Cible de sécurité CSPN

Bibliothèque "Digital DNA CoreLib" version 3.2.0

Référence : CSPN-ST-LOE002-1.03

Date : le 05/02/2014

Siège : 4 bis allée du Bâtiment ● 35000 Rennes ● France ● www.amossys.fr

SIRET : 493 348 890 00036 ● **NAF** : 6202 A ● RCS Rennes B 493 348 890 ● SAS au capital de 38.000 Euros

MAÎTRISE DU DOCUMENT

	NOM	FONCTION	DATE	SIGNATURE
Contrôle technique	APE	RTCs	05/02/2014	[ORIGINAL SIGNE]
Contrôle qualité	APE	RTCs	05/02/2014	[ORIGINAL SIGNE]
Approbation	ACT	RTC	05/02/2014	[ORIGINAL SIGNE]

Ce document a été validé par LoginPeople.

FICHE D'ÉVOLUTIONS

Révision	Date	Description	Rédacteur
1.00	31/05/2013	Création du document	ALR
1.01	24/06/2013	Prise en compte des remarques de l'ANSSI	APE
1.02	21/11/2013	Modifications de la cible de sécurité avec changement de la version de la TOE	ACT, APE
1.03	05/02/2014	Mise à jour des hypothèses	APE

SOMMAIRE

1. INTRODUCTION 5
1.1. Objet du document 5
1.2. Documents applicables 5
1.1. Glossaire 5
2. IDENTIFICATION DU PRODUIT 6
3. DESCRIPTION DU PRODUIT 7
3.1. Description générale 7
3.2. Fonctionnement 8
3.3. Description de la manière d'utiliser le produit 8
3.3.1. L'enrôlement 9
3.3.2. L'authentification 9
3.4. Description de l'environnement prévu pour son utilisation 11
3.5. Description des hypothèses sur l'environnement 12
3.6. Description des dépendances 12
3.7. Description des utilisateurs typiques concernés 12
3.8. Définition du périmètre de l'évaluation 12
4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT ... 13
4.1. Matériel compatible ou dédié 13
4.2. Système d'exploitation retenu 13
5. DESCRIPTION DES BIENS SENSIBLES 14
6. DESCRIPTION DES MENACES 15
7. DESCRIPTION DES FONCTIONS DE SÉCURITÉ DU PRODUIT 16

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma CSPN, de la bibliothèque « Digital DNA CoreLib » développée par la société **LoginPeople**.

Ce document est soumis au contrôle technique et qualité d'**AMOSSYS** ainsi qu'à la validation de **LoginPeople**. Les mises à jour de ce document sont effectuées par l'équipe projet d'**AMOSSYS**.

1.2. DOCUMENTS APPLICABLES

Ref.	Descriptions
[CER-I-01.1]	*Méthodologie pour l'évaluation en vue d'une Certification de Sécurité de Premier Niveau.* N°1416/ANSSI/SR du 30 mai 2011.
[CER-I-02.1]	*Critères pour l'évaluation en vue d'une Certification de Sécurité de Premier Niveau.* N°1417/ANSSI/SR du 30 mai 2011.

1.1. GLOSSAIRE

Acronymes	Définitions
Plugin	*Module d'extension*
SDK	*Software Development Kit*
ST	*Security Target (Cible de sécurité)*
TOE	*Target Of Evaluation (Cible d'évaluation)*

2.IDENTIFICATION DU PRODUIT

Editeur	**LoginPeople** Buropolis 2 – 1240 route des Dolines Sophia Antipolis 06560 VALBONNE
Lien vers l'organisation	www.loginpeople.com
Nom commercial du produit	Digital DNA Corelib
Numéro de la version évaluée	3.2.0
Catégorie du produit	identification, authentification, contrôle d'accès

3.DESCRIPTION DU PRODUIT

3.1. DESCRIPTION GÉNÉRALE

La société **LoginPeople** développe des solutions de sécurité pour les accès aux réseaux publics et privés.

Le produit phare de la marque est le serveur d'authentification multi-facteur appelé « Digital DNA Server ». Il fournit les fonctionnalités permettant aux utilisateurs de s'authentifier avec « *ce qu'ils savent* » (un identifiant, un mot de passe), mais également avec « *ce qu'ils possèdent* » (leur ordinateur, *smartphone*, tablette, clé USB, disque dur… tout périphérique à stockage de masse). **LoginPeople** a donc développé divers moyens (composants client) pour utiliser la solution.

