



Single Sign On

(l'apport déterminant du SSO dans un projet d'IAM)

Yves RAISIN - bioMérieux

Sommaire

- Concepts du SSO
- Intégration du SSO dans un projet d'IAM
- Spécifications fonctionnelles et techniques du SSO
- L'offre du marché SSO lourd

Concepts du SSO

L'**authentification unique** (Single Sign On) est une méthode permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder ensuite à plusieurs applications informatiques.

Le SSO permet d'atteindre trois objectifs majeurs :

- *Simplifier la vie de l'utilisateur en gérant automatiquement le cycle de vie de ses mots de passe et l'authentification auprès des applications.*
- *Augmenter le niveau de sécurité (authentification forte, mots de passe complexes), mais également traçabilité des utilisateurs.*
- *Diminuer les coûts liés à la gestion des mots de passe et apporter à l'utilisateur une autonomie contrôlée.*

Comment ça marche

- *Le SSO va gérer les crédeniels de l'utilisateur en lieu et place de l'utilisateur*
- *Les crédeniels de l'utilisateur sont stockés dans un coffre-fort*
- *Le SSO remplace les utilisateurs pendant les phases :*
 - *D'authentification*
 - *De changement de mots de passe*

Typologie de SSO

- « *WEBSSO* »
Pour application Web
Nécessite des applications adaptées
- « *SSO LOURD* »
Pour toutes les applications
Plus complexe à mettre en oeuvre

La partie visible de l'IAM

La réussite d'un projet d'IAM nécessite l'adhésion de multiples fonctions de l'entreprise, de la direction générale à l'ensemble des utilisateurs : comment justifier le retour sur investissement ? comment en rendre visibles les bénéfices pour l'entreprise ? Plus simplement, comment obtenir cette adhésion ?

Le SSO, partie « émergée » de l'IAM est le moyen le plus simple de réaliser cette quadrature.

Le SSO dans l'IAM

On peut distinguer plusieurs axes dans la justification d'un projet d'IAM :

- *Le premier critère consiste à obtenir **l'adhésion des utilisateurs** pour le projet. Le SSO est le seul projet de sécurité plébiscité par les utilisateurs; c'est le seul projet de sécurité qui n'apporte pas de nouvelles contraintes, mais qui en supprime.*
- *Le second est **le retour sur investissement** : le SSO permet également de calculer et de justifier un ROI en diminuant les coûts de help desk, etc...*
- ***La sécurisation de l'accès au SI** : le SSO permet d'améliorer notablement le niveau de sécurité, via des mots de passe plus complexes, une tracabilité des actions des utilisateurs, l'adjonction d'éléments physiques, une sensibilisation non contraignante des utilisateurs à la sécurité.*
- *Dans la mise en place d'un projet IAM, **le SSO permet d'avoir un livrable rapide et visible de tous.***

Le SSO dans l'IAM

Responsable	Problème
DSI / RSSI	<ul style="list-style-type: none">☞ S'assurer de la robustesse des méthodes d'authentification☞ Éliminer les risques liés à l'authentification☞ S'assurer que la politique de sécurité définie est suivie
Direction Générale	<ul style="list-style-type: none">☞ S'assurer de la conformité du système d'information aux normes réglementaires (SOX, Bale II, LSF, FDA, HIPAA...)
Direction Financière	<ul style="list-style-type: none">☞ Diminuer les coûts de fonctionnement☞ Favoriser la productivité des employés☞ Optimiser les investissements
Support	<ul style="list-style-type: none">☞ Fournir le meilleur support aux utilisateurs☞ Se consacrer à des projets productifs

