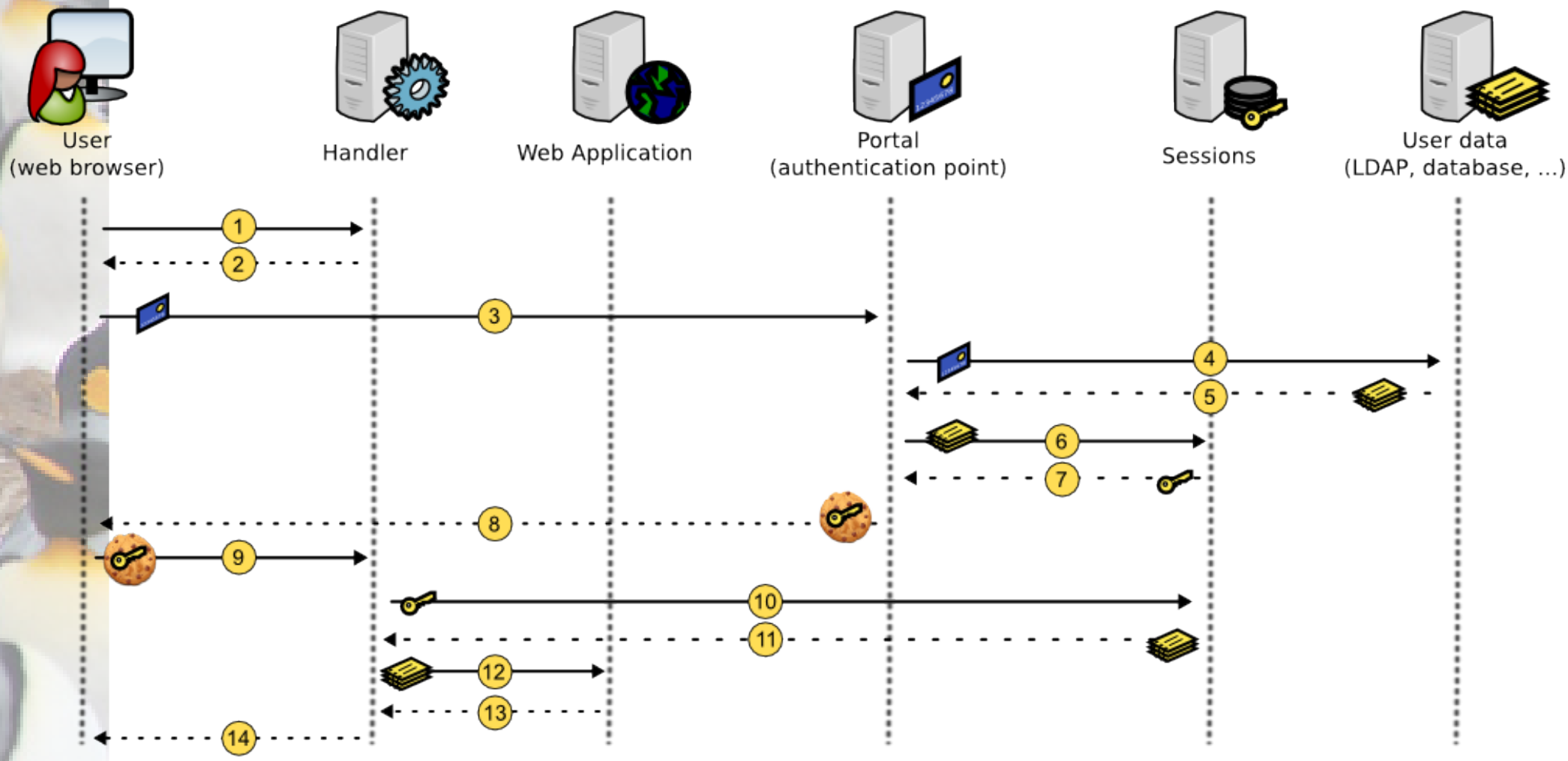
Architecture



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, ...)
- 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