Le produit « `Digital DNA CoreLib` » (la TOE) est la bibliothèque qui représente le noyau de la technologie développée par la société **LoginPeople**. Cette bibliothèque est présente dans tous les clients identifiés :

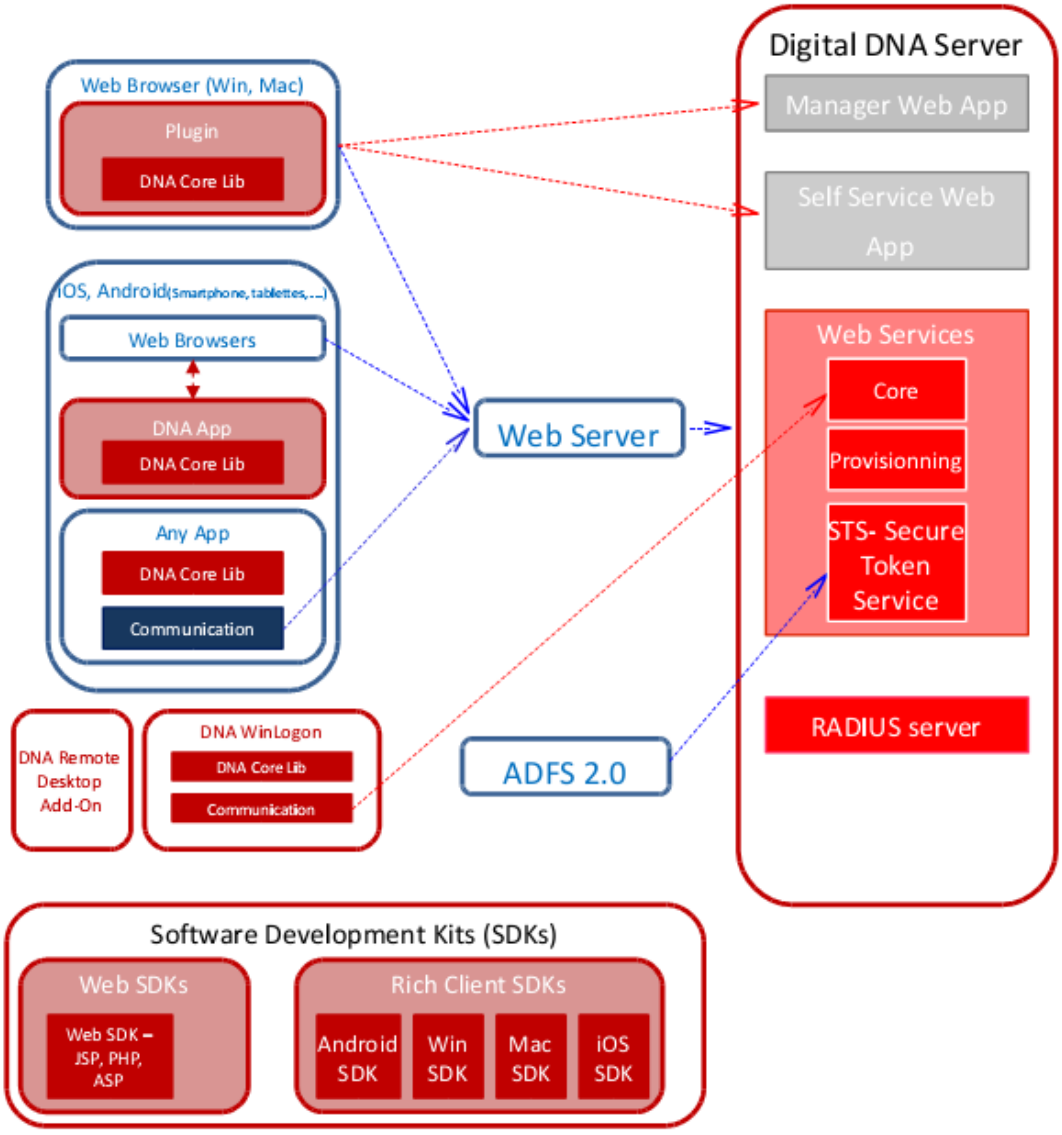

Figure 1 – Composants embarquant CoreLib

Détails concernant les composants clients embarquant la TOE :