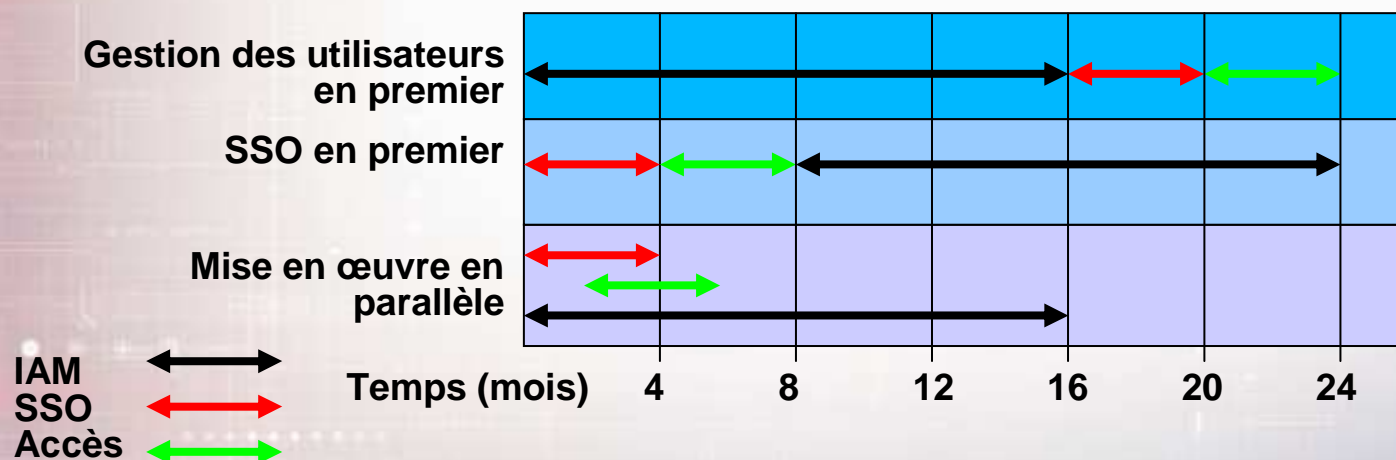
Le SSO dans l'IAM

Critère	Bénéfice	Bénéficiaire
Ergonomie utilisateurs	<ul style="list-style-type: none"> ☞ Réduction du nombre de mots de passe ☞ Réduction du temps d'authentification ☞ Gestion automatique des changements 	Utilisateurs Dir. Générale
Retour sur investissement	<ul style="list-style-type: none"> ☞ Diminution des appels au support ☞ Augmentation de la productivité des utilisateurs 	Support Dir. Générale Dir. Financière
Renforcement de la sécurité	<ul style="list-style-type: none"> ☞ Élimination des mots de passe notés en clair ☞ Possibilité de prendre en compte tous les types d'applications ☞ Augmentation de la complexité des mots de passe ☞ Changement périodique et automatique des mots de passe ☞ Renforcement du contrôle d'accès aux postes ☞ Audit des actions et événements 	RSSI DSI Dir. Générale

Le SSO dans l'IAM

La mise en œuvre des différentes étapes de votre projet IAM (Gestion des utilisateurs, SSO et Accès) peut être découpée dans le temps suivant plusieurs schémas :

- *La Gestion des utilisateurs en premier*
- *Le SSO en premier*
- *La mise en œuvre en parallèle des briques de l'IAM*



Couverture fonctionnelle

Une solution de SSO doit offrir les fonctions suivantes :

- *La gestion des crédeniels de l'utilisateur (SSO)*
- *L'authentification auprès du SSO et des applications secondaires (Accès)*
- *La traçabilité des utilisateurs*
- *Le Self Service*

Ces modules doivent garantir :

- *Une administration centralisée*
- *La gestion des éléments physiques*
- *Une haute disponibilité*
- *Des modes de connexion alternatifs*
- *Un mode non intrusif dans les applications*

Gestion des créidentiels

Comptes Multiples

- *Un utilisateur peut disposer de plusieurs créidentiels d'accès à une application.*
 - *Ex: un utilisateur est à la fois administrateur et utilisateur normal d'une application*

Comptes Partagés

- *Les créidentiels d'accès à une application doivent pouvoir être partagés entre plusieurs utilisateurs.*

