MPP SIGN & GO D'ILEX

Solution pour la gestion des identités et des accès : MPP SIGN & GO D'ILEX

Sign&go est une solution complète de signature unique (Single Sign On) performante et souple. Elle répond à l'ensemble des problématiques de contrôle d'accès, de web SSO et de eSSO tout en apportant des services de réinitialisation de mot de passe ou encore de fédération d'identités et d'audit. Compatible avec l'ensemble des applications du marché et les environnements client léger, elle s'adapte à des environnements variés et hétérogènes et permet de renforcer la sécurité des applications. Elle en facilite l'usage car elle simplifié les phases d'authentification**.**

Sign&go en bref

✓ Authentification forte puis contrôle d'accès

Sign&go est un produit de SSO modulaire et conçu de façon à correspondre à l'ensemble des besoins du marché en matière de sécurité des échanges et de Single Sign-On. Il facilite le déploiement et l'utilisation de moyens d'authentification forts. Aussi bien dans un contexte web, avec la mise en place de Serveur d'authentification supportant un grand nombre d'authentifications forte du marché (Certificats X505, Radius, OTP, Kerberos, CPS, RFID…) que dans un contexte « poste » avec le déploiement de Login Windows (Sign&go Login) spécifiques (CPS, PKCS#11, Carte sans contact, Citrix…)
Sign&go permet ensuite d'appliquer des politiques de sécurité multicritères d'accès aux ressources (période, topologie, moyen d'authentification, informations de profil, interrogation d'outils de gestion de droits).
Véritable point de contrôle, Sign&go est à même de contrôler l'accès aux applications en amont de ces dernières en fonction de critères définis dans les référentiels de l'entreprise. Sign&go est ainsi le complément idéal d'une solution de gestion des identités en appliquant la sécurité définie.

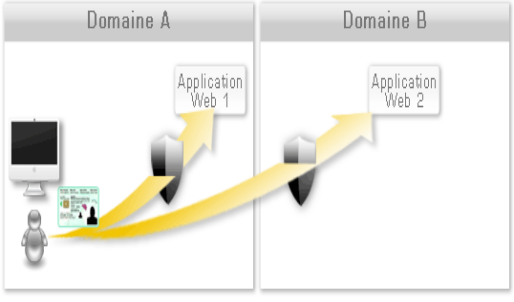
✓ Web Single Sign on (Web SSO)

Conforme à l'état de l'art en termes de contrôle d'accès Web, Sign&go n'impose pas d'installation sur les postes des utilisateurs, la protection est opérée via des agents installés indifféremment sur les serveurs Web ou Reverse-Proxy existants. Sign&go est ainsi à même de prendre en charge la protection des infrastructures de type Intranet et Extranet de l'entreprise.

La fonction de SSO de Sign&go est la plus souple du marché. Il est ainsi possible d'automatiser l'authentification de l'utilisateur sur ses applications suivants de nombreuses stratégies dont certaines ne nécessitent ni de synchroniser les annuaires, ni d'être intrusif sur les applications.

