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-2016/08

Systancia

IPdiva Secure

Version 8.0 (build 8.1066, patch IPD-15934)

Paris, le 19 mai 2016

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-2016/08

Nom du produit

IPdiva Secure

Référence/version du produit

Version 8 (build 8.1066, patch IPD-15934)

Référence de la cible de sécurité

Cible de sécurité

Référence : CSPN-ST-IPdiva Secure-2.02 en date du 3 mai 2016

Catégorie de produit

Identification, authentification et contrôle d'accès

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*

Commanditaire

Systancia
3 rue Paul Henri Spaak
68390 Sausheim
France

Centre d'évaluation

Amossys
4 bis allée du bâtiment, 35000 Rennes, France

Fonctions de sécurité évaluées

Authentification et contrôle d'accès
Audit
Communication externes sécurisées
Communication internes sécurisées
Gestion des biens cryptographiques
Vérification de l'intégrité de la solution par comparaison d'empreintes

Fonctions de sécurité non évaluées

Néant

Restrictions 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 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 « IPdiva Secure, version 8.0 (build 8.1066, patch IPD-15934) » développé par *SYSTANCIA*.
Ce produit permet la protection, le contrôle et la traçabilité de tous les accès externes aux ressources d'un système d'information.
IPdiva Secure est une solution à architecture répartie, qui permet un cloisonnement entre les serveurs applicatifs situés sur le réseau interne, et le réseau externe. Ce produit permet que les ressources internes ne soient pas directement exposées sur Internet.
La solution comprends trois composants séparés : le serveur IPdiva (ou serveur de médiation) la passerelle IPdiva (ou *IPdiva Gateway*) et un serveur de journalisation IPdiva IIS.
IPdiva Server doit constituer l'unique point d'entrée vers les réseaux hébergeant les systèmes à accéder ou les applications à protéger. Il permet de mutualiser l'authentification et le contrôle d'accès aux serveurs ainsi protégés. Les traces des accès distants sont par ailleurs centralisées sur le serveur IPdiva IIS.
IPdiva Gateway est l'interface de relais entre IPdiva Server et les applications, les fichiers ou les systèmes devant être accessibles à distance. La communication est sécurisée entre IPdiva Server et IPdiva Gateway par un tunnel SSL.
La Figure 1 décrit une architecture type.

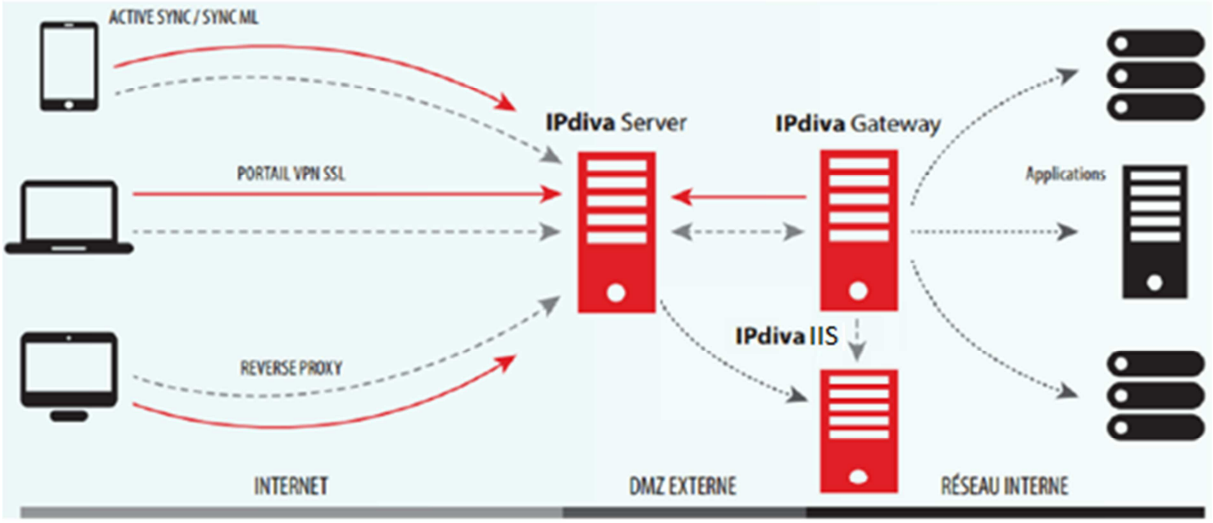

Figure 1 – Architecture type d'un déploiement.

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 – environnement d'exécution sécurisé
☐ 11 – matériel et logiciel embarqué
☐ 12 – terminal de réception numérique (Set top box, STB)
☐ 13 – automate programmable industriel

1.2.2. Identification du produit

Nom du produit	IPdiva Secure
Numéro de la version analysée	8.0 (build 8.1066, patch IPD-15934)

La version certifiée du produit peut être identifiée sur l'interface d'administration, une fois authentifié dans le coin inferieur droit de cette interface.

1.2.3. Configuration évaluée

Conformément à la cible de sécurité [CDS], le produit évalué ne correspond qu'à la version logicielle (et non à la version boîtier ou *appliance* du produit*).*
La configuration évaluée correspond à :

- un déploiement en mode dual, c'est-à-dire que le serveur IPdiva serveur se trouve en DMZ et les serveurs IPdiva Gateway et IP diva IIS se trouvent dans le réseau interne du système d'information ;
- une utilisation reverse proxy avec authentification ;
- une authentification par certificats.

Le paquet ipdiva-hostmanager-webserver (patch référence IPD-15934) a été installé.
Les composants IPDiva Server, IPDiva Gateway et IPDiva IIS ont été installés suivant la documentation d'installation [GUIDES] sur un système Debian de base correspondant à une installation strictement minimale conformément aux recommandations de sécurité [MAN-SECU].

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 a été 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, menaces, utilisateurs et fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Plateforme de test

La plateforme de test est constituée des éléments suivants pour les composants serveur :

- un serveur de médiation « IPdiva Server » : Linux Debian Jessie 8.2 64 bits ;
- une passerelle « IPdiva Gateway » : Linux Debian Jessie 8.2 64 bits ;
- un serveur de journalisation et d'intégrité « IPdiva IIS » sous la forme d'une machine virtuelle Linux Debian Jessie 8.2 64 bits.

Les trois postes clients suivants correspondent à des machines virtuelles :

- une machine client : Windows 7 professionnel Service Pack 1 64 bits ;
- une machine d'administration : Windows 7 professionnel Service Pack 1 64 bits ;
- une machine attaquante qui joue également le rôle de routeur : Kali 2 64 bits.

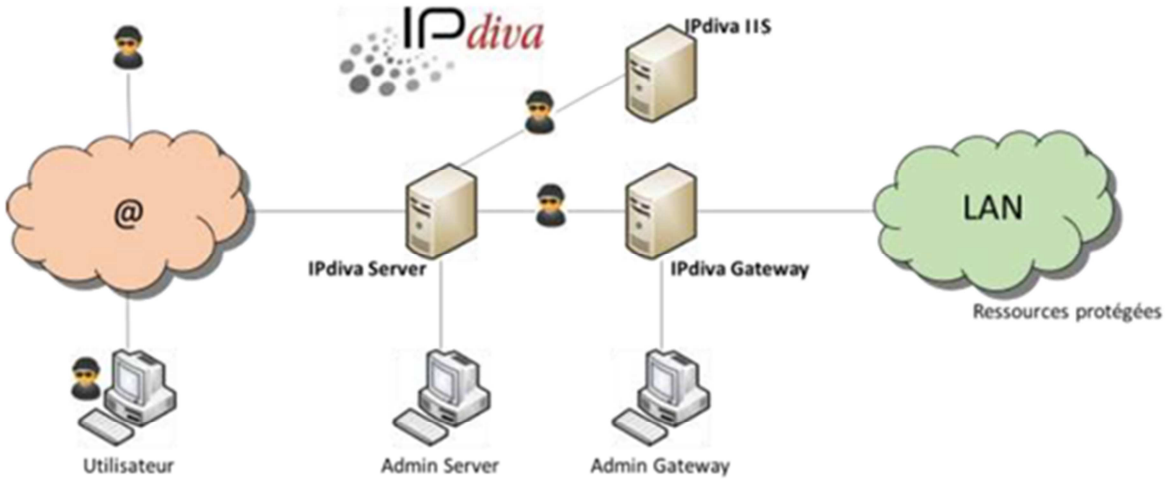

Figure 2 – Plateforme de test.

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

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.3.

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

Néant

2.3.1.4. Durée de l'installation

L'installation a été réalisée par un consultant de la société SYSTANCIA et a nécessité une demi-journée.

2.3.1.5. Notes et remarques diverses

Néant

2.3.2. Analyse de la documentation

La documentation est claire et bien illustrée.

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

Les fonctions de sécurité ont été testées et sont conformes à la cible de sécurité [CDS].
Concernant la fonction de sécurité « Vérification de l'intégrité de la solution par comparaison d'empreintes », il doit être noté que si la vérification de l'intégrité du produit est en échec, cet évènement n'est pas journalisé. Mais dans ce cas le produit ne sera pas opérationnel.

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

Toutes les fonctions de sécurité testées ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation de la cible d'évaluation.

2.3.6. Analyse des vulnérabilités (conception, construction…)

2.3.6.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues et exploitables sur ce produit dans sa version évaluée.

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

Il n'a pas été découvert de vulnérabilité propre au produit ou son implémentation pouvant remettre en cause la sécurité du produit.

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

Sans objet.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Outre le suivi des recommandations de sécurité [MAN-SECU], l'administrateur doit maîtriser les concepts et usages des certificats électroniques et devra s'attacher à les générer en respectant les règles du [RGS].
Il s'assurera grâce à la fonctionnalité « centre de sécurité » offerte par le produit qu'elle affiche le message suivant : « Toutes les recommandations de sécurité de Systancia sont respectées ».
L'administration du produit devra se faire en respectant le guide d'hygiène informatique de l'ANSSI [GUIDE-ANSSI] et en particulier la règle 29 relative à l'utilisation d'un réseau dédié à l'administration des équipements.
Enfin, dans la mesure où certaines actions sont traitées et journalisées par le serveur Apache d'IPdiva Server, l'administrateur devra soit auditer ces journaux directement sur le serveur Apache, soit les centraliser.

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

L'évaluateur n'a pas identifié de cas où un administrateur, formé et compétent s'appuyant sur les guides [GUIDES], ainsi que les recommandations de sécurité [MAN-SECU], viendrait à configurer ou utiliser le produit de façon non sûre. En particulier le « centre de sécurité » mentionné au paragraphe 2.3.8.2 vise à éviter une telle situation.

2.3.8.4. Notes et remarques diverses

Sans objet.

2.4. Analyse de la résistance des mécanismes cryptographiques

L'analyse de la résistance des mécanismes cryptographique a été effectuée par l'évaluateur. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [RTE]. Si certains algorithmes employés sont non conforme au référentiel cryptographique de l'ANSSI [REF-CRY], l'évaluation n'a pas mis en évidence de vulnérabilité liée à l'emploi de ces algorithmes.

2.5. Analyse du générateur d'aléas

Les moyens mis en œuvre pour la génération et le retraitement des nombres aléatoires utilisés par la solution *IPdiva Secure*, 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 *IPdiva Secure, version 8.0 (build 8.1066, patch IPD-15934)* 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 de ce certificat doit configurer le produit selon les prescriptions du paragraphe 1.2.3 et à suivre les recommandations du paragraphe 2.3.8.2.
L'utilisateur devra par ailleurs s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN Produit IPdiva Secure 8* Référence : CSPN-ST-IPdiva Secure-2.02; Version : 2.02 ; Date : *03/05/2016*
[RTE]	*Rapport Technique d'Évaluation CSPN Produit IPdiva Secure - version 8* Référence : RTE-CSPN-IPDIVA2-1.01 ; Version : 1.01 ; Date : *04/05/2016*
[CRY]	*Expertise des mécanismes cryptographiques Produit IPdiva Secure - version 8* Référence : CRY-CSPN-IPDIVA2-1.00 ; Version : 1.00 ; Date : *01/04/2016*
[GUIDES]	*Ipdiva Secure 8 - Guide d'installation et des premiers pas – Version Client Mode* Référence : Documentation IPdiva Standalone CSPN_v4 ; Date : *24/03/2016* *Ipdiva Secure 8 – Manuel Utilisateur - Guide de l'utilisateur* Référence : MU-MEDV8-0_V06 *IPdiva Secure 8 – Manuel Super-Utilisateur – Guide du Super-Utilisateur*, Référence : MSU-MEDV8-0_V07, Date : *Février 2016*
[MAN-SECU]	*Ipdiva Secure 8 – Sécurisation avancée* Version : 1.06 ; Référence : MSA-MED7-Securisation avancée_V06 ; Date : *22/02/2016*

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 (CSPN) 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 http://www.ssi.gouv.fr/
[NOTE-3]	Méthodologie pour l'évaluation logicielle d'automates programmables industriels en vue d'une certification de sécurité de premier niveau ANSSI-CSPN-NOTE-03/1 du 30 juillet 2015. Documents disponibles sur http://www.ssi.gouv.fr/
[REF-CRY]	Référentiel général de sécurité, version 2.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03. 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. Disponible sur www.ssi.gouv.fr/hygiