Cible de sécurité
Enterprise SSO v8.06

Référence : 39 F2 46LZ 01
Date : 24/01/2017
Version : 1.2
Etat du document : Définitif

A l'attention de :	**Copie :**
Secrétariat général de la défense et de la sécurité nationale Agence nationale de la sécurité des systèmes d'information Centre de certification 51, boulevard de La Tour-Maubourg 75700 PARIS 07 SP France	
Emetteur Evidian :	**Copie :**
Gérard DEDIEU Titre : Product Manager Email : gerard.dedieu@evidian.com	Thierry Winter Email : thierry.winter@evidian.com

Modification(s) du document

Date Version	Motif	Rédacteur
12/12/2014 Version 1.0	Version initiale	Evidian
18/12/2014 Version 1.1	Mise à jour sur l'ensemble du document	Evidian
24/01/2017 Version 1.2	Changement de version	Evidian

Sommaire

1. Identification du produit 4
2. Argumentaire du produit 5
2.1 Description générale du produit 5
2.2 Utilisation du produit 8
2.3 Environnement d'utilisation 9
2.4 Utilisateurs du produit 9
2.5 Hypothèses sur l'environnement 10
2.6 Périmètre de l'évaluation 10
3. Environnement technique de fonctionnement du produit 11
4. Biens sensibles devant être protégés 12
4.1 Données applicatives 12
4.2 Evènement d'audit 12
5. Description des menaces 13
5.1 Agents menaçants 13
5.2 Liste des menaces 13
6. Spécification des fonctions dédiées à la sécurité 15
6.1 Liste des fonctions de sécurité 15
6.2 Argumentaire des fonctions de sécurité 15
6.3 Spécification des mécanismes cryptographiques 16

1. Identification du produit

Cette cible de sécurité a été élaborée en vue d'une évaluation Certification Sécurité de Premier Niveau (CSPN).

Organisation éditrice	Evidian
Lien vers l'organisation	https://www.evidian.com/fr
Nom commercial du produit	Enterprise SSO
Numéro de la version évaluée	8.06b5386.30
Catégorie de produit	Identification, authentification et contrôle d'accès Audit

2. Argumentaire du produit

2.1 Description générale du produit

Le système Enterprise SSO (Single Sign-On) est un système d'authentification unique.

Ce système permet aux utilisateurs du SI (Système d'Information) de s'authentifier une seule fois pour toute la durée d'une session, indépendamment du nombre d'applications qui nécessitent une authentification.

Les utilisateurs du SI peuvent alors accéder à leurs données en toute transparence, sans contrainte de ressaisie d'un nouveau couple nom d'utilisateur/mot de passe. « Enterprise SSO » permet donc :

- **de faciliter l'administration des droits d'accès** : en centralisant les identifiants et mots de passe des utilisateurs, ce qui permet aux administrateurs de consacrer moins de temps aux tâches de gestion de mots de passe. Ainsi, certaines applications partagent la même authentification, tandis que d'autres disposent de bases d'utilisateurs dédiées.

- **de simplifier l'informatique aux utilisateurs** : la saisie et le renouvellement de mots de passe s'effectuent automatiquement. Les utilisateurs gagnent du temps et accèdent sans contrainte à leurs applications (qu'il s'agisse de clients Windows ou d'applications web : domaine Windows, portail CRM, applications Oracle ou SAP, messagerie ou portail fournisseurs). Les utilisateurs se consacrent à leurs tâches sans craindre d'oublier un mot de passe, et sans devoir en changer fréquemment selon des critères toujours plus complexes : caractères spéciaux, longueur, casse…

- **d'améliorer la sécurité d'accès** : l'utilisateur n'a plus une multitude d'authentifiant à retenir. Il se contente de mémoriser son mot de passe principal. Il n'y a donc plus de mots de passe notés sur un Post-it, ou communiqués à un autre utilisateur lorsqu'il a oublié le sien. Impossible également de multiplier abusivement le même mot de passe sur plusieurs applications.

- **de déléguer des accès à d'autres utilisateurs :** un utilisateur peut déléguer à un autre utilisateur l'accès à une application, sans faire appel au help desk. Il le fait sans communiquer son mot de passe et pour la période qu'il détermine. L'utilisateur peut ainsi anticiper ses absences imprévues (maladie). Il utilise pour cela son agent SSO (voir figure 1). Les délégations se font sous le contrôle strict de la politique de sécurité définie par l'administrateur de sécurité SSO. Cette politique définie ce qui peut être délégué, dans quelles circonstances et qui peut être délégué. Les accès délégués sont logués et audités.

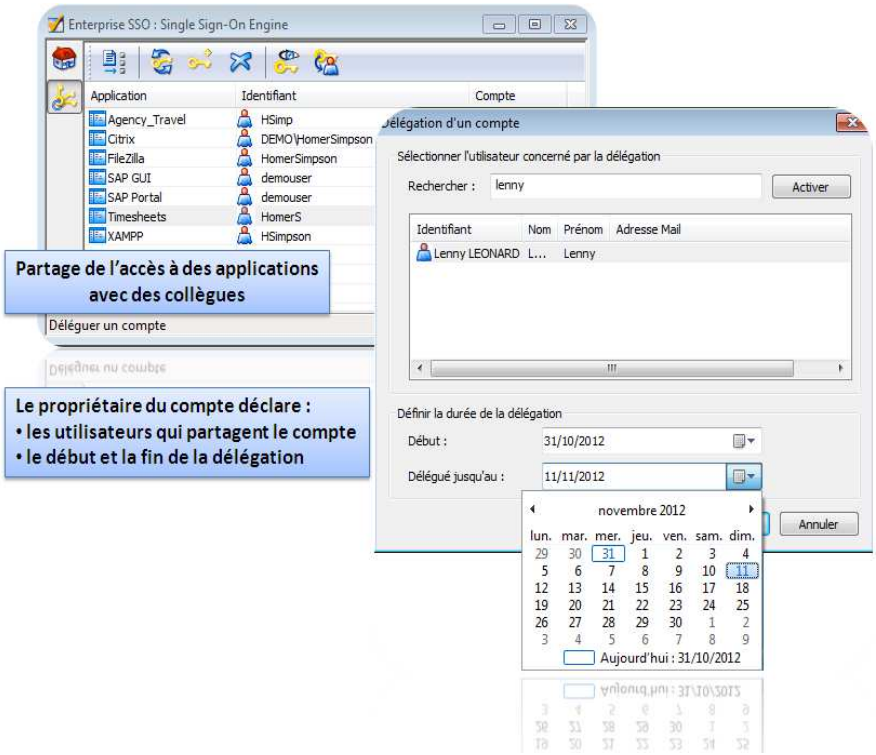

Figure 1 : Agent SSO de l'utilisateur

(Le compte et le mot de passe primaires sont les identifiants du système d'exploitation sur le poste de travail de l'utilisateur).

Les trois types d'architectures d'un système d'authentification unique sont:

- **Serveur de SSO** : les informations sont stockées sur un serveur, par exemple Novell ou Unix, qu'il faut généralement dédier à cette tâche. Le client sur le PC interroge donc le serveur quand c'est nécessaire. Ce serveur est souvent répliqué en plusieurs instances pour une plus grande disponibilité et capacité, même si des mécanismes de cache sur le PC permettent de pallier à une indisponibilité temporaire. Des coûts de démarrage et d'opération doivent donc être pris en compte : serveurs, installation du logiciel, synchronisations périodiques de sa base de compte utilisateurs avec l'annuaire en place dans l'entreprise. Dans une entreprise distribuée, le nombre de ces serveurs peut être important, les synchronisations de comptes complexes présentant un risque de cohérence pour la gestion des droits d'accès.

