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-2014/02

## Digital DNA Corelib
## Version 3.2.0

*Paris, le 21 mars 2014*

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

[Original signé]
Contre-amiral Dominique RIBAN

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.anssi@ssi.gouv.fr

| |
|---|
| *Référence du rapport de certification*<br>**ANSSI-CSPN-2014/02** |
| *Nom du produit*<br>**Digital DNA Corelib** |
| *Référence/version du produit*<br>**Version 3.2.0** |
| *Catégorie de produit*<br>**Identification, authentification et contrôle d'accès** |
| *Critères d'évaluation et version*<br>**CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*** |
| *Développeur*<br>**Login People**<br>**Buropolis 2**<br>**1240 route des Dolines**<br>**Sophia Antipolis**<br>**06560 Valbonne** |
| *Commanditaire*<br>**Login People**<br>**Buropolis 2**<br>**1240 route des Dolines**<br>**Sophia Antipolis**<br>**06560 Valbonne** |
| *Centre d'évaluation*<br>**AMOSSYS**<br>**4 bis allée du Bâtiment**<br>**35000 Rennes** |

# 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 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 la bibliothèque logicielle « *Digital DNA Corelib* » développée par Login People, en version 3.2.0.

La bibliothèque, intégrée dans son environnement d'exploitation, permet de renforcer le processus d'authentification pour l'accès au réseau d'une organisation, en utilisant un ou plusieurs périphériques[1] appartenant à l'utilisateur et connectés au poste client.
Le produit permet ainsi notamment de n'autoriser les connexions au réseau cible que depuis un terminal maîtrisé par l'organisation.

Lors de la phase d'enrôlement, les empreintes des matériels sélectionnés et connectés au poste client sont calculées par la bibliothèque (intégrée sous forme de *plug in* sur le poste ou accessible via RDP[2] depuis une machine distante) et envoyées de manière sécurisée au serveur *Digital DNA*.

Lors de la phase d'authentification, les empreintes des matériels présentés par l'utilisateur sont à nouveau calculées et vérifiées par le serveur Digital DNA au cours d'un échange de type challenge/réponse. L'utilisateur est authentifié, si et seulement si l'identifiant, le mot de passe et les empreintes présentés sont identiques à ceux utilisés lors de l'enrôlement.

La bibliothèque *Digital DNA Corelib* est intégrée dans les composants clients suivants :
- le *Plug In*, fourni sous la forme d'un module pour navigateur web ou d'un kit de développement web ou client riche ;
- le *Winlogon*, basé sur le *Credential Provider* de Windows et installable sous la forme d'un package MSI ;
- le *Remote Desktop Add-On*, installé sur une machine distante via RDP ;
- l'application *DDNA Tech* qui remplace le *Plug In* pour les terminaux mobiles équipés du système Android ou iOS. Elle est téléchargeable depuis les magasins d'applications officiels de ces deux plateformes.

La bibliothèque *DDNA Corelib* se base elle-même sur d'autres bibliothèques qui fournissent des fonctions nécessaires à son fonctionnement :
- *Utils* : fonctions usuelles pour toutes les autres bibliothèques comme la manipulation de chaînes de caractères, de hash, etc.
- *Reader* : récupération des données matérielles ;
- *QKI* : définition des objets représentant les équipements et leur ADN ;
- *SAWS-Native* : interface haut-niveau pour le système de gestion des équipements.

[1] Les périphériques pouvant être utilisés avec le produit sont de type ordinateur, ordiphone, tablette tactile, clé USB et plus globalement tout dispositif de stockage de masse.
[2] Remote Desktop Protocol.

Pour fonctionner, le composant client intégrant la bibliothèque doit pouvoir communiquer avec un serveur *Digital DNA Server*. Ce dernier inclut un serveur Radius permettant de simplifier l'intégration dans le réseau de l'entreprise.

## 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 – firewall |
| ☐ 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 - matériel et logiciel embarqué |
| ☐ 99- Autres |

### *1.2.2. Identification du produit*

La version certifiée du produit est la bibliothèque *Digital DNA Corelib* version 3.2.0, incluse pour les besoins de l'évaluation dans un *Plug In* installé sur les navigateurs suivants :

- Mozilla Firefox,
- Internet Explorer,
- Google Chrome.

