Contrôle d'Accès : Authentification Forte, Kiosque…

Principe du Contrôle d'Accès

Le contrôle d'accès permet de garantir l'identité de l'utilisateur par l'adjonction de mécanismes d'authentification forte (jeton cryptographique, carte à puce, calculette OTP, biométrie...).

SSOX supporte de nombreux modes d'authentification adaptés à l'ensemble des cas d'usage : postes personnels, identification rapide et sécurisée, support des modes de connexions dégradés, gestion des postes partagés (kiosque), gestion des grappes de postes (multiposte).

Fonctionnalités du Contrôle d'accès :

- **Authentification forte :**

  La bannière d'authentification de SSOX permet de gérer de multiples modes d'authentification :
  - par carte à puce ou jeton cryptographique ;
  - par carte sans contact ;
  - par carte et certificat ;
  - par Questions/Réponses ;
  - par mots de passe dynamiques (OTP) ;
  - biométrique (Match On card, Match On Server, Match On Device, Match On PC);
  - par identifiant/mot de passe.

- **Support du SmartCard Logon de Microsoft :**

  Le SmartCard Logon de Microsoft permet nativement une authentification par certificat sur les postes Windows. Lorsque ce mode d'authentification est utilisé, le mot de passe Windows de l'utilisateur n'est plus renouvelé. SSOX étend le mode de fonctionnement de Microsoft en gérant le renouvellement du mot de passe Windows et en permettant, en cas d'oubli de la carte, une authentification par Questions / Réponses (en mode connecté et déconnecté).

- **Support de multiples cartes à puces et jetons cryptographiques :**

  SSOX supporte la quasi-totalité des cartes et jetons du marché tels que les cartes Gemalto (.Net Classic Client, Cyberflex, Cryptoflex), Sagem YpsID, Aladdin eToken, cartes IAS et IAS ECC, Oberthur...

- **Support des modes de connexion dégradés :**

  En cas d'indisponibilité du réseau, un cache local sur la carte permet d'assurer l'authentification de l'utilisateur au poste de travail.

- **Contrôle d'accès :**

  Il est possible de mettre en place des politiques d'accès aux postes sur lesquels différentes populations d'utilisateurs auront le droit de se connecter en fonction des plages horaires définies.

- **Intégration avec le Self Service :**

  L'utilisateur peut accéder au Self Service depuis la bannière d'authentification pour s'authentifier par Questions/Réponses ou débloquer sa carte.

- **Support 32 et 64 bits :**

  Le contrôle d'accès de SSOX supporte toutes les versions de Windows 32bits (Windows 2000 XP / XPE / Vista / Seven / 2003 / 2003R2 / 2008) et de Windows 64bits (Vista / Seven / 2008 / 2008R2).

Poste Kiosque :

Le poste Kiosque permet de gérer les changements rapides d'utilisateurs sur un même poste de travail. Au démarrage, le poste effectue un auto-logon via un compte générique, puis le poste est immédiatement et automatiquement verrouillé. Les utilisateurs déverrouillent la session lors de leur authentification.

- **Changement rapide d'utilisateurs :**

  Un poste en mode kiosque permet de gérer les changements rapides d'utilisateurs. L'identification de l'utilisateur via une carte sans contact peut prendre moins de 2 secondes.

- **Gestionnaire de sessions :**

  Dans la session générique, le gestionnaire de sessions gère l'arrivée d'un nouvel utilisateur, le retour du même utilisateur et le verrouillage du poste.

Les scripts correspondant à chacune de ces 3 actions peuvent être définis et adaptés pour exécuter des opérations spécifiques.

- **Itinérance de session (*roaming*) :**

L'intégration avec les solutions de publication d'applications (Systancia / Citrix / TSE) est native.
Lors de son authentification sur le poste, les applications publiées, lancées par l'utilisateur, sont automatiquement connectées et reconnectées si l'utilisateur a changé de poste.

- **Session virtuelles :**

Les sessions virtuelles permettent de gérer, en local, des bureaux Windows propres à chaque utilisateur. Chaque utilisateur peut donc lancer ses applications qui sont masquées aux autres utilisateurs du poste.
L'utilisateur possède un bureau Windows qui s'exécute sous sa propre identité ; les applications sont lancées avec les droits de cet utilisateur (ex. : Outlook).
En option, si l'utilisateur ne s'est pas reconnecté dans un certain délai (paramétrable), son bureau Windows peut être fermé.

- **Identification rapide :**

L'option d'identification rapide permet, après une authentification forte réussie (carte et certificat), de générer un jeton de session qui est stocké sur les parties contact et sans contact de la carte. Ce jeton de session permet une **identification rapide sécurisée** de l'utilisateur par une simple présentation de la carte pendant la durée de validité du jeton de session, **sur n'importe quel autre poste kiosque** de l'entreprise.

Grappes de postes :

L'accès à plusieurs postes simultanément avec une authentification forte pose des problèmes spécifiques : en effet, l'utilisateur n'a qu'une seule carte ou qu'un seul capteur biométrique, mais plusieurs postes. Ce cas d'usage se rencontre fréquemment sur les postes des *traders* dans les salles de marché bancaires.
La solution multiposte de SSOX permet à un utilisateur de ne s'authentifier qu'une seule fois sur l'un des postes (maitre). L'ensemble des autres postes suivent automatiquement la politique qui a été définie pour cette grappe de postes en fonction de l'état du poste maitre.

- **Gestion des grappes de postes :**

La stratégie de gestion de postes multiples est définie par le poste maitre qui gouverne le comportement des autres postes de la grappe.

- **Gestion des stratégies :**

Le poste maitre définit le comportement des postes esclaves lors de l'arrêt du poste maitre, lors d'une coupure réseau entre le poste esclave et le poste maitre. Les différentes stratégies peuvent exécuter un arrêt de la session, un verrouillage des postes...

- **Signature :**

Lors d'une demande de réauthentification par une application, la demande de réauthentification est automatiquement redirigée vers le poste maitre sur lequel se trouve le capteur biométrique ou l'élément physique d'authentification.

- **Délégation :**

Un utilisateur peut déléguer la supervision de l'un de ses postes à un autre utilisateur, s'il y est autorisé.

AVENCIS
8, passage Brûlon
F-75012 Paris – France

☎: +33 (0)1 755 78 755
✉: info@avencis.net
🌐: http://www.avencis.net/