- **« Appliance » de SSO** : matériels et logiciels sont livrés ensemble Par contre, il n'est pas possible d'installer le logiciel sur un serveur existant, ce qui peut augmenter les coûts de mise en place. Enfin, il est souvent impossible d'ajouter mémoire et disque sur une « Appliance », contrairement à un serveur. La solution « Appliance » a une capacité limitée, elle nécessite plusieurs instances d'« Appliance » pour chaque environnement (production, intégration, site de secours), elle introduit un nouveau système d'exploitation, un nouvel annuaire à synchroniser. Comme ci-dessus, les

synchronisations de comptes complexes présentent un risque de cohérence pour la gestion des droits d'accès.

- **Annuaire de l'entreprise** : les informations de SSO sont tout simplement stockées, sous forme chiffrée, dans l'annuaire, garantissant un haut niveau de confidentialité avec un chiffrement de type AES256. Par exemple : l'annuaire Microsoft Active Directory où sont déclarés les utilisateurs et par lequel ils accèdent à leur session Windows, ou bien son instance applicative Microsoft AD-LDS dans lequel peuvent être stockées des données d'applications associées aux utilisateurs déclarés dans l'Active Directory. Il n'y a donc aucun serveur ni Appliance à installer. Les stations sont déjà configurées pour accéder aux informations, puisqu'elles accèdent déjà à l'annuaire.

Le système Enterprise SSO utilise une architecture basée sur l'annuaire de l'entreprise. Cette solution est la plus simple et la plus rapide à mettre en œuvre, en gardant un niveau de sécurité élevé.

2.2 Utilisation du produit

Le produit Enterprise SSO fonctionne sur les systèmes d'exploitation de type Windows et permet aux utilisateurs de se connecter à leurs applications.

Le principe de fonctionnement du produit est le suivant :

