

Mise en Œuvre d'une Authentification Centrale et Unique à l'Université

Jean-Christophe Gay
Vincent Bruhier
Martial Lebec

Université Paris Dauphine

JRES 2013



1 Contexte

- Description du contexte
- Objectifs du projet

2 Mise en place d'une solution

- Kerberos
- Avantages & inconvénients
- Infrastructure mise au point

3 Déploiement et Accompagnement Utilisateur

- Déploiement en plusieurs phases
- Promotion auprès des utilisateurs
- Difficultés rencontrées

Situation initiale

- Une gestion de l'identité numérique découplée ;

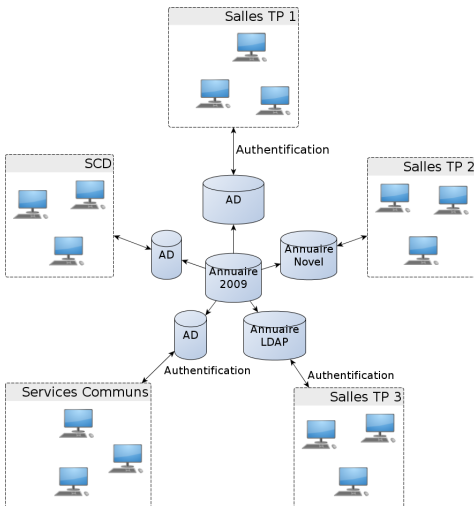
Situation initiale

- Une gestion de l'identité numérique découplée ;
- Des référentiels incomplets et nombreux ;

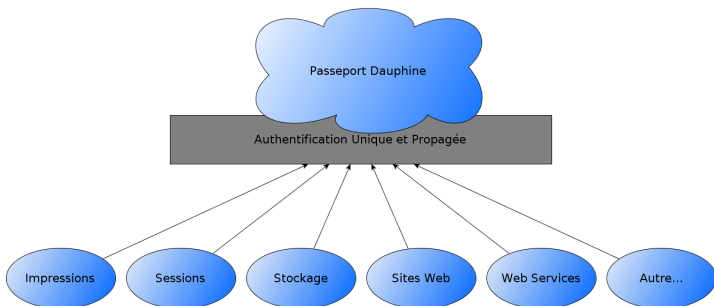
Situation initiale

- Une gestion de l'identité numérique découplée ;
- Des référentiels incomplets et nombreux ;
- Des identités dupliquées en partie.

Situation initiale



Situation visée



Objectifs

- Unification des identités ;

Objectifs

- Unification des identités ;
- Construction d'un référentiel unique et exhaustif ;

Objectifs

- Unification des identités ;
- Construction d'un référentiel unique et exhaustif ;
- Renforcement de la sécurité autour des mots de passe.

Objectifs

- Unification des identités ;
- Construction d'un référentiel unique et exhaustif ;
- Renforcement de la sécurité autour des mots de passe.

Un moyen d'action

Le mot de passe unique !

Avantages

Avantages d'un mot de passe unique :

- Un seul guichet pour les utilisateurs ;

Avantages

Avantages d'un mot de passe unique :

- Un seul guichet pour les utilisateurs ;
- Un seul référentiel à investiguer pour résoudre des problèmes ;

Avantages

Avantages d'un mot de passe unique :

- Un seul guichet pour les utilisateurs ;
- Un seul référentiel à investiguer pour résoudre des problèmes ;
- Un seul point d'accès au compte utilisateur.

Avantages

Avantages d'un mot de passe unique :

- Un seul guichet pour les utilisateurs ;
- Un seul référentiel à investiguer pour résoudre des problèmes ;
- Un seul point d'accès au compte utilisateur.

Inconvénients d'un mot de passe unique :

- Un seul mot de passe, une fois compromis le système est vulnérable.

Sommaire

1 Contexte

2 Mise en place d'une solution

- Kerberos
- Avantages & inconvénients
- Infrastructure mise au point

3 Déploiement et Accompagnement Utilisateur



Une solution : Kerberos

Kerberos

Kerberos est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs.

A voir

Nicolas Grenèche. (Securely) Kerberize my University. JRES 2011.
Guillaume Rousse. Kerberos, le sso universel. GNU/Linux Magazine Novembre 2011 et Retour d'expérience sur l'utilisation de Kerberos à l'INRIA, JRES 2011.