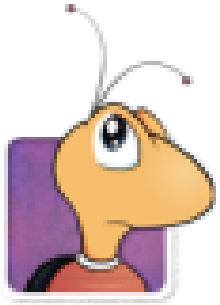
Règles d'accès

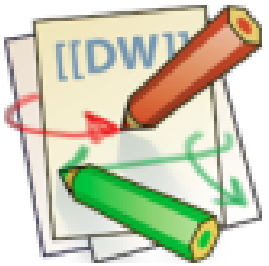
- Accès pour tous les utilisateurs authentifiés :
  - Default => accept
- Accès pour le groupe « admin » :
  - Default => $groups =~ /admin/
- Interception du logout de l'application :
  - ^/logout.php => logout_sso

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 :
  - Auth-User => $uid
  - Auth-Name => uc($sn)."; ".ucfirst($gn)

Applications nativement compatibles



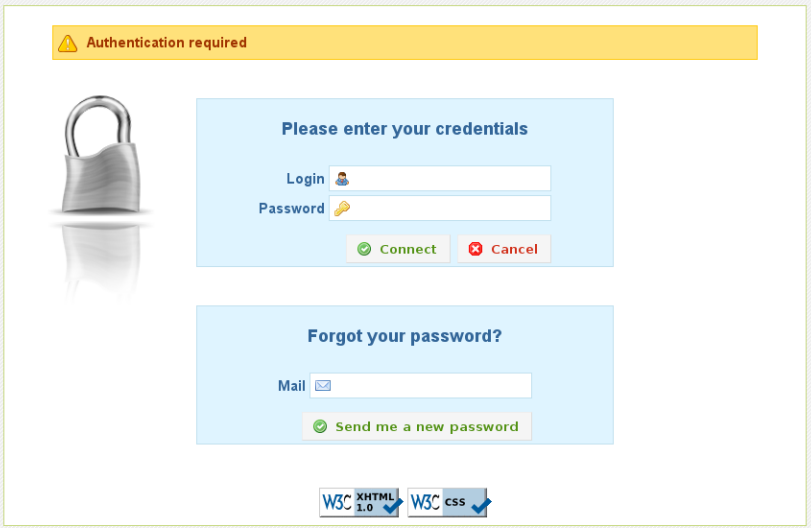


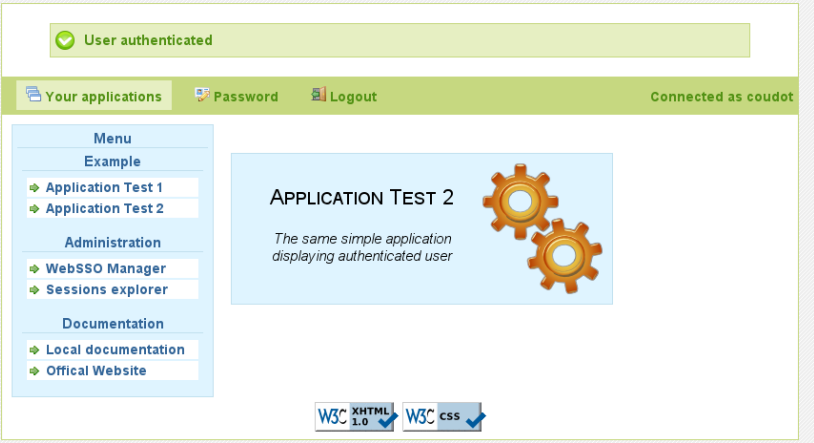
LINAGORA

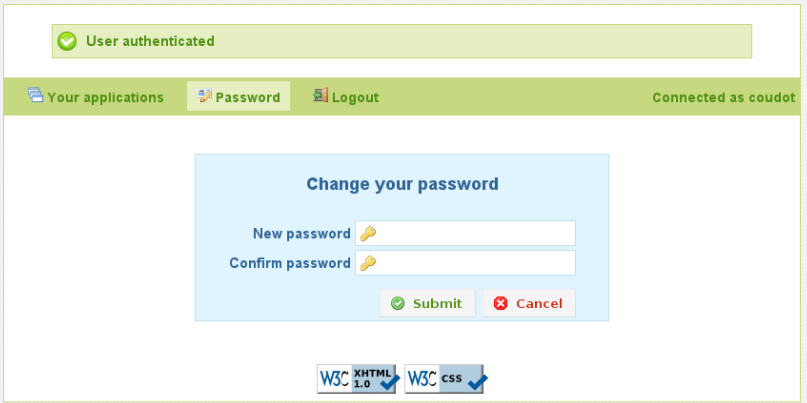
Autres applications compatibles

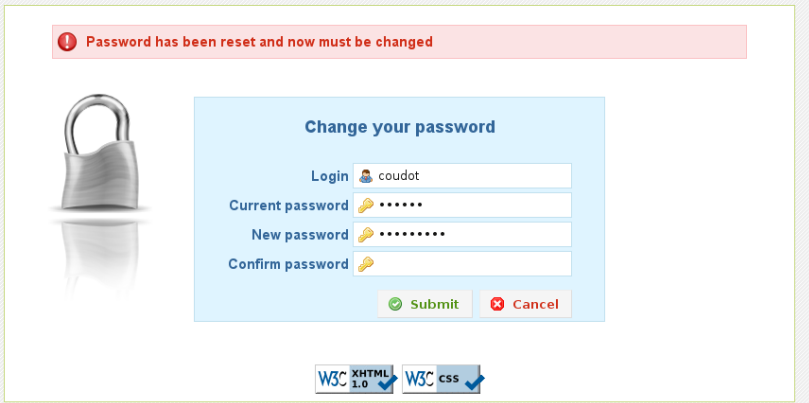
- Applications reposant sur la sécurité Apache (.htaccess) : Nagios, ...
- Applications reposant sur la sécurité Tomcat (users.xml) : Lutece, Probe, ...
- Applications utilisant HTTP Basic : Domino Web Access, Outlook Web Access, ...
- Applications compatibles SiteMinder