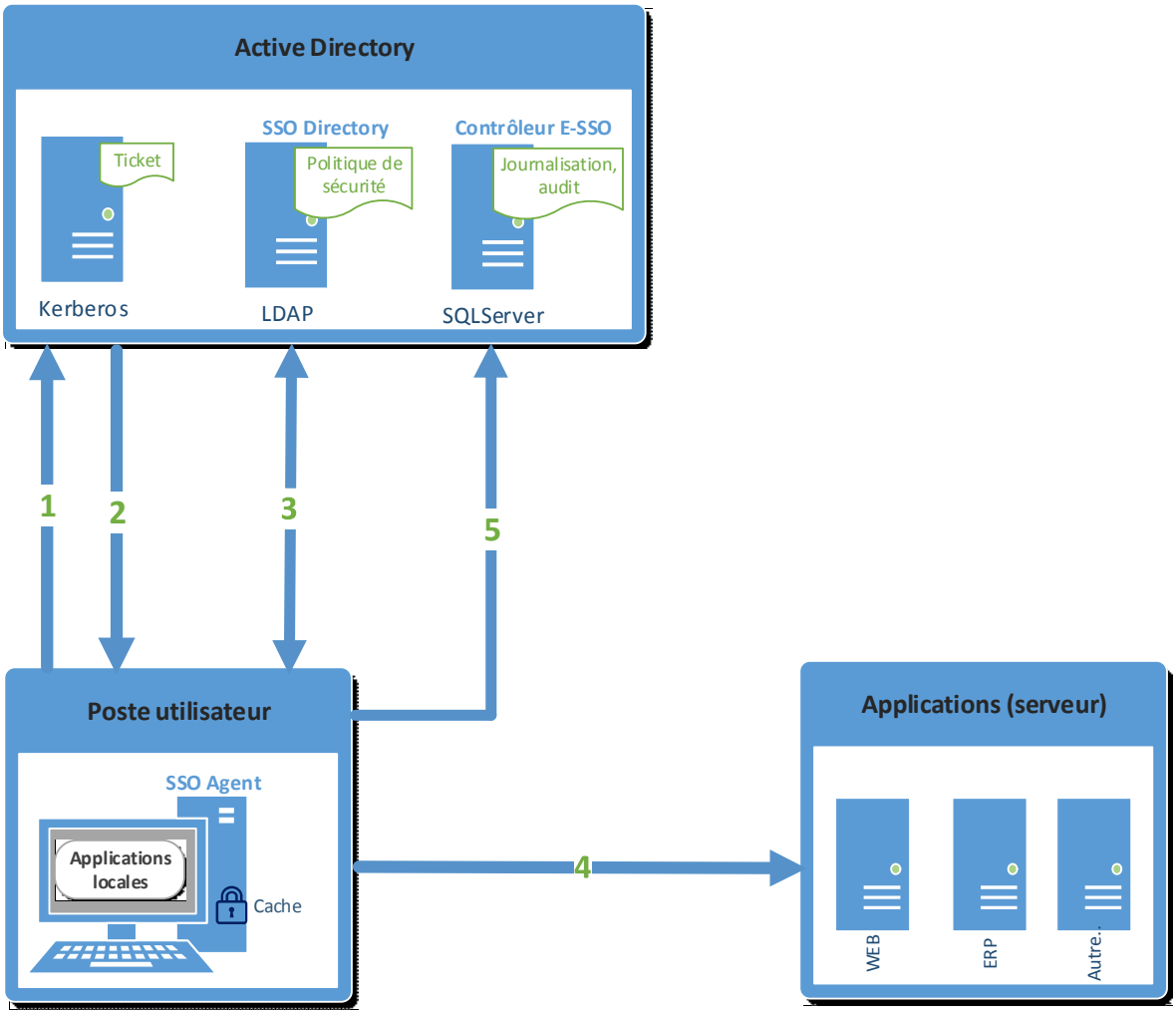

Figure 2 : fonctionnement du système «Enterprise SSO»

1. l'utilisateur SSO s'authentifie sur sa session Windows en envoyant une demande d'authentification au service KERBEROS de l'Active Directory ;

2. le service KERBEROS authentifie l'utilisateur en envoyant un ticket au « SSO agent » ;

3. « SSO agent » utilise l'identifiant et le mot de passe de la session Windows de l'utilisateur SSO pour récupérer auprès de l'annuaire LDAP les données applicatives :

les autorisations d'accès aux applications (politique de sécurité liée au compte de l'utilisateur SSO) et les identifiants/ mot de passe de connexion pour chaque application. Les données applicatives sont transmises dans un cache sur le poste utilisateur SSO. Ces données applicatives contenues dans le cache sont chiffrées (AES256);

4. l'utilisateur SSO lance une application. « SSO agent » :
   - détecte la fenêtre d'authentification de l'application ;
   - récupère l'identifiant / mot de passe de l'application stockés en local sur le poste utilisateur dans le cache ;
   - remplit automatiquement la fenêtre d'authentification et l'utilisateur SSO se retrouve connecter sur le serveur de l'application ;

5. toutes les authentifications de l'utilisateur SSO sur chaque application sont remontées du cache du poste utilisateur SSO vers le « Contrôleur E-SSO ».

2.3 Environnement d'utilisation

Le produit Enterprise SSO fonctionne sur les systèmes d'exploitation de type Windows et permet aux utilisateurs de se connecter à leurs applications.

Figure 3 : Exemples d'applications accessibles

2.4 Utilisateurs du produit

Utilisateur SSO : un utilisateur SSO est l'utilisateur souhaitant utiliser les applications à partir de son poste.

Administrateur SSO : un administrateur SSO définit et configure la politique de sécurité des utilisateurs SSO. Cette politique comporte tous les accès d'un utilisateur SSO à toutes ses applications. Il configure les délégations possibles pour chaque utilisateur SSO. Il visualise aussi les évènements d'audit.

Administrateur système : un administrateur système administre les postes de travail de chaque utilisateur. Il installe le logiciel Enterprise SSO sur les postes de travail des utilisateurs.