- le ***Plug In*** permet la lecture, l'enrôlement de tous les équipements ainsi que l'authentification. Il ne fait qu'interagir entre la **CoreLib** et le serveur DDNA (communications provenant/vers le serveur DDNA). Il est présent et installable sous deux formes :
  - via un navigateur, en accédant aux applications web : *Digital DNA Self-Service* ou *Digital DNA Manager* ;
  - via les kits de développements *Web* ou *Rich client* : ces kits sont fournis à des clients désireux de réaliser leur propres applications ;
- le ***Winlogon*** est basé sur le *Credential Provider* de Windows et renforce la sécurité d'une session Windows en utilisant la Technologie *Digital DNA* de la bibliothèque ***CoreLib***. Il est installable sous forme d'un package MSI ;
- le ***Remote Desktop Add-On*** permet l'utilisation des équipements locaux sur une application *Digital DNA* (*WinLogon*, *Digital DNA Manager*, …) installée sur une machine distante via RDP. Il est installable sous forme d'un package MSI ;
- l'application ***DDNA Tech*** remplace le ***Plug In*** sous *Android* et *iOS*. Elle utilise la bibliothèque ***CoreLib*** pour réaliser les mêmes fonctions : la lecture, l'enrôlement de tous les équipements ainsi que l'authentification. Elle est disponible sous l'Apple Store et Google Play Store.

3.2. FONCTIONNEMENT

La ***CoreLib*** se base sur quatre autres bibliothèques pour fonctionner :

- ***Utils*** : fournit des fonctions usuelles pour toutes les autres bibliothèques comme la manipulation de chaînes de caractères, de hash, etc.) ;
- ***Reader*** : récupère les données matérielles ;
- ***QKI*** : définit les objets représentant les équipements et leur ADN[1] ;
- ***SAWS-Native*** : présente une interface haut-niveau par rapport au système de gestion des équipements et permet de récupérer facilement des QKI en demandant un type d'équipement.

Le package entier (la CoreLib et les quatre autres bibliothèques) va ainsi permettre d'implémenter les fonctions d'**enrôlement** et d'**authentification** présentées dans la cible de sécurité.

La TOE correspond à l'ensemble de ces cinq bibliothèques.

3.3. DESCRIPTION DE LA MANIÈRE D'UTILISER LE PRODUIT

La bibliothèque ***CoreLib*** implémente les processus d'enrôlement et d'authentification en se basant sur l'analyse des équipements par les bibliothèques précédemment décrites.

L'utilisation du produit se déroule en deux étapes distinctes :

1. processus d'enrôlement où l'empreinte du matériel est calculée;
2. processus d'authentification avec la combinaison des éléments login, mot de passe et empreinte.

Chacune de ces étapes est décrite en détail ci-après.

[1] *Acide DésoxyriboNucléique* (dans le cadre de cette cible de sécurité, le terme ADN est à comprendre comme « empreinte numérique »)

3.3.1. L'enrôlement

La phase d'enrôlement est le seul moment où l'ADN d'un équipement (matériel) à enrôler transite sur le réseau (l'ADN numérique est l'empreinte du matériel enrôlé). Pour éviter l'interception des informations, une communication sécurisée (via HTTPS) est établie et l'ADN est chiffré en utilisant un algorithme de chiffrement à clé publique, dont la clé (« clé d'enrôlement ») est fournie par le serveur DDNA.

Le diagramme ci-dessous décrit la phase d'enrôlement via un site web, assimilé à une intégration en mode client léger :

