Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2018/01

Evidian Enterprise SSO
Version 8.06PL5 b5386.30

Paris, le 16 février 2018

Le directeur général de l'agence nationale
de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

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 cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2018/01**
Nom du produit **Evidian Enterprise SSO**
Référence/version du produit **Référence Evidian Enterprise SSO, Version 8.06PL5 b5386.30**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Evidian** **Rue Jean Jaurès, BP68,** **78340 Les Clayes sous Bois, France**
Développeur **Evidian** **Rue Jean Jaurès, BP68,** **78340 Les Clayes sous Bois, France**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B,** **78180 Montigny le Bretonneux, France**
Fonctions de sécurité évaluées **Authentification des utilisateurs SSO** **Authentification des administrateurs SSO** **Contrôle des accès aux applications** **Protection des données applicatives** **Protection des évènements d'audit**
Fonction(s) de sécurité non évaluées **N/A**
Restriction(s) d'usage **Oui (cf. §3.2)**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Evidian Enterprise SSO, version 8.06PL5 b5386.30 » développé par *EVIDIAN*.

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

La principale fonction du produit est d'éviter aux utilisateurs la ressaisie d'un nom d'utilisateur et d'un mot de passe pour chaque application utilisée. Il permet également à un utilisateur de déléguer l'accès à une application à un autre utilisateur, sans avoir à divulguer son mot de passe.

La figure ci-dessous explicite l'architecture du produit. Le produit met en œuvre deux composants logiciels « SSO Agent » et « Contrôleur E-SSO ». Le produit utilise l'annuaire d'entreprise préexistant afin de stocker ses données (« SSO Directory »).