Avantages

L'utilisation de Kerberos présente certains avantages :

Avantages

L'utilisation de Kerberos présente certains avantages :

- SSO Système multi-OS (Windows, GNU/Linux, MacOS) ;

Avantages

L'utilisation de Kerberos présente certains avantages :

- SSO Système multi-OS (Windows, GNU/Linux, MacOS) ;
- Compatible avec CAS ;

Avantages

L'utilisation de Kerberos présente certains avantages :

- SSO Système multi-OS (Windows, GNU/Linux, MacOS) ;
- Compatible avec CAS ;
- Renforcement de la sécurité autour de l'utilisation du mot de passe ;

Inconvénients !

Notre approche comporte certains inconvénients :

Inconvénients !

Notre approche comporte certains inconvénients :

- la création du principal Kerberos nécessite le mot de passe de l'utilisateur ;

Inconvénients !

Notre approche comporte certains inconvénients :

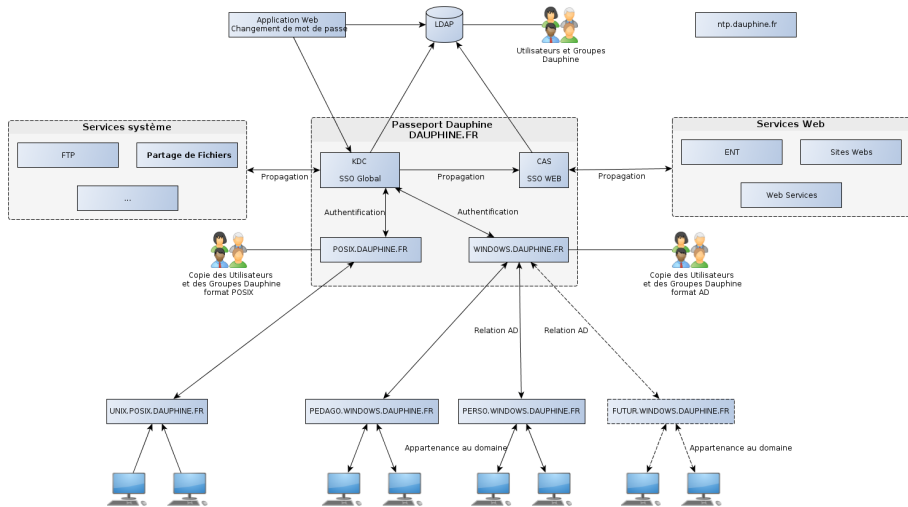
- la création du principal Kerberos nécessite le mot de passe de l'utilisateur ;
- les solutions de partage locales aux composantes sont gérées de manière globale ;

Inconvénients !

Notre approche comporte certains inconvénients :

- la création du principal Kerberos nécessite le mot de passe de l'utilisateur ;
- les solutions de partage locales aux composantes sont gérées de manière globale ;
- les gestions des parcs locaux doivent satisfaire à de nouvelles exigences ;

Schéma de l'infrastructure



Sommaire

1 Contexte

2 Mise en place d'une solution

3 Déploiement et Accompagnement Utilisateur

- Déploiement en plusieurs phases
- Promotion auprès des utilisateurs
- Difficultés rencontrées

Phases de déploiements

- 1 Remplacement de l'interface de gestion de compte. Mise en place des nouvelles règles de force des mots de passe. Création des principaux des nouvelles identités.

Phases de déploiements

- 1 Remplacement de l'interface de gestion de compte. Mise en place des nouvelles règles de force des mots de passe. Création des principaux des nouvelles identités.
- 2 Déploiement du nouveau server CAS, migration des applications web.

Phases de déploiements

- 1 Remplacement de l'interface de gestion de compte. Mise en place des nouvelles règles de force des mots de passe. Création des principaux des nouvelles identités.
- 2 Déploiement du nouveau server CAS, migration des applications web.
- 3 Transfert de compétences sur l'utilisation de la nouvelle authentification auprès des gestionnaires de parcs.

Phases de déploiements

- ➊ Remplacement de l'interface de gestion de compte. Mise en place des nouvelles règles de force des mots de passe. Création des principaux des nouvelles identités.
- ➋ Déploiement du nouveau server CAS, migration des applications web.
- ➌ Transfert de compétences sur l'utilisation de la nouvelle authentification auprès des gestionnaires de parcs.
- ➍ Promotion auprès des utilisateurs, incitation à l'obtention du « Passeport Dauphine ». Intégration dans des salles de TP.

Phases de déploiements

- ➊ Remplacement de l'interface de gestion de compte. Mise en place des nouvelles règles de force des mots de passe. Création des principaux des nouvelles identités.
- ➋ Déploiement du nouveau server CAS, migration des applications web.
- ➌ Transfert de compétences sur l'utilisation de la nouvelle authentification auprès des gestionnaires de parcs.
- ➍ Promotion auprès des utilisateurs, incitation à l'obtention du « Passeport Dauphine ». Intégration dans des salles de TP.
- ? Déploiement des domaines AD. Rattachement des postes individuels au projet.