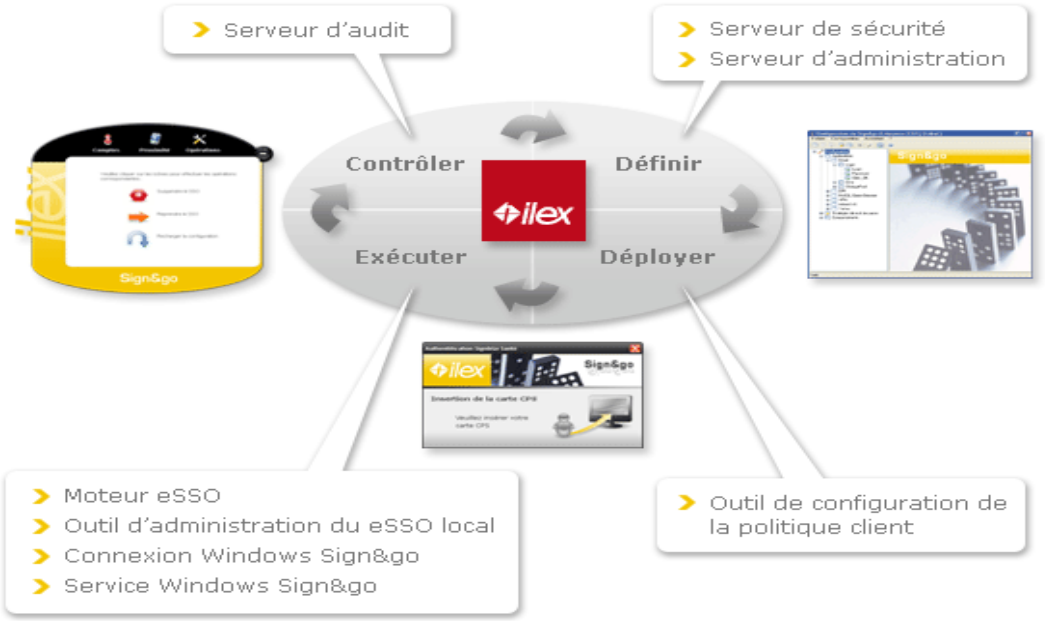
✓ Federation d'identités

La propagation des identités dans des systèmes hétérogènes est devenue un véritable défi, aussi bien pour les grands groupes internationaux que pour les échanges B2B.
Compatible avec les protocoles de fédération d'identité (SAMLv1, SAML v2 et OAuth2), Sign&go assure la pérennité de l'infrastructure sécurité de l'entreprise en l'autorisant à tisser des partenariats de propagation d'identités avec ses partenaires. Ceci permet notamment de répondre aux problématiques d'externalisation des applications de l'entreprise.
Sign&go est en mesure de propager une authentification vers un site partenaire en lui fournissant l'identité des utilisateurs. De même, il est capable d'exploiter une authentification réalisée par un système tiers en exploitant les assertions SAML transmises par une infrastructure Liberty Alliance.



Enterprise Single Sign on (E-SSO)

Avec Sign&go eSSO, l'enrôlement des applications client/serveur devient une opération triviale'. Il suffit en effet de viser les fenêtres, les champs et les boutons que l'on veut prendre en compte. Après une phase d'auto-Apprentissage, Sign&go s'occupe non seulement de jouer les authentifications secondaires mais également des phases de changement de mot de passe avec génération automatique respectant la stratégie de sécurité de l'application.
Enfin, Au travers d'une interface utilisateur conviviale, il est possible de gérer ses différents comptes applicatifs, la remise à zéro des accréditations secondaires et l'activation ou non du SSO sur le poste.
Entre exigence de sécurité, performance et ergonomie, la solution d'E-SSO proposée par Ilex permet :
d'automatiser les opérations de changement de mots de passe,
d'améliorer la productivité des collaborateurs,
de réduire les coûts de gestion,
de renforcer la sécurité de vos systèmes.



✓ Self-service

Ce mode alternatif d'authentification permet de répondre à la problématique de perte ou d'oubli du badge ou encore du mot de passe primaire. Accessible directement depuis la mire d'authentification Windows ou à travers une interface web, il est proposé à l'utilisateur de s'authentifier au travers d'un système de questions/réponses. La toute première fois que l'utilisateur se connecte au SSO, il devra renseigner un ensemble de questions/réponses, le nombre et la nature des questions pouvant être déterminé par l'administrateur.
On distingue deux types de questions :
Les questions administratives, définies par l'administrateur
Les questions personnelles, définies par l'utilisateur.
L'administrateur peut également définir le score autorisé pour réaliser l'authentification, les questions seront alors tirées aléatoirement et proposées à l'utilisateur.
Enfin, un niveau d'authentification peut être positionné pour une connexion par self-service : ainsi l'utilisateur connecté en mode dégradé peut être limité quant à ses accès aux applications sensibles.

✓ Self-service

Ilex a conçu un « e-SSO Bridge » dans Sign&go 5.0. Ce composant permet de traiter les problématiques de SSO sur des applications Client/Serveur au travers de cinématiques purement Web et de flux purement HTTP. Dans la pratique, l'utilisateur peut accéder à ces applications locales via un portail, et ce sans aucun déploiement préalable.