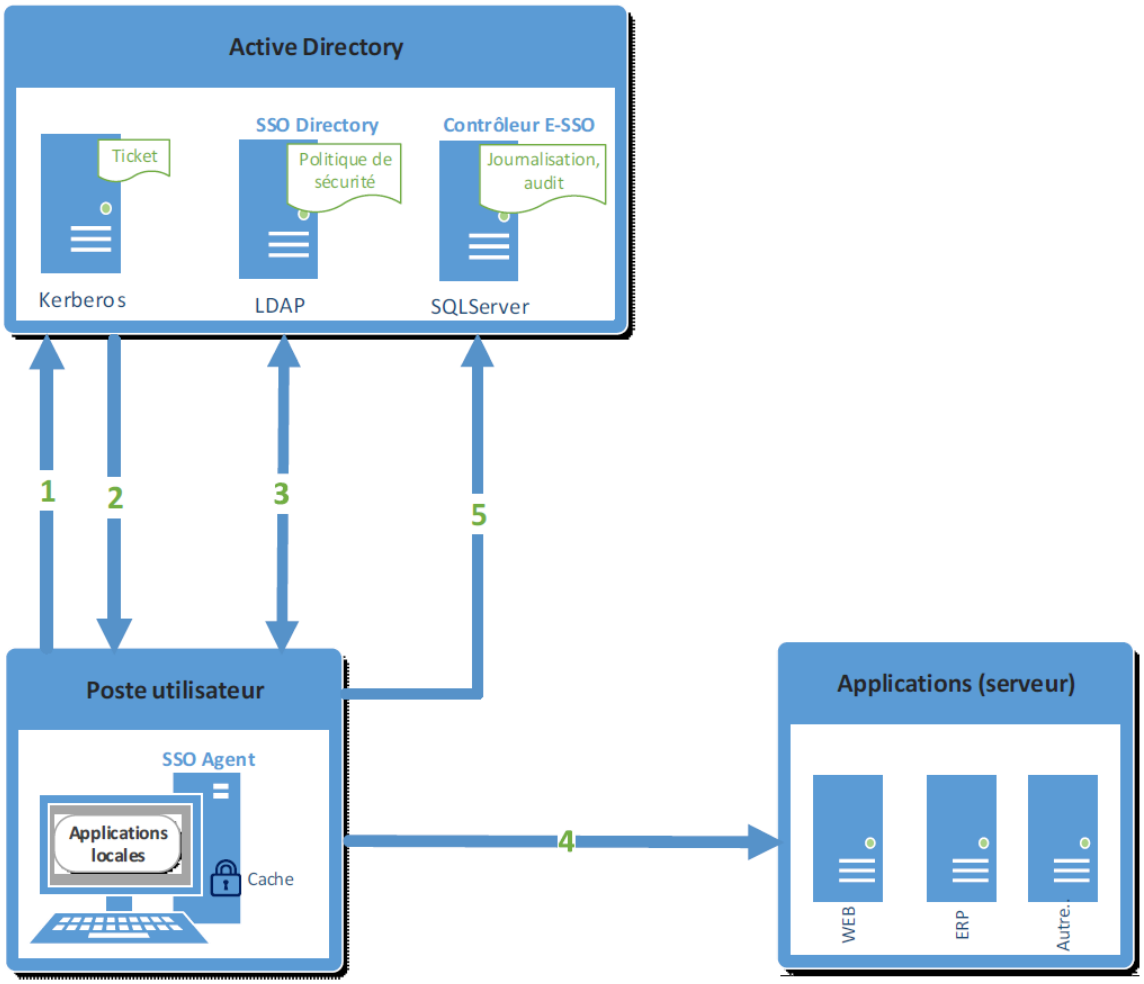

Figure 1 - Architecture Produit.

La cinématique d'utilisation du produit est la suivante :

1) l'utilisateur SSO s'authentifie sur sa session Windows en envoyant une demande d'authentification au service KERBEROS 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 :
   a) les autorisations d'accès aux applications (politique de sécurité liée au compte de l'utilisateur),
   b) les identifiants/ mot de passe de connexion pour chaque application.

   Ces données sont transmises dans un cache chiffré (AES256) sur le poste utilisateur SSO ;
4) l'utilisateur SSO lance une application « SSO agent » qui :
   a) détecte la fenêtre d'authentification de l'application,
   b) récupère l'identifiant / mot de passe de l'application stockés en cache sur le poste utilisateur,
   c) remplit automatiquement la fenêtre d'authentification ;
5) l'utilisateur SSO est alors connecté sur le serveur de l'application ;
6) toutes les authentifications de l'utilisateur SSO sur chaque application sont journalisées du cache du poste utilisateur SSO vers le « Contrôleur E-SSO ».

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 – détection d'intrusions
☐ 2 – anti-virus, protection contre les codes malicieux
☐ 3 – pare-feu
☐ 4 – effacement de données
☐ 5 – administration et supervision de la sécurité
☒ **6 – identification, authentification et contrôle d'accès**
☐ 7 – communication sécurisée
☐ 8 – messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 – environnement d'exécution sécurisé
☐ 11 – terminal de réception numérique (*Set top box*, STB)
☐ 12 – matériel et logiciel embarqué
☐ 13 – automate programmable industriel
☐ 99 – autre

1.2.2. Identification du produit

Nom du produit	Evidian Enterprise SSO
Numéro de la version évaluée	8.06PL5 b5386.30

Le produit inclut plusieurs exécutables :

- *client Entreprise SSO* ;
- *authentication Manager* ;
- *user Access Console* ;
- *user Access.*

Les versions de tous les exécutables sont les mêmes : 8.06PL5 b5386.30. Elles peuvent être consultées en suivant les procédures décrites ci-après.