Promotion auprès des utilisateurs

- Affichage dans le hall de l'Université ;

Promotion auprès des utilisateurs

- Affichage dans le hall de l'Université ;
- Distribution de flyers aux étudiants ;

Promotion auprès des utilisateurs

- Affichage dans le hall de l'Université ;
- Distribution de flyers aux étudiants ;
- Affichage dans les salle de TP et mise à disposition de kiosques pour changer son mot de passe ;

Promotion auprès des utilisateurs

- Affichage dans le hall de l'Université ;
- Distribution de flyers aux étudiants ;
- Affichage dans les salle de TP et mise à disposition de kiosques pour changer son mot de passe ;
- Mise en place d'une reconnaissance du type de compte sur l'ENT ;

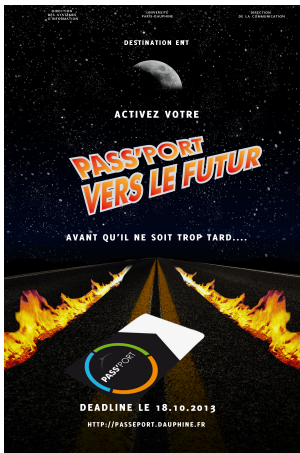
Promotion auprès des utilisateurs

- Affichage dans le hall de l'Université ;
- Distribution de flyers aux étudiants ;
- Affichage dans les salle de TP et mise à disposition de kiosques pour changer son mot de passe ;
- Mise en place d'une reconnaissance du type de compte sur l'ENT ;
- Campagne mail incitant à la modification du mot de passe à partir de l'ENT.

Promotion auprès des utilisateurs

- Affichage dans le hall de l'Université ;
- Distribution de flyers aux étudiants ;
- Affichage dans les salle de TP et mise à disposition de kiosques pour changer son mot de passe ;
- Mise en place d'une reconnaissance du type de compte sur l'ENT ;
- Campagne mail incitant à la modification du mot de passe à partir de l'ENT. **Pas d'url dans le mail !**

Documents de communication



DAUPHINE
UNIVERSITÉ PARIS

PASSEPORT

Migration Passeport

Dauphine se modernise afin de mieux protéger vos informations personnelles et de vous offrir un meilleur service.

Faites évoluer votre compte ENT en compte "Passeport Dauphine".

[Activer mon Passeport](#)

L'unique site qui peut vous demander votre mot de passe est :
<https://passeport.dauphine.fr/>

En cas de problème contactez : support.passeport@dauphine.fr

Difficultés rencontrées

Nous avons rencontrés quelques difficultés de la part des utilisateurs :

Difficultés rencontrées

Nous avons rencontrés quelques difficultés de la part des utilisateurs :

- Personnel récalcitrant au changement de mot de passe ;

Difficultés rencontrées

Nous avons rencontrés quelques difficultés de la part des utilisateurs :

- Personnel récalcitrant au changement de mot de passe ;
- Nouvelles règles plus contraignantes ;

Difficultés rencontrées

Nous avons rencontrés quelques difficultés de la part des utilisateurs :

- Personnel récalcitrant au changement de mot de passe ;
- Nouvelles règles plus contraignantes ;
- Avertissement mail signalé comme phishing ;

Difficultés rencontrées

Nous avons rencontrés quelques difficultés de la part des utilisateurs :

- Personnel récalcitrant au changement de mot de passe ;
- Nouvelles règles plus contraignantes ;
- Avertissement mail signalé comme phishing ;
- Invisibilité de la migration au « Passeport Dauphine ».

État d'avancée du projet

- Infrastructure déployée ;

État d'avancée du projet

- Infrastructure déployée ;
- Captation des identités en progression ;
- Captation de nouvelles identités ;

État d'avancée du projet

- Infrastructure déployée ;
- Captation des identités en progression ;
- Captation de nouvelles identités ;
- Il faut déployer les différents domaines AD pour y insérer les postes utilisateurs.

Perspectives



Perspectives

- Ouverture possible vers une fédération d'identités ;

Perspectives

- Ouverture possible vers une fédération d'identités ;
- Kerberos et OTP ;

Perspectives

- Ouverture possible vers une fédération d'identités ;
- Kerberos et OTP ;
- Mise en place de niveau de confiance SSO ;

Questions ???