Délégation

- *Un utilisateur doit pouvoir déléguer l'accès à une application en permettant à un autre utilisateur d'y accéder sans diffuser son identifiant/mot de passe.*
 - *Ex: déléguer l'accès à la messagerie pendant une absence*

Gestion des accès

Disponibilité d'un module d'authentification qui :

- *complète la GINA Microsoft*
- *doit être paramétrable*

Module qui doit permettre :

- *l'authentification par éléments physiques*
- *l'accès à des modes de connexion alternatifs*
- *un accès direct aux fonctionnalités de self service*

Traçabilité

Les audits doivent être dans un format standard (CSV, SQL...)

Ils doivent permettre de superviser :

- *Les connexions / déconnexions sur les postes de travail*

Les connexions (et éventuellement les déconnexions) applicatives

- *Les changements de mots de passe*
- *La délégation de crédeniels*
- *Les échecs de connexion/changements de mots de passe...*
- *Tout événement paramétré par l'administrateur.*

Self Service

Le Self Service doit permettre :

- A l'utilisateur :
 - *De débloquer sa carte lorsqu'il a oublié son code PIN.*
 - *De changer son mot de passe primaire lorsqu'il a perdu sa carte ou oublié son mot de passe primaire.*
- A l'administrateur :
 - *D'authentifier l'utilisateur par une série de Questions / Réponses avant de lui fournir les informations de déblocage de carte ou de connexion par Challenge/Response*

Administration centralisée

L'administration de la solution de SSO doit être centralisée et distribuée :

- *Appuyée sur les infrastructures existantes (AD, LDAP...)*
- *Gestion des profils utilisateurs*
- *Configuration des applications*
- *Gestion des éléments physiques*
- *Possibilité de distribuer des droits aux administrateurs applicatifs (via une interface web)*

Gestion des éléments physiques

Le déploiement des cartes/jetons doit être simplifié :

- *Auto-initialisation des éléments vierges*
- *Ré-authentification forte immédiate optionnelle*

La gestion des éléments physiques doit être centralisée :

- *Inscription dans l'annuaire*
- *Gestion des cartes vierges/perdues/rendues*
- *Gestion d'une liste Noire*

Disponibilité

Réplication des containers de l'utilisateur

Pour permettre une disponibilité du SSO, les crédeniels de l'utilisateur doivent pouvoir être répliqués dans différents types de supports :

- *Annuaire*
- *Carte à puce*
- *Cache local sur le poste*

Modes de connexion alternatifs

La solution de SSO doit assurer aux utilisateurs une totale continuité de service