1.2.2.1. Versions de *Client Entreprise SSO* et *Authentication Manager*

Sur le poste Windows client, deux icones sont présentes dans la zone de notification :

Un clic droit sur ces icones permet d'obtenir les versions de *Client Entreprise SSO* et *Authentication Manager* :

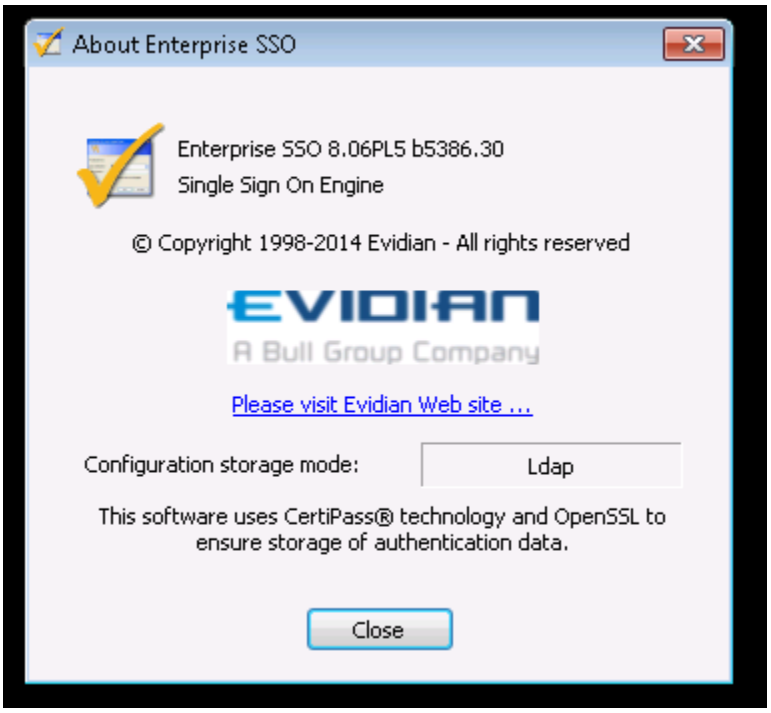

Figure 2 : Version constatée sur l'exécutable « client Entreprise SSO »

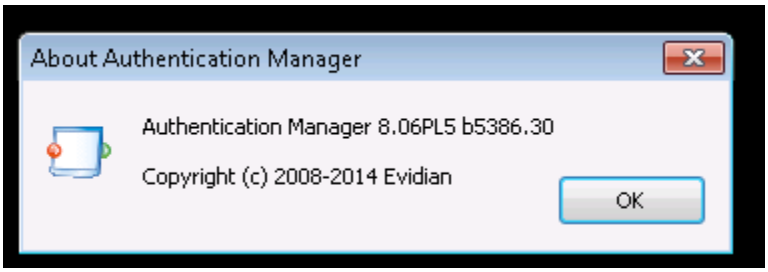

Figure 3 : Version constatée sur l'exécutable « Authentication Manager »

1.2.2.2. Version de *User Access Console*

Dans le menu Démarrer, sélectionner *User Access Console* puis aller dans *help/about*.

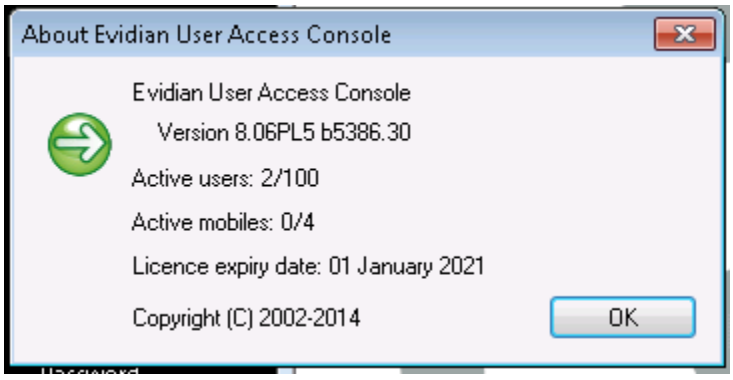

Figure 4 : Version constatée sur l'exécutable « User Access Console »

1.2.2.3. Versions de *User Access*

Dans le menu Démarrer, sélectionner *Errors and Events*.