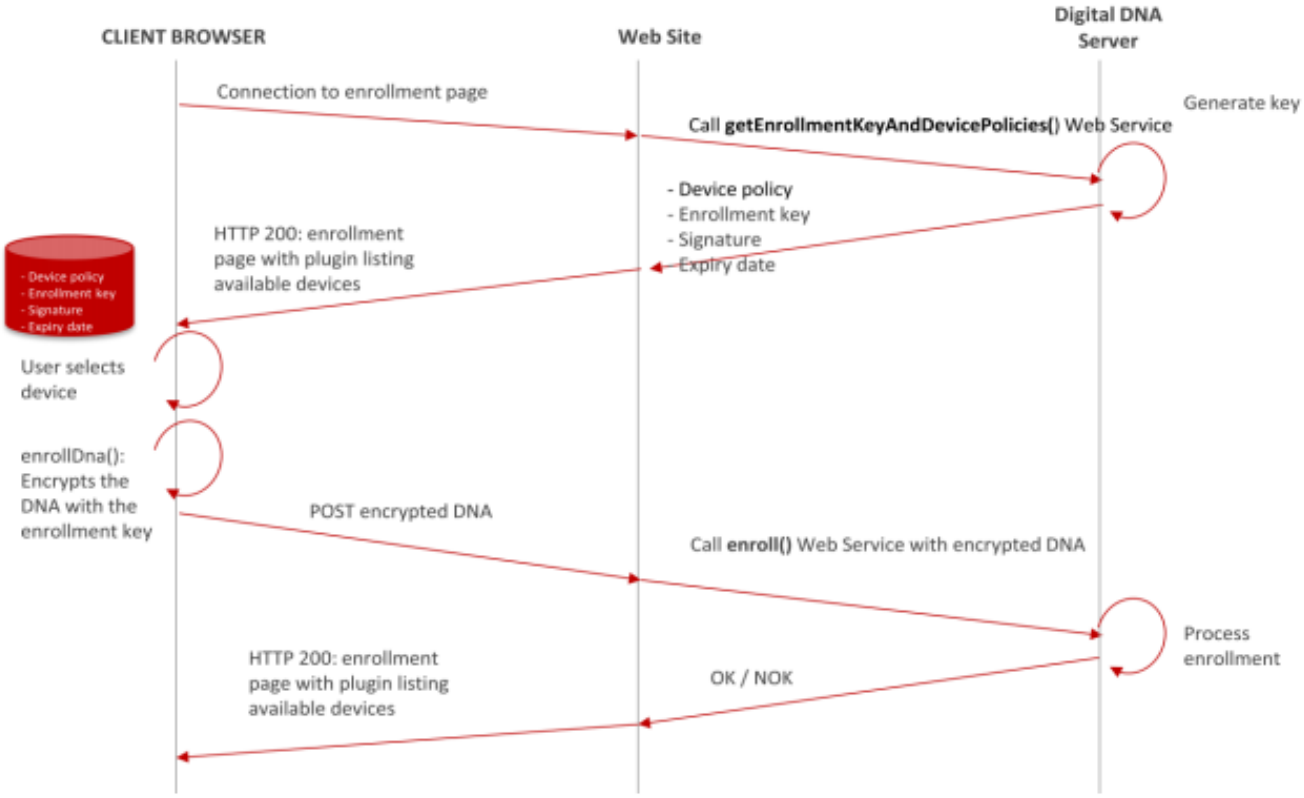

Figure 2 - Phase d'enrôlement

3.3.2. L'authentification

Durant la phase d'authentification, l'empreinte des équipements disponibles n'est jamais communiquée sur le réseau. De plus, comme lors de l'enrôlement, toute communication vers le serveur se fait au travers des *Web services* en HTTPS. Le processus d'authentification est basé sur le protocole de défi/réponse, pour lequel seule la réponse, construite par la bibliothèque ***CoreLib*** utilisant le défi et les informations sur l'ADN numérique, est soumise.

Le schéma suivant décrit la phase d'authentification :