### *1.2.3. Services de sécurité*

Les services de sécurité fournis par le produit faisant l'objet de l'évaluation sont :

- l'enrôlement, comprenant la récupération et l'analyse des politiques de sécurité depuis le serveur *Digital DNA (DDNA)*, l'analyse des équipements connectés au poste client et le calcul de leur empreinte, le hachage et le chiffrement de l'empreinte et l'envoi au serveur via HTTPS ;
- l'authentification, comprenant la récupération et l'analyse des politiques de sécurité et du défi depuis le serveur et la génération de la réponse au défi ;
- la communication sécurisée entre le client et le serveur d'authentification via l'utilisation du protocole HTTPS.

### *1.2.4. Configuration évaluée*

La TOE est constituée des cinq bibliothèques définies au chapitre 1.1.

Dans le cadre de l'évaluation et comme indiqué dans la cible de sécurité [CDS], le produit a été livré en version 3.2.0 sous la forme du *Plug In* « *The Digital DNA Technology plugin* ».
Il a été installé sur les navigateurs suivants :

- Mozilla Firefox, version 25.0.1,

- Microsoft Internet Explorer, version 10.0.9200.16635,
- Google Chrome, version 31.0.1650.63m.

La version 5.6.2 du serveur DDNA a été utilisée pour l'évaluation.
Le chapitre 2.3.2 détaille l'installation du produit et la plateforme mise en place pour l'évaluation.

# 2. L'évaluation

## 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. 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 a été conforme à la charge de travail prévue par la procédure CSPN.

## 2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

### *2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité*

#### 2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 3 « Description du produit »).

#### 2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 5 « Description des biens sensibles »).

#### 2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 6 « Description des menaces »).

#### 2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 7 « Description des fonctions de sécurité du produit »).

#### 2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 3.7 « Description des utilisateurs typiques concernés »).

### *2.3.2. Installation du produit*

#### 2.3.2.1. Plate-forme de test

Le *Plug In* « *The Digital DNA Technology plugin* » livré par le développeur a été installé sur les navigateurs suivants :

- Mozilla Firefox version 25.0.1,
- Microsoft Internet Explorer version 10.0.9200.16635,
- Google Chrome version 31.0.1650.63m.

Les postes client et administrateur utilisés pour l'évaluation sont situés sur deux réseaux distincts, et équipés respectivement du système Windows 7 Pro 32 et 64bits (avec Service Pack 1 dans les deux cas).
Les deux réseaux sont connectés chacun à une interface du serveur VMWare ESXi, lequel exécute deux machines virtuelles pour le serveur DDNA (version 5.6.2) et le serveur web.

La Figure 1 illustre la plateforme utilisée pour l'évaluation.

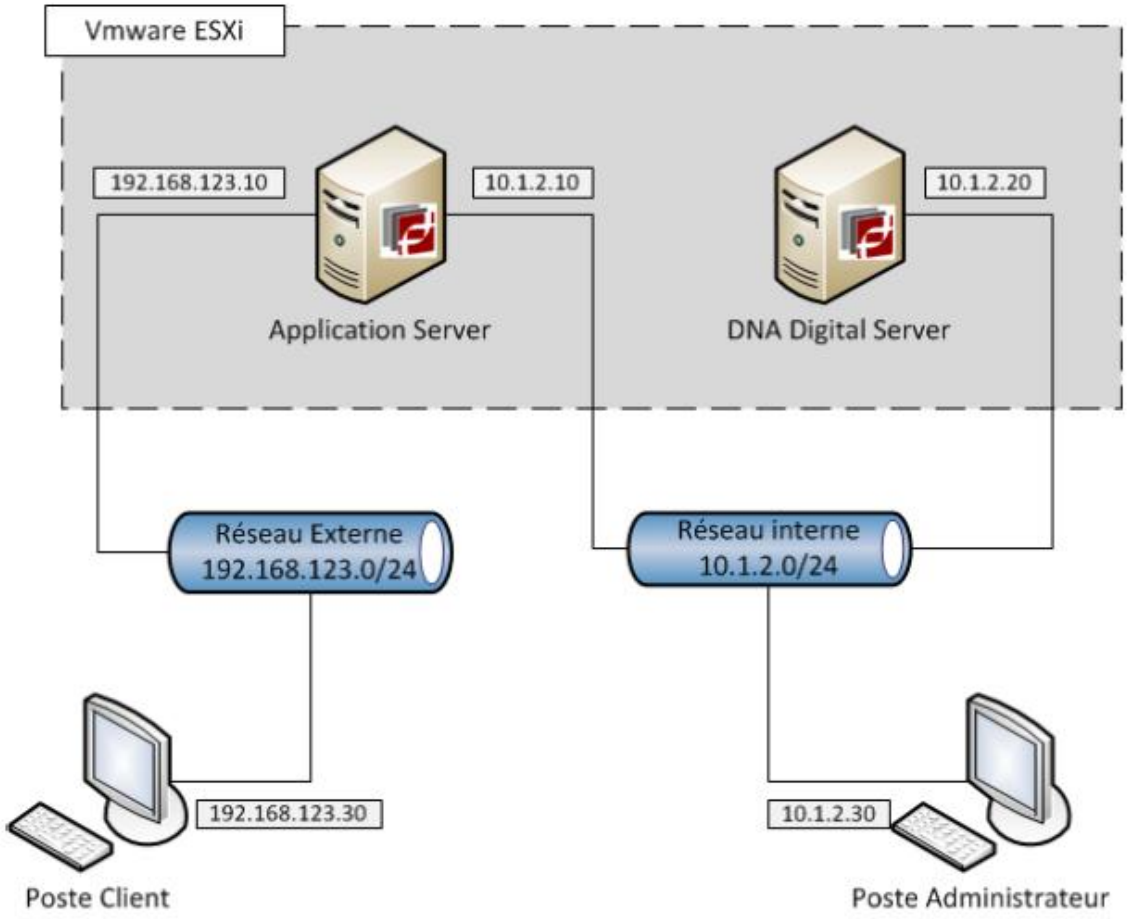


**Figure 1 : schéma de la plateforme d'évaluation**

#### 2.3.2.2. Particularités de paramétrage de l'environnement

Lors de l'installation de la plateforme, le navigateur du poste client ne parvenait pas à se connecter au serveur d'applications. En effet le serveur d'application utilise le protocole TLS en version 1.1 pour sécuriser ses communications. Or, cette version est prise en charge par Firefox (en version 25.0.1) ou Internet Explorer mais n'est pas activée par défaut.
Pour que le navigateur puisse se connecter au serveur d'applications, la procédure suivante doit être réalisée :

- ouvrir la page « *about:config* » du navigateur (pour Firefox) ;
- positionner la valeur du paramètre *security.tls.version.max* à 2.

Il faut aussi installer dans les navigateurs le certificat de l'autorité de certification qui a signé les certificats des deux serveurs.

Il est également à noter que, afin de pouvoir se connecter au serveur web pour enrôler un périphérique (connexion grâce à un OTP), le type de confirmation pour l'évènement « DNA Registration » dans la politique de sécurité, initialement positionné sur la valeur « none » doit être positionné sur la valeur « email ».

#### 2.3.2.3. Options d'installation retenues pour le produit

Le cloisonnement entre les deux serveurs a été mis en place et est recommandé dans la documentation du produit, de même que l'utilisation d'un certificat signé par une autorité de certification de confiance.
Aucune autre option d'installation particulière n'a été retenue. La configuration utilisée est détaillée au chapitre 2.3.2.1.

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

Sans objet.

#### 2.3.2.5. Durée de l'installation

L'installation a nécessité une journée.

#### 2.3.2.6. Notes et remarques diverses

L'installation du produit et sa configuration initiale sont bien documentées et peuvent être réalisées facilement.

### *2.3.3. Analyse de la documentation*

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et précise. Aucune non-conformité n'a été relevée.

### *2.3.4. Revue du code source (facultative)*

Le code source de la bibliothèque *Digital DNA Corelib* a été fourni par LoginPeople. Il s'agit de code C++ dont l'arborescence est décrite dans le document [DOC]. L'évaluateur s'est concentré sur le répertoire « *common* », identifié comme répertoire racine du code source concernant directement la TOE.
Dans l'ensemble, le code source est clair, bien commenté et réparti dans divers répertoires et fichiers correspondant aux classes et objets représentés.

#### *2.3.5. Fonctionnalités testées*

| Fonctionnalité | Résultat |
|---|---|
| Enrôlement | **Réussite** |
| Authentification | **Réussite** |
| Communication sécurisée | **Réussite** |

#### *2.3.6. Fonctionnalités non testées*

Sans objet.

#### *2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités*

Sans objet.

#### *2.3.8. Avis d'expert sur le produit*

Le fonctionnement du produit est conforme à ses spécifications fonctionnelles.

#### *2.3.9. Analyse de la résistance des mécanismes et des fonctions*

##### 2.3.9.1. Liste des fonctions et des mécanismes testés

Les fonctions listées au 2.3.5 ont été évaluées.

##### 2.3.9.2. Avis d'expert sur la résistance des mécanismes

Le produit dans sa version évaluée offre des mécanismes globalement robustes et à l'état de l'art.

#### *2.3.10. Analyse des vulnérabilités (conception, construction…)*

##### 2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier.

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

Aucune politique de mot de passe n'étant définie par défaut, l'évaluateur a mis en évidence la possibilité de mettre en œuvre une attaque en force brute applicable aux mots de passe faibles. Les guides du produit (voir [GUIDES]) contiennent cependant des recommandations pour la mise en place d'une politique de mot de passe forte. Cette vulnérabilité est donc considérée comme résiduelle.

De plus, certaines informations peuvent être lues depuis la mémoire du navigateur à l'aide d'outils accessibles au grand public. Ces informations ne suffisent cependant pas à un attaquant potentiel pour être authentifié à la place d'utilisateur légitime.

#### *2.3.11. Accès aux développeurs*

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit, lequel a fait preuve de disponibilité et d'une bonne maîtrise de son produit.

#### *2.3.12. Analyse de la facilité d'emploi et préconisations*

##### 2.3.12.1. Cas où la sécurité est remise en cause

La solution évaluée ne permet pas de compenser l'utilisation d'un mot de passe faible. Il est ainsi fortement recommandé, comme indiqué dans les [GUIDES], de mettre en place une politique de gestion des mots de passe forte.

##### 2.3.12.2. Recommandations pour une utilisation sûre du produit

Les hypothèses définies dans la cible doivent être respectées pour assurer une utilisation sûre du produit, notamment l'hypothèse « H4.Client_Poste_sécurisé » qui demande que le poste client soit utilisé comme composant matériel pour l'enrôlement et l'authentification.
En outre, comme indiqué au chapitre précédent, il est recommandé de mettre en place une politique de gestion des mots de passe forte.

##### 2.3.12.3. Avis d'expert sur la facilité d'emploi

Moyennant le respect des recommandations évoquées précédemment, l'évaluateur n'a pas identifié de cas où le produit serait configuré ou utilisé de façon non sûre mais qu'un utilisateur pourrait raisonnablement croire sûre.

##### 2.3.12.4. Notes et remarques diverses

Sans objet.

## 2.4. Analyse de la résistance des mécanismes cryptographiques

La liste de référence des mécanismes cryptographiques est celle fournie par la cible de sécurité [CDS] et les spécifications cryptographiques [SPEC_CRY]. La résistance de ces mécanismes a été analysée par l'évaluateur. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [RTE] et concluent que, si les recommandations présentes dans [GUIDES] sont appliquées, les mécanismes analysés atteignent le niveau standard défini dans le référentiel cryptographique de l'ANSSI (voir [REF-CRY]) sauf en ce qui concerne l'utilisation de la fonction de hachage SHA-1. L'utilisation de cette dernière n'entraine cependant pas de vulnérabilité exploitable pour le niveau d'attaquant considéré.

## 2.5. Analyse du générateur d'aléas

Les moyens mis en œuvre pour la génération des nombres aléatoires qui sont utilisés dans différentes fonctions permettent d'atteindre le niveau de résistance aux attaques visé par la CSPN.

# 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 « *Digital DNA Corelib*, version 3.2.0 » 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 d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport.

# Annexe 1. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | *Cible de sécurité CSPN - Bibliothèque "Digital DNA CoreLib" version 3.2.0* ;<br>Référence : *CSPN-ST-LOE002-1.03* ;<br>Version : *1.03* ;<br>Date : *05 février 2014.* |
| [RTE] | *Rapport Technique d'Evaluation CSPN*<br>*Digital DNA Corelib version 3.2.0 ;*<br>Référence : *CSPN-RTE-ELLIMAC-2.01* ;<br>Version : 2.01 ;<br>Date : *05 février 2014.* |
| [SPEC-CRY] | Digital DNA CoreLib Version 1. 1 - Spécifications Cryptographiques *;*<br>Version : 1.1 ; |
| [GUIDES] | Guide d'utilisation :<br>*Digital DNA Corelib Version 3.2.0 – Documentation ;*<br>*Digital DNA Server – Installation & Configuration Guide (plugin : version 3.2.0) ;*<br>Guide d'administration :<br>*Digital DNA Server – Integration Guide (plugin :version 3.2.0) ;*<br>*Digital DNA Server –Configuration & Administration Guide (plugin : version 3.2.0) ;*<br>*Installation VMs Version 1.0 – Quick start Guide.* |

# 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 (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011.<br><br>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011.<br><br>Documents disponibles sur http://www.ssi.gouv.fr/ |
| [REF-CRY] | Référentiel général de sécurité, version 1.0, annexe B1 :<br>Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20.<br><br>Documents disponibles sur http://www.ssi.gouv.fr/ |
| [GUIDE-ANSSI] | Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013.<br>Disponible sur www.ssi.gouv.fr/hygiene-informatique. |