Figure 5 : Version de l'exécutable « User Access »

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :
- l'authentification des utilisateurs SSO ;
- l'authentification des administrateurs SSO ;
- le contrôle des accès aux applications ;
- la protection des données applicatives ;
- la protection des évènements d'audit.

1.2.4. Configuration évaluée

L'environnement technique pour l'évaluation est le suivant :
- postes de travail utilisateurs SSO. Système d'exploitation Windows 7 (64 bits) PROFESSIONNEL :
  - 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 SSO :
  - système d'exploitation Windows 7 (64 bits) PROFESSIONNEL ;
  - 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 SSO :
  - webSite : support.Evidian.com ;
  - émulateur : 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.

La plateforme de test est décrite dans la figure ci-dessous :

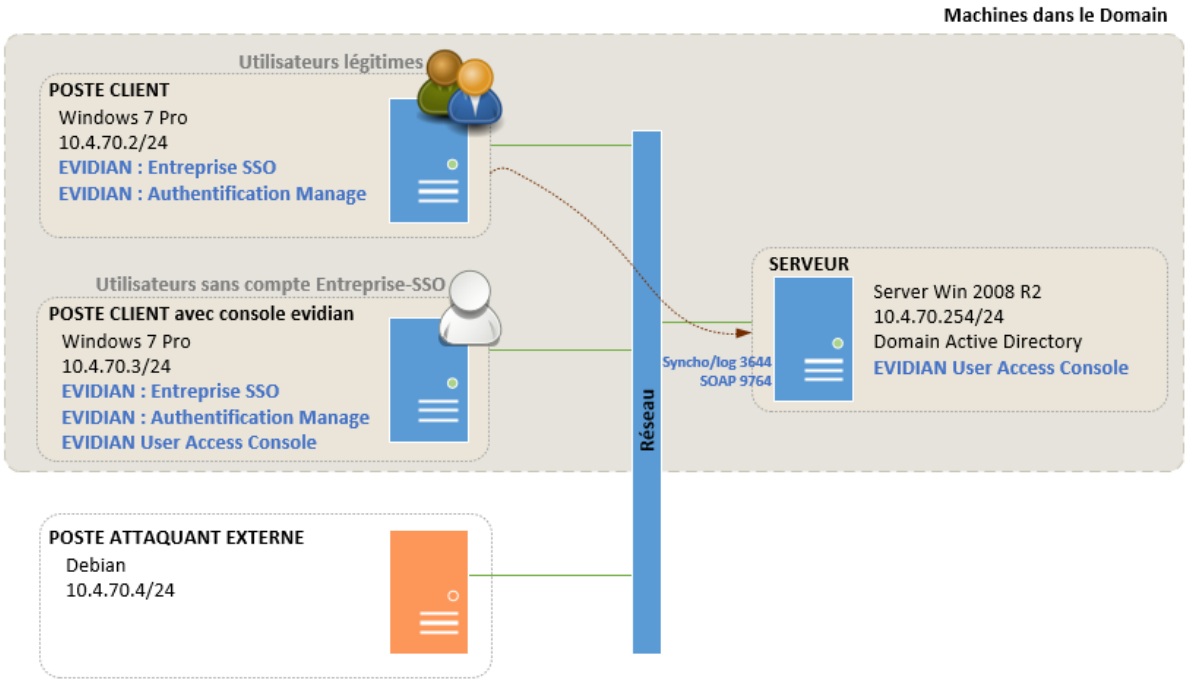

Figure 6: plate-forme de test

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.3.1.2. Description de l'installation et des non-conformités éventuelles

Aucune non-conformité n'a été relevée.

2.3.1.3. Durée de l'installation

Il faut une demi-journée pour installer le serveur, un client et configurer des applications.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

La documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit. Elle s'adresse à des administrateurs ayant des compétences *Active Directory*.
L'évaluateur a relevé deux incohérences dans la cible de sécurité :

- la cible considère comme une menace « les personnes malveillantes ayant un accès physique au poste de travail lorsque l'utilisateur légitime n'est pas authentifié ». Or cette menace est toujours réalisable si le disque dur du poste client n'est pas chiffré ;
- la cible pose comme hypothèse que « 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 ». Or cette hypothèse n'est pas triviale à mettre en œuvre par l'utilisateur, et nécessite une analyse spécifique de la part de l'administrateur des postes utilisateurs.