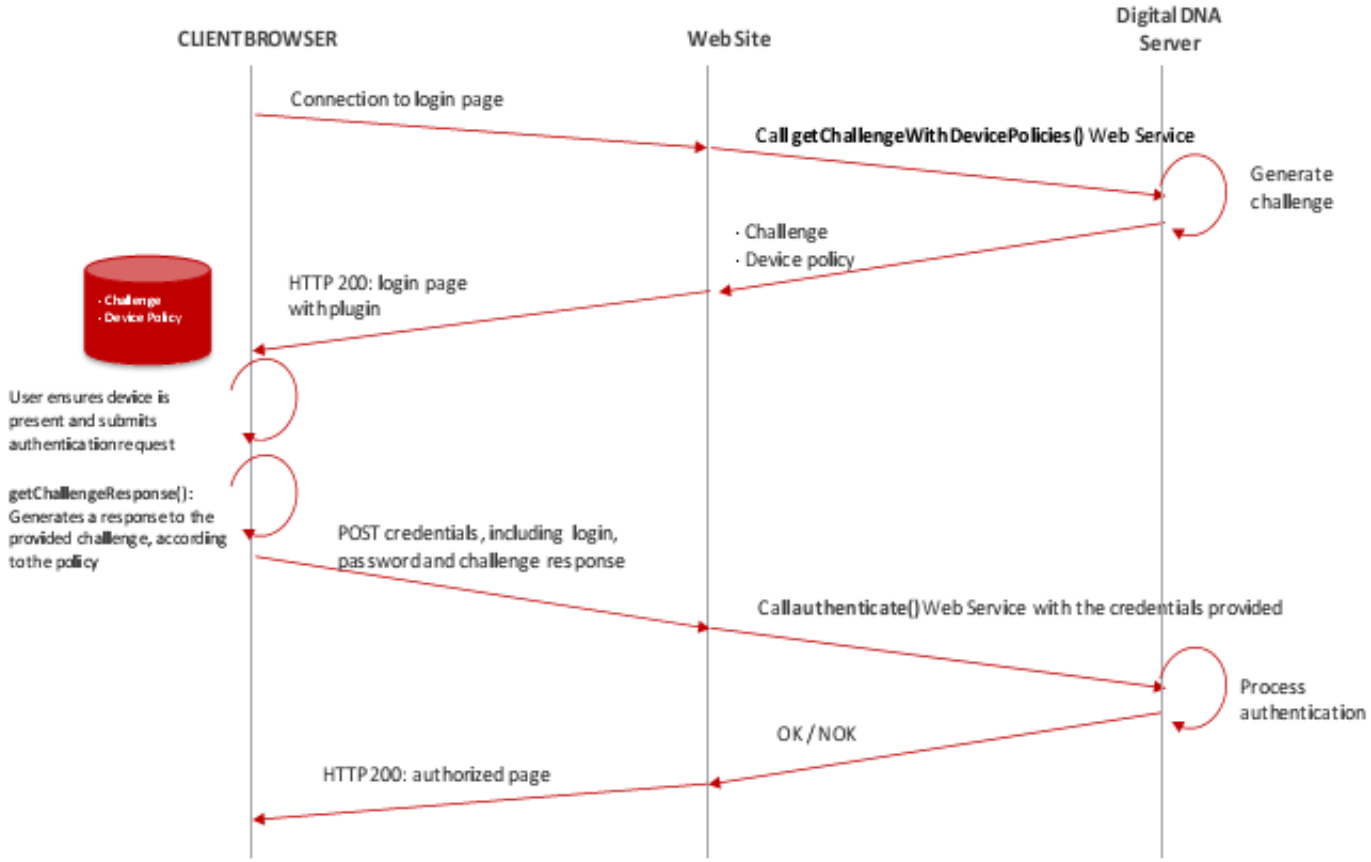

Figure 3 - Phases d'authentification

1- l'utilisateur accède à un site web sécurisé par l'ADN numérique de l'équipement enrôlé précédemment ;

2- avant de générer la page d'authentification, le site web demande un défi au Serveur de l'ADN avec le web service correspondant (`getChallengeWithDevicePolicies`) et construit ensuite une page de login contenant un défi et les politiques des équipements autorisés via le Plug In ;

3- la page d'authentification est chargée dans le navigateur. La bibliothèque ***CoreLib*** (Plug In) intègre le défi récupéré ;

4- l'utilisateur soumet son nom d'utilisateur, son mot de passe et s'assure que son équipement permettant de calculer son ADN numérique est bien présent ;

5- après avoir soumis sa requête d'authentification, la bibliothèque ***CoreLib*** détecte si un équipement est connecté (en fonction des politiques des équipements), lit leurs ADN et retourne une réponse créée en fonction du défi et l'ADN de chaque équipement (au travers de la méthode `getChallengeResponse` du Plug In) ;

6- le défi et sa réponse correspondante sont soumis au serveur web en même temps que le nom d'utilisateur et le mot de passe ;

7- le serveur web fait appel au Web Service d'authentification (méthode *authenticate*) du serveur avec les précédentes informations : nom d'utilisateur, mot de passe et défi - réponse) ;

8- le serveur répond « OK/NOK » et le serveur web agit en fonction de cette réponse.

3.4. DESCRIPTION DE L'ENVIRONNEMENT PRÉVU POUR SON UTILISATION

Comme présenté précédemment, la solution se compose :

- d'un serveur (*Digital DNA Server*) en version 5.6.2 permettant de gérer les utilisateurs et l'authentification multi-facteur incluant un serveur Radius pour simplifier l'intégration avec les autres systèmes. Le serveur est disponible sous forme d'un fichier ISO permettant l'installation directe sur un équipement hardware ou une solution virtuelle telle que `VMWare`, `Hyper-V`, `KVM` ou `XEN`. Celui-ci est isolé dans une DMZ des autres composants de la plateforme ;

  La plate-forme retenue, pour le serveur et dans le cadre des travaux d'évaluation CSPN, est `VMWARE ESXi` en version 5.0u1.