Quelques captures d'écran





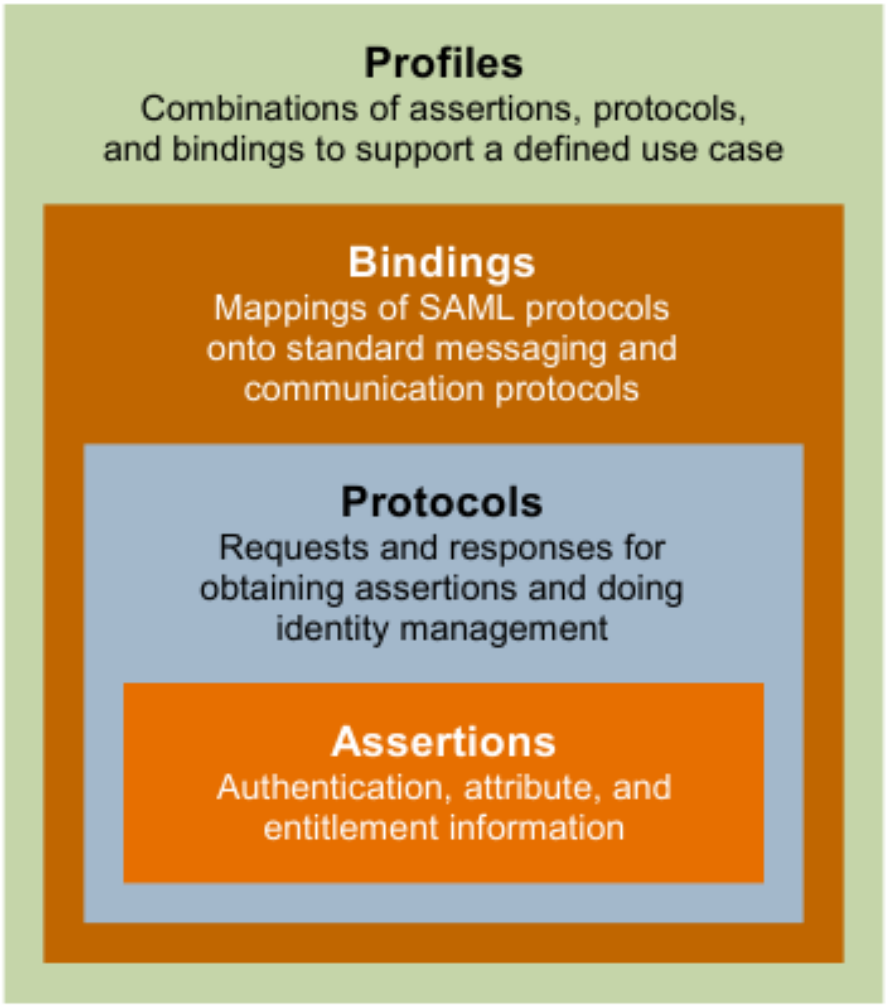




Le protocole SAML

- La fédération d'identité permet de créer des cercles de confiance entre fournisseurs de service et fournisseurs d'identités
- Les comptes des différents fournisseurs de services peuvent être fédérés avec le compte du fournisseur d'identité (ce compte est appelé principal)
- Chaque fournisseur de service dialogue alors avec le fournisseur d'identité pour s'assurer que l'utilisateur est bien reconnu sur le cercle de confiance
- Les standards d'origine SAML1, Liberty Alliance et Shibboleth convergent aujourd'hui vers SAML2
- SAML gère également la déconnexion (Single Logout), l'échange d'attributs, l'autorisation...