Ces points donnent lieu à des restrictions d'usage au chapitre 3.2.

2.3.3. Revue du code source (facultative)

L'évaluation n'a pas fait l'objet d'une revue de code source.

2.3.4. Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

2.3.6.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

2.3.7. Accès aux développeurs

Le centre d'évaluation a eu accès aux développeurs pour répondre à des questions sur le produit.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

Deux cas d'usage entraînant un risque ont été relevés par l'évaluateur :

- la sécurité du produit serait remise en cause si un utilisateur côté client était en mesure d'exécuter un outil pouvant accéder à des informations de bas niveau (par exemple un débogueur ou *Autoit*).
- la confidentialité des données d'authentification serait compromise dans un cas de délégation pour les applicatifs permettant de journaliser en clair ces authentifiants. C'est notamment le cas pour l'application *Putty*.

Ces points donnent lieu à des restrictions d'usage au chapitre 3.2.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Il est conseillé de déployer la TOE dans un environnement possédant des contres mesures contre les attaques par déni de service sur le réseau, afin d'empêcher un attaquant de forcer la TOE à rester en mode déconnecté par un déni de service sur l'annuaire LDAP.

Enfin, les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [INSTALL] fournis.

2.3.8.3. Avis d'expert sur la facilité d'emploi

Le produit est simple d'utilisation. Une bonne connaissance en *Active Directory* est cependant nécessaire pour la mise en place de l'outil côté serveur.

2.3.8.4. Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN.
Celle-ci a relevé des non-conformités mineures au RGS :

- la TOE utilise le schéma PKCS# RSA v1.5 pour le chiffrement et le déchiffrement des données SSO ;
- la TOE utilise la fonction de hachage SHA1 dans l'algorithme AES256-CTS-HMAC-SHA1-96 ;
- la TOE utilise une empreinte de taille trop faible (96 bits) en sortie de l'algorithme AES256-CTS-HMAC-SHA1-96.

Cependant, ces points ne remettent pas en cause la sécurité globale du produit.

2.5. Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé. L'évaluateur n'a pas relevé de vulnérabilité exploitable lors de l'analyse.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Evidian Enterprise SSO, version 8.06PL5 b5386.30 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.
L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations énoncées dans le présent rapport (voir 2.3.8.2).

L'évaluation a également mis en avant des restrictions d'usage à respecter pour une utilisation sécurisée du produit décrites ci-après. L'utilisateur devra ainsi :

- suivre les recommandations du document [INSTALL], en particulier :
  - chiffrer le disque du poste utilisateur,
  - ne pas permettre aux utilisateurs d'être administrateur des postes clients ;
- mettre en œuvre une politique de restrictions logicielles sur les postes clients pour restreindre l'utilisation d'outils pouvant accéder à des informations de bas niveau (il est conseillé de suivre les recommandations du document [DAT-NT-13]) ;
- ne pas permettre la délégation pour des applications journalisant en clair les identifiants.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité Enterprise SSO v8.06* Référence : 39 F2 46LZ 01 ; Version : *1.2* ; Date : *24 janvier 2017*
[RTE]	*Rapport Technique d'Évaluation CSPN ENTERPRISE-SSO2 – Evidian Enterprise SSO* Référence : OPPIDA/CESTI/ENTERPRISE-SSO2/RTE ; Version : 1.3 ; Date : 16 janvier 2018
[INSTALL]	*Manuel d'installation du produit.* Référence : *39 A2 24LY 09* ; Date : *janvier 2018*
[DAT-NT-13]	Note technique – Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows, référence DAT-NT-13/ANSSI/SDE/NP

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.