✓ Mobility Center

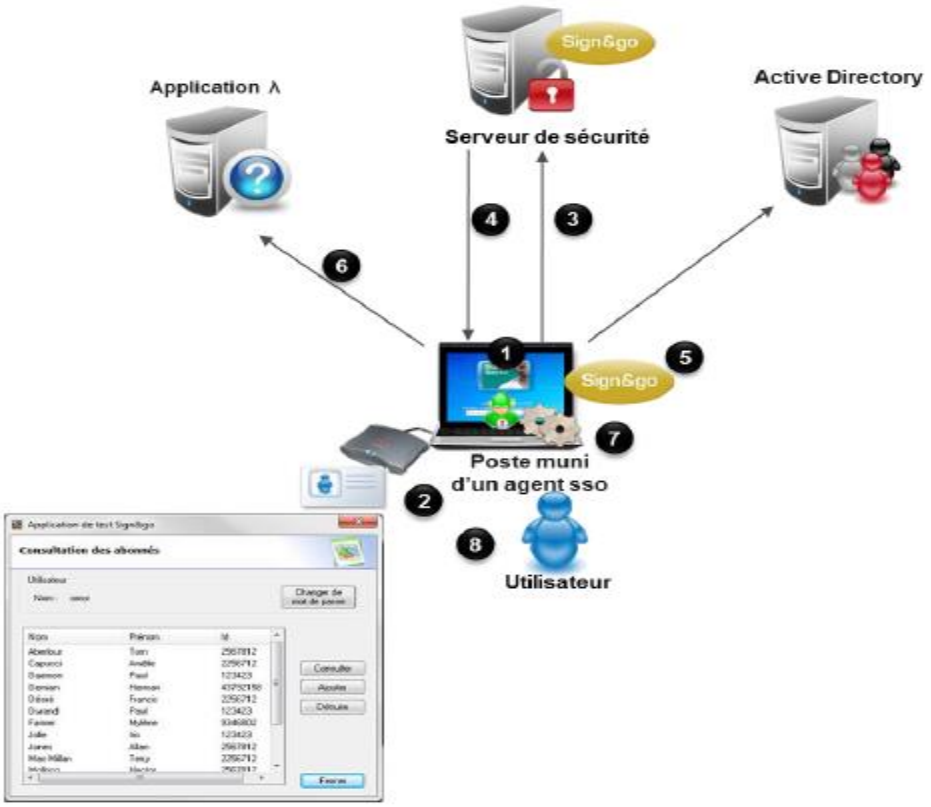
Sign&go Mobility Center permet de gérer et d'intégrer à une infrastructure Sign&go des périphériques mobiles de type tablettes :
Tablettes fonctionnant sous système Google Android (exemple : Samsung Galaxy Tab)
Tablettes fonctionnant sous iOS (exemple Apple iPad2 ou iPad3).
Sign&go Mobility Center répond aux deux grandes stratégies d'intégration de ce type de périphériques mobiles :
La mise en libre-service de tablettes : l'entreprise dispose d'un ensemble de tablettes banalisées qu'elle veut affecter dynamiquement à des utilisateurs ayant besoin de ces périphériques pour effectuer des tâches demandant de la mobilité. La tablette n'est pas donnée de façon permanente à un utilisateur mais affectée de façon temporaire pour permettre d'assurer un service.
Le support des tablettes appartenant aux collaborateurs de l'entreprise ou **BYOD** (« ***Bring your own device*** ») : Les collaborateurs possèdent une tablette personnelle qu'ils souhaitent utiliser dans le cadre de leur travail. Il s'agit de conditionner cette utilisation aux règles de sécurité de l'entreprise et de permettre simplement à l'utilisateur de rejoindre le Système d'Information.

Audit

Sign&go est muni d'un moteur de journalisation historisant l'ensemble des événements d'authentification et d'habilitation. Ce moteur, intégré au serveur de sécurité, facilite la consolidation d'informations d'audit sous la forme de fichiers ou bien directement en base de données.
Une application Sign&go indépendante permet d'afficher les informations d'audit de manière lisible. Cette application est accessible à partir de l'interface d'administration Sign&go.
Sign&go fournit également un générateur de rapports d'audit, application Web qui propose des rapports instantanés sur l'utilisation des applications protégées par Sign&go sur une période donnée. Il bénéficie d'une grande modularité sur les formats de génération des rapports (pdf, docx, pptx, csv, xls, html, rtf, xml), et il est possible de rajouter simplement de nouveaux rapports en fonction des besoins.

Architecture logique Sign&go eSSO

Nous invitons le lecteur à se référer à l'annexe de présentation de Sign&go fournie en annexe à notre réponse pour bien appréhender différents composants du produit.
La cinématique ci-après met en œuvre les différents composants de la solution :



1. Le poste est protégé par Sign&go qui propose différentes méthodes d'authentification
L'utilisateur réalise une authentification : login/mot de passe, certificats (carte, token…)
Le Serveur de sécurité vérifie l'identité de l'utilisateur (par exemple la validité du certificat.)
Un jeton SSO est généré pour l'utilisateur avec une durée de vie paramétrable.
Sign&go démarre la session Windows de l'utilisateur
L'utilisateur lance une application
Le moteur de SSO détecte la fenêtre d'authentification et transmet les accréditations de l'utilisateur à l'application
L'utilisateur accède à l'application (en étant authentifié)
En résumé les composants fournis par la solution sont les suivants :

Avec, pour ce qui est déployé au niveau des postes de travail :

Choix des solutions iLex

- **Des solutions complètes, modulaires, non intrusives et basées sur les standards du marché**
- **Une mise en œuvre itérative et pragmatique (par lot), favorisant les aspects fonctionnels et métier du projet**
- **L'apport rapide de services utilisateurs et l'utilisation du provisioning et de la gestion des droits à bon escient**
- **Une maîtrise de la solution par les équipes de ses clients**
- **L'intervention de spécialistes du domaine et le bénéfice de nombreuses expériences**
- **Une réactivité et une proximité accrues**