Concepts SAML

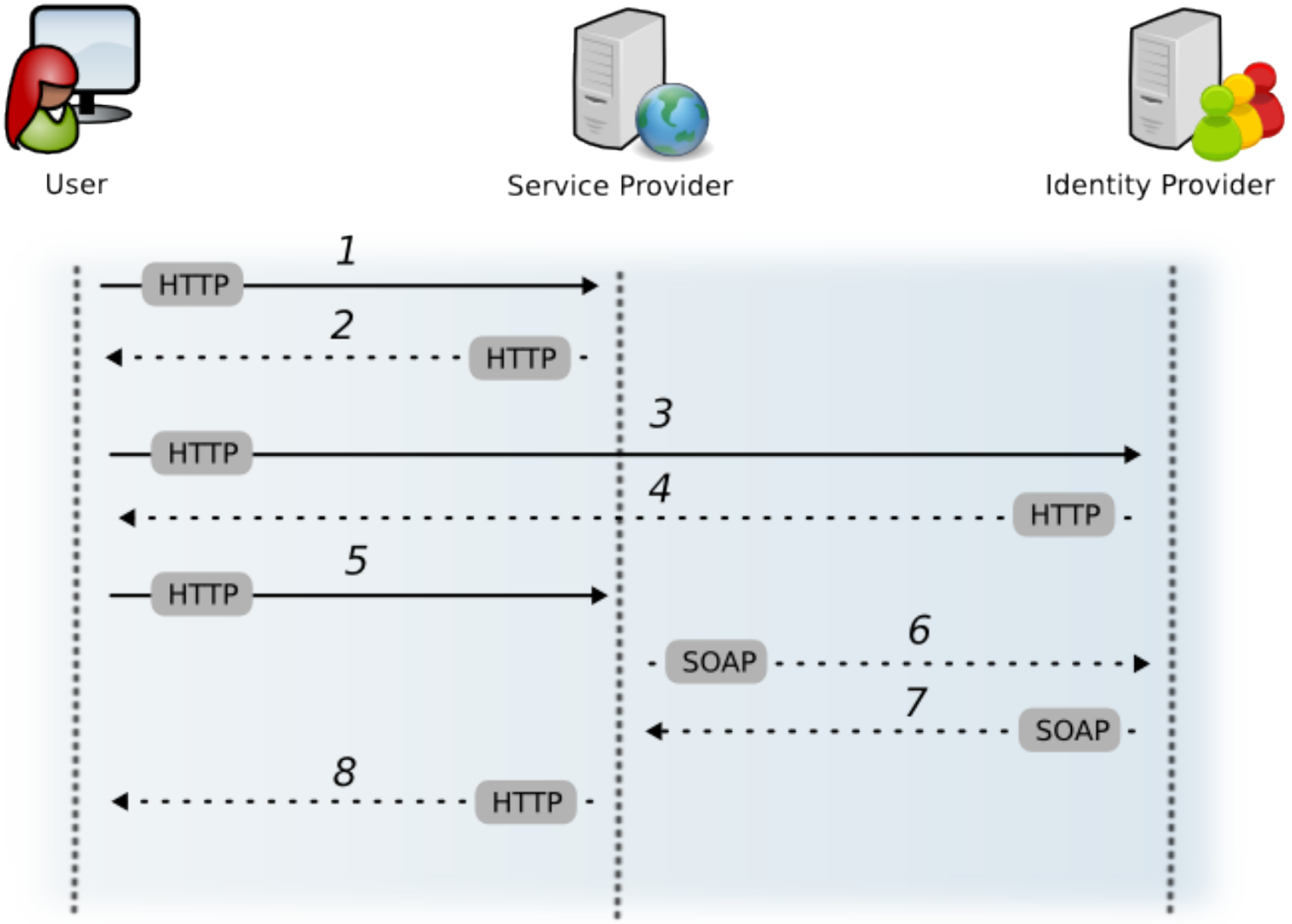


Authentication Context
Detailed data on types and strengths of authentication

Metadata
Configuration data for identity and service providers

SAML-concepts

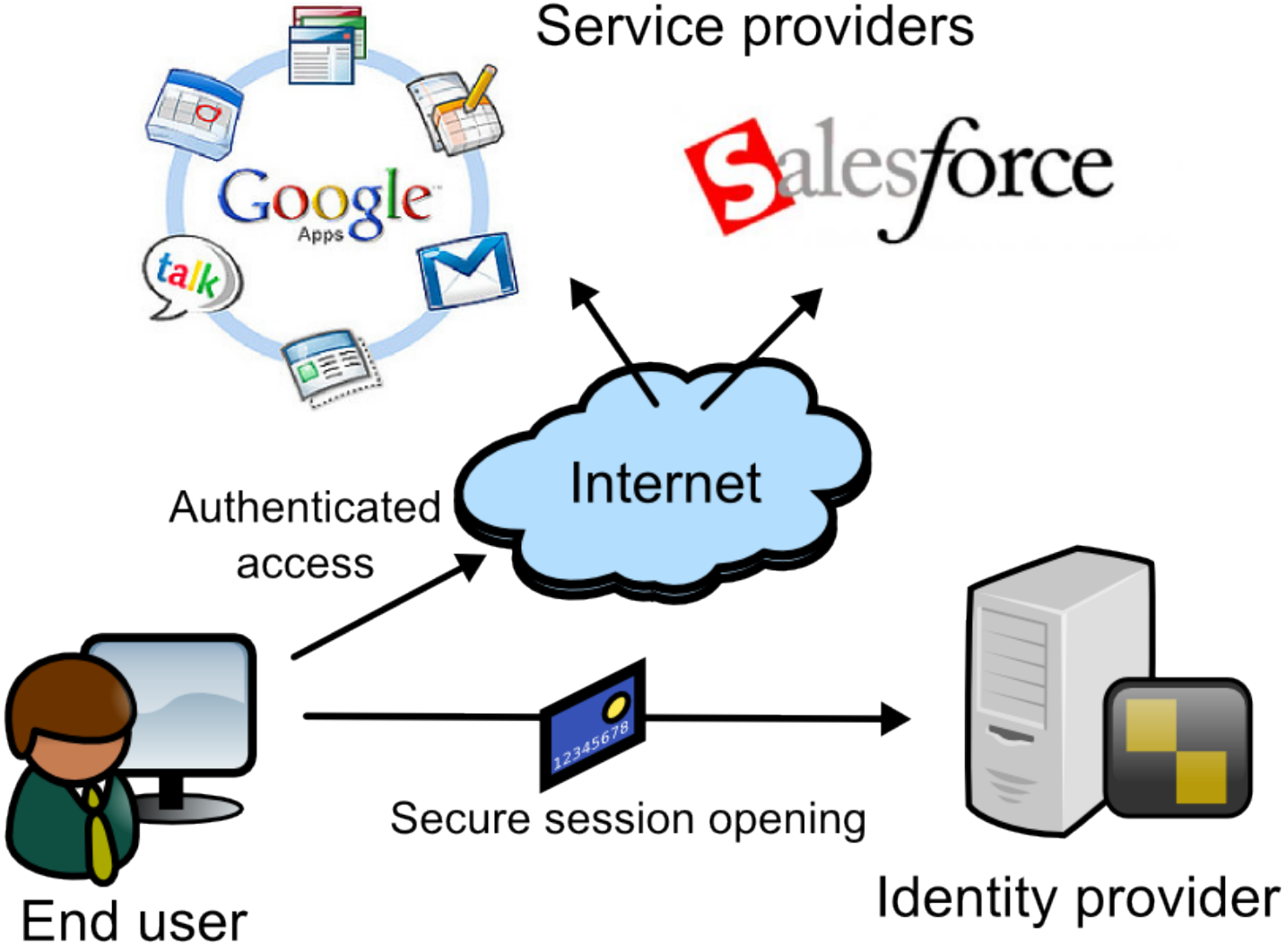
Cinématique d'authentification



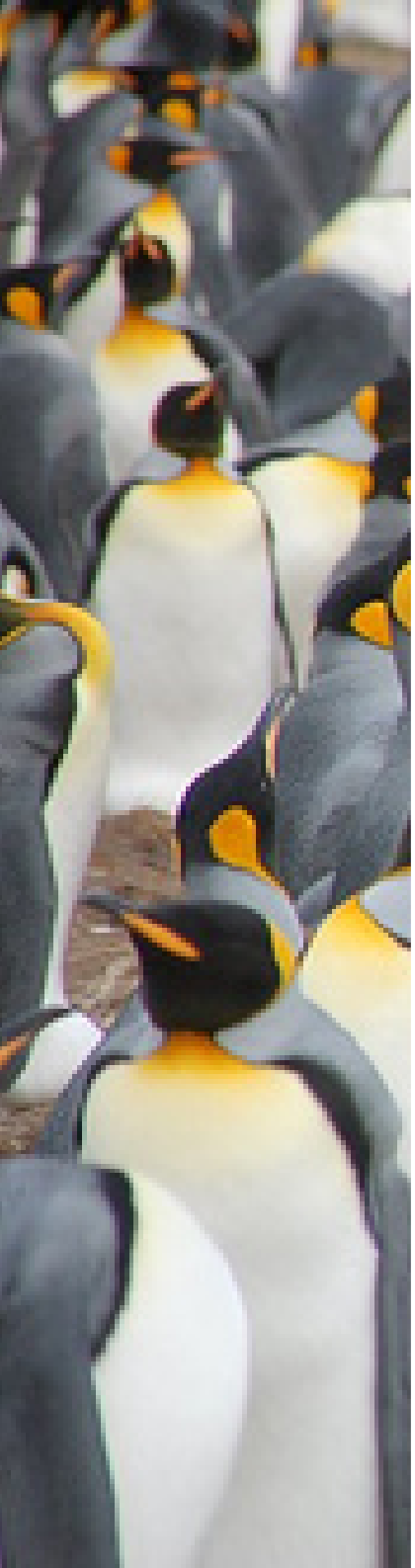
SAML2 et LemonLDAP::NG

- Utilisation de la bibliothèque GPL Lasso
- Modules :
  - LemonLDAP::NG en tant que fournisseur de service (SP) : l'authentification et la récupération d'attributs sont faites sur un fournisseur d'identité SAML2
  - LemonLDAP::NG en tant que fournisseur d'identité (IDP) : l'ouverture d'une session locale WebSSO ouvre également une session SAML2
  - LemonLDAP::NG en tant que fournisseur d'attributs (AA) : délivrance d'attributs issus de la session utilisateur
  - LemonLDAP::NG en tant que mandataire d'identité (Proxy IDP) : les modules SP et IDP sont activés simultanément

SAML dans la vraie vie



Démonstration



LINAGORA

Merci de votre attention

16, 17 et 18 MARS 2010