- d'une application cliente (liste des clients fournie au paragraphe 3.1), qui collecte l'information matérielle du client. Il intègre le *plugin* « `Digital DNA CoreLib` » en version 3.2.0.

Le serveur d'authentification et l'application cliente utilisent un format de message propriétaire (dont le contenu est chiffré avec l'algorithme AES 256 bits) pour échanger leurs données.

La TOE est le package « ***CoreLib*** » implémenté dans un plugin pour navigateur web.

3.5. DESCRIPTION DES HYPOTHÈSES SUR L'ENVIRONNEMENT

Les hypothèses sur l'environnement de la TOE sont les suivantes :

- **H1.Serveur_Administrateur**

  L'administrateur du serveur est considéré comme non hostile et est formé pour exécuter les opérations dont il a la responsabilité (définition des politiques de sécurité notamment) en suivant les recommandations du guide d'administration.

- **H2.Serveur_sécurité**

  Il appartient au prestataire de service de s'assurer de la mise en place et du respect de procédures de sécurité sur les serveurs et de la protection des serveurs face au réseau.

- **H3.Client_Utilisateurs**

  Les utilisateurs du produit doivent assurer la confidentialité de leurs données d'authentification personnelles et veiller à protéger leur équipement enregistré. En cas de perte ou de vol de ce matériel, l'utilisateur doit contacter le prestataire pour désactiver l'authentification à partir de celui-ci.

- **H4.Client_Poste_sécurisé**

  Le poste client est à jour des configurations et correctifs de sécurité (pare-feu correctement configuré, antivirus avec base virale et applicative à jour, anti-*spyware*, anti-*rootkit*, etc.).

  Ce poste client doit être utilisé comme composant matériel en tant que donnée d'entrée des processus d'enrôlement et d'authentification. Il est également laissé la possibilité à un utilisateur final de rajouter un composant de type clé USB comme composant matériel supplémentaire pour l'identification. Dans ce cas, l'utilisateur doit s'assurer que ce composant est maitrisé et sain.

3.6. DESCRIPTION DES DÉPENDANCES

La procédure d'identification des utilisateurs fait appel à des matériels spécifiques (tout équipement à stockage de masse) choisis par l'utilisateur mais cette cible de sécurité ne pose aucune exigence particulière concernant ce type de matériel qui n'est pas considéré dans l'évaluation.

3.7. DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNÉS

Les rôles suivants seront pris en considération dans le cadre de l'analyse :

- ***Utilisateur :*** il cherche à s'authentifier auprès du service concerné ;
- ***Administrateur (hors périmètre) :*** il est chargé de définir la politique de sécurité et de surveiller les alertes de sécurité.

3.8. DÉFINITION DU PÉRIMÈTRE DE L'ÉVALUATION

L'évaluation porte sur la bibliothèque « CoreLib » implémentée dans le plugin pour navigateur web.

4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

4.1. MATÉRIEL COMPATIBLE OU DÉDIÉ

Le plugin comportant la TOE s'installe sur un navigateur Web. La compatibilité est donc inhérente au navigateur.

Aucun matériel dédié n'est nécessaire. Dans le cadre de la certification, l'évaluateur choisira le matériel qu'il souhaite en tant que composant source du fournisseur d'ADN.

4.2. SYSTÈME D'EXPLOITATION RETENU

La machine cliente est de type PC muni d'un système d'exploitation Microsoft Windows 7 SP1 64 bits.

Le plugin contenant la TOE (bibliothèque CoreLib v3.2.0) est installé sur les navigateurs web suivants (compatibles TLS1.1) :

- Mozilla Firefox v.25.0.1 ;
- Google Chrome v.27 ;
- Microsoft Internet Explorer v.9.

5.DESCRIPTION DES BIENS SENSIBLES

Les biens à protéger côté application cliente sont les suivants :

- **Données utilisateurs** : les biens sensibles à protéger sont les données d'authentification collectées et transmises au serveur (données matérielles du/des composants à protéger en confidentialité) ;
- **Données de sécurisation** : il s'agit des données sensibles utilisées par le produit pour sécuriser les échanges avec le serveur (confidentialité) ;
- **Données de gestion** : le client est amené à manipuler des éléments de sa propre politique de sécurité transmise par le serveur (type de matériel à interroger).

6.DESCRIPTION DES MENACES

Les différents agents menaçants sont :

- attaquants internes : entités appartenant au réseau de confiance telles qu'un **utilisateur** ayant obtenu un accès illégitime à la TOE ;
- attaquants externes : entités n'appartenant pas au réseau de confiance telles que :
  - une **entité non autorisée** qui ne dispose pas d'accès légitime à la TOE ;
  - un **logiciel tiers** ne faisant pas partie de la TOE et qui cherche à introduire des attaques (virus ou dénis de service par exemple).

Les administrateurs ne sont pas considérés comme des attaquants.

Les menaces qui portent sur les biens sensibles de la TOE sont les suivantes :

- **M1.Falsification_composant_matériel**

  Un attaquant tente de s'authentifier auprès du serveur sans posséder le composant matériel de l'utilisateur (en tentant de simuler celui-ci par exemple par essai des différentes combinaisons).

- **M2.Interception_réseau**

  Un attaquant intercepte les trames échangées entre le client et le serveur (pendant l'enrôlement ou l'authentification) de manière à connaître les données d'authentification de l'utilisateur.

- **M3.Rejeu**

  Un attaquant rejoue les trames d'authentification échangées entre le client et le serveur de manière à s'authentifier comme l'utilisateur légitime.

- **M4.Vol_local**

  Un attaquant tente de capturer des données sensibles sur le poste client à la fin de la session (pour retrouver les données d'authentification par exemple).

7. DESCRIPTION DES FONCTIONS DE SÉCURITÉ DU PRODUIT

La bibliothèque CoreLib représente la couche bas-niveau du Plugin.

Le produit a pour fonctionnalité principale de collecter et de transmettre au serveur de façon sécurisée les données matérielles côté client pour permettre une authentification multi-facteur non rejouable associée à un élément matériel au choix de l'utilisateur client.

Les fonctions de sécurité de la bibliothèque sont les suivantes :

- **F1.Enrôlement**

  La bibliothèque met en œuvre les étapes suivant dans le processus d'enrôlement :

  - récupération des politiques de sécurité pour les équipements autorisés et des propriétés de ces équipements (fournit par le serveur Digital DNA) ;
  - analyse des équipements « connectés » au poste client : l'empreinte est calculée en récupérant diverses informations du matériel sélectionné par l'utilisateur : numéros de séries, nom du fabriquant, du produit, etc. ;
  - hashage et chiffrement des empreintes (ADNs) obtenus : dans cette phase les algorithmes SHA1 et SHA256 sont utilisés dans la génération de l'ADN afin d'en assurer l'intégrité et l'ADN est chiffré avec l'algorithme RSA-OAEP ;
  - envoi de ces données au serveur de façon chiffrée : le chiffrement par RSA permet de transporter l'ADN du matériel dans un canal sécurisé vers le serveur DDNA.

  Pour assurer l'intégrité des données échangées durant l'enrôlement, en particulier l'ADN des équipements envoyés par la CoreLib, la fonction de hachage SHA-2, soit SHA-256 issue de la bibliothèque Crypto++ (http://www.cryptopp.com/, voir fichier « sha2.h » pour plus de détails) est utilisée. Pour assurer l'authenticité de la réponse du serveur, l'algorithme HMAC-SHA256, également issue de la bibliothèque Crypto++, est utilisé.

- **F2.Authentification**

  La bibliothèque permet d'authentifier un utilisateur :

  - récupérations des politiques (équipements autorisés) et du défi;
  - génération de la réponse au défi: les mécanismes SHA256 et HMAC-SHA256 servent à générer une réponse à un défi en employant l'ADN.

- **F3.Communication_sécurisée**

  Les communications entre le client et le serveur d'authentification sont protégées via le protocole HTTPS et les informations transmises sont également protégées en confidentialité par l'AES.

	F1.Enrôlement	F2.Authentification	F3.Communication_sécurisée
M1.Falsification_composant_matériel	X	X	
M2.Interception_réseau		X	X
M3.Rejeu		X	
M4.Vol_local	X	X	

Tableau 1 - Matrice de traçabilité

Fin du document