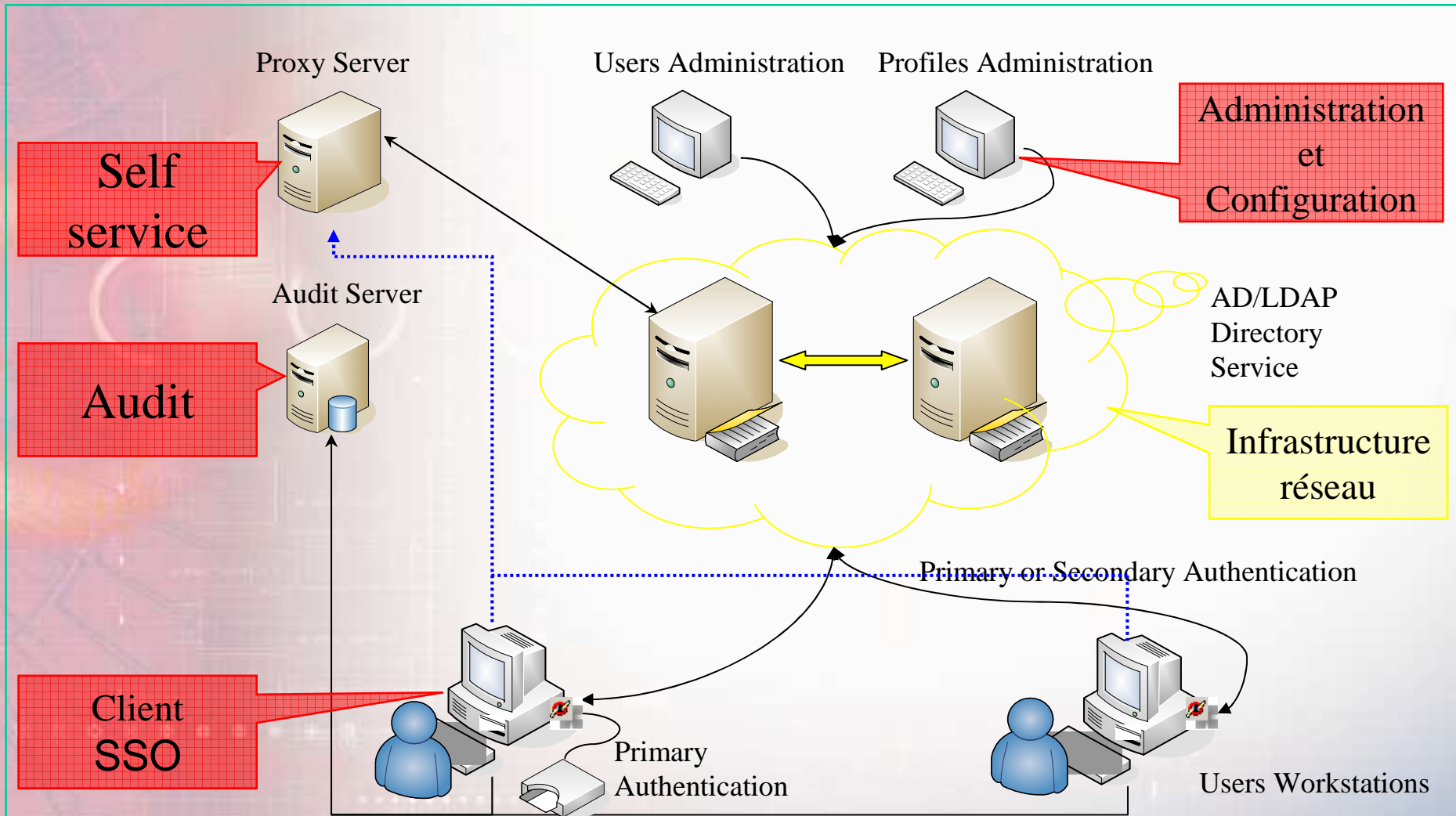
Exemples :

L'utilisateur s'authentifie avec un élément physique.

- *S'il oublie sa carte :*
- *S'il est connecté au réseau: l'administrateur doit pouvoir lui fournir un login et un mot de passe temporaire pour travailler.*
- *S'il n'est pas connecté au réseau (poste nomade): il doit pouvoir, via un mode type Challenge/Response, s'authentifier sur son poste.*
- *S'il bloque sa carte, il doit pouvoir la débloquer via un mode type Challenge / Response*

L'utilisateur s'authentifie avec un Login/Mot de passe (LDAP/AD), et que réseau n'est pas disponible, il doit pouvoir se reconnecter de manière transparente via le cache de connexion LDAP.

Infrastructure



Les acteurs du marché SSO lourd

PROTOCOM



Secure Login

PASSLOGIX



Enterprise SSO

EVIDIAN



Wiseguard

CITRIX



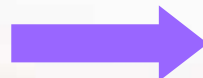
Password Manager

CA



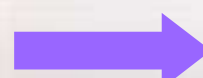
E-Trust SSO

AVENCIS



SSOX

UTIMACO



Safeguard SSO

Conclusions

Le SSO est un des leviers permettant de mieux appréhender un projet d'IAM

Il apporte des ions positifs à l'ensemble des fonctions de l'entreprise

En prenant les mesures adéquates, il permet un renforcement de la Politique de Sécurité des SI.