2.5 Hypothèses sur l'environnement

2.5.1 Hypothèses sur les utilisateurs du produit

H.Administrateur_SSO : les administrateurs SSO sont considérés compétents, formés et de confiance.

H.Administrateur_Système : les administrateurs Systèmes sont considérés compétents, formés et de confiance.

2.5.2 Hypothèses sur l'environnement technique

H.Active_Directory : le serveur AD est situé dans un local informatique dont l'accès est limité à des personnes de confiance.

H.Applications : les applications accessibles par l'utilisateur protègent les informations de connexions. C'est-à-dire que les applications ne permettent pas d'afficher les identifiants / mots de passe en clair à l'utilisateur.

H.OS : le système d'exploitation des postes utilisateurs est considéré comme proprement configuré, sécurisé et de confiance.

2.6 Périmètre de l'évaluation

L'évaluation porte sur les composants suivants :

- Le logiciel « SSO agent » installé sur les postes de travail des utilisateurs SSO ;
- Le logiciel « Contrôleur E-SSO» installé sur le serveur Active Directory.

3. Environnement technique de fonctionnement du produit

L'environnement technique pour le fonctionnement d'Enterprise SSO est le suivant :

- **postes de travail utilisateurs** : système d'exploitation Windows 7 (64 bits) PROFESSIONNELLE :
  - 2 postes de travail « Utilisateur SSO » pour le compte partagé ;
  - 1 poste de travail « Utilisateur SSO » pour le compte unique ;
  - 1 poste de travail « Utilisateur SSO » pour la délégation de compte ;

- **poste de travail administrateur** :
  - système d'exploitation Windows 7 (64 bits) PROFESSIONNELLE ;
  - navigateur : Internet Explorer 11

- **protocole d'authentification réseau** : Kerberos version 5.0 ;

- **active directory / base de données**: 1 serveur Windows Server 2008 R2 avec l'annuaire AD et la base de données SQL server 2008 Express ;

- **applications accessibles sur les postes utilisateurs** :
  - WebSite : support.evidian.com ;
  - Emulateur : Putty version 0.61 (ou supérieure) en utilisant le plugin MSTelnetW2KXP ;
  - Application locale : Filezilla version 3.9.0.6 (ou supérieure);

Les modes de configuration des comptes utilisateurs SSO et qui sont retenus pour cette évaluation sont les suivants :

- **« compte unique »** : un utilisateur SSO possède des applications. Cet utilisateur a donc un identifiant unique pour chacune de ses applications.

- **« compte partagé »** : une application est partagée pour plusieurs utilisateurs SSO. Ces utilisateurs partagent les mêmes identifiants pour ces applications.

- **« délégation de compte »** : un utilisateur SSO délègue à d'autres utilisateurs SSO l'accès à ses applications. Cette délégation n'est possible que si la politique définie par l'administrateur SSO l'autorise.

4.Biens sensibles devant être protégés

Enterprise SSO doit protéger les données suivantes :

4.1 Données applicatives

Les données applicatives sont :

- les identifiants de connexion aux applications : le mot de passe de l'utilisateur SSO qui permet de se connecter sur les applications.
- L'identifiant de connexion de la politique d'accès aux applications : l'administrateur SSO configure les accès autorisés des utilisateurs SSO pour chaque application du SI.

Ces données applicatives sont stockées dans le cache du poste de travail de chaque utilisateur SSO et sont échangées entre le poste local (SSO agent) et l'annuaire AD (SSO directory). Ces données sont chiffrées (AES256) dans le cache.

Ces données applicatives doivent être protégées en Disponibilité, Intégrité et Confidentialité.

4.2 Evènement d'audit

Les connexions aux applications sont journalisées.

Ces évènements sont stockés temporairement dans le cache du poste de travail de chaque utilisateur SSO et sont périodiquement remontés à l'annuaire AD (Contrôleur E-SSO). La remontées des évènements est chiffrée (AES256).

Ces évènements doivent être protégés en Intégrité.

5.Description des menaces

5.1 Agents menaçants

Les agents menaçants considérés pour l'évaluation sont:

- les personnes malveillantes ayant un accès physique au poste de travail lorsque l'utilisateur légitime n'est pas authentifié,
- un utilisateur SSO malveillant tentant d'accéder à des mots de passe d'applications et de politiques d'accès aux applications auxquels il n'aurait pas les droits,
- les personnes malveillantes ayant un accès logique au canal de communication entre le « SSO Agent » et le « SSO directory » et « SSO Agent » et le « Contrôleur E-SSO ».

5.2 Liste des menaces

Écoute du canal SSO agent – SSO directory : une personne malveillante écoute le canal de communication entre le « SSO Agent » et le « SSO directory » pour compromettre la confidentialité des données transmises.

Données impactées : Confidentialité des données applicatives.

Écoute du canal SSO agent – Contrôleur E-SSO : une personne malveillante écoute le canal de communication entre le « SSO Agent » et le « Contrôleur E-SSO » pour compromettre la confidentialité des données transmises.

Données impactées : Confidentialité des évènements d'audit.

Altération des données transmises sur le canal SSO agent – SSO directory : une personne malveillante intercepte et modifie les données applicatives.

Données impactées : Intégrité des données applicatives.

Altération des données transmises sur le canal SSO agent – Contrôleur E-SSO : une personne malveillante intercepte et modifie les évènements d'audit.

Données impactées : Intégrité des évènements d'audit.

Usurpation d'identité utilisateur SSO : un utilisateur SSO tente d'usurper l'identité d'un utilisateur SSO légitime pour accéder à ses applications.

Données impactées : Intégrité et confidentialité des données applicatives accessibles avec le compte usurpé.

Usurpation d'identité administrateur SSO : Une personne malveillante tente d'usurper l'identité d'un administrateur SSO . Cette usurpation permettrait d'accéder à la politique d'accès aux applications.

Données impactées : Intégrité et confidentialité des données applicatives accessibles avec le compte usurpé.

6.Spécification des fonctions dédiées à la sécurité

6.1 Liste des fonctions de sécurité

Le périmètre d'évaluation couvre les fonctions de sécurité suivantes :

Authentification des utilisateurs SSO : les utilisateurs SSO sont authentifiés par « SSO agent » avec un identifiant / mot de passe avant de pouvoir accéder à leurs applications.

Authentification des administrateurs SSO : les administrateurs SSO sont authentifiés par « SSO agent » avec un identifiant / mot de passe.

Contrôle des accès aux applications : la politique de sécurité stockée en local sur le poste de l'utilisateur définit les accès possibles et les délégations possibles pour chaque utilisateur SSO.

Protection des données applicatives : les données applicatives sont stockées en local dans un cache sur chaque poste utilisateurs SSO. Ces données sont transmises du « SSO directory » vers « SSO Agent » en étant chiffrées (AES256).

Protection des évènements d'audit : les données (évènements d'audit) sont stockées temporairement dans un cache du poste utilisateur SSO ; les données sont chiffrées (RSADSI RC4) lors de leur transit vers du « SSO Agent » vers le « Contrôleur E-SSO ».

6.2 Argumentaire des fonctions de sécurité

Menaces	**Fonctions de sécurité permettant de contrer les menaces**
Écoute du canal SSO agent – SSO directory	Protection des données applicatives
Écoute du canal SSO agent – Contrôleur E-SSO	Protection des évènements d'audit

Altération des données transmises sur le canal SSO agent – SSO directory	Protection des données applicatives
Altération des données transmises sur le canal SSO agent – Contrôleur E-SSO	Protection des évènements d'audit
Usurpation d'identité utilisateur SSO	Authentification des utilisateurs SSO Contrôle des accès aux applications
Usurpation d'identité administrateur SSO	Authentification des administrateurs SSO

6.3 Spécification des mécanismes cryptographiques

Le document traitant des spécifications des mécanismes cryptographiques porte la référence suivante : 39 F2 03LZ 00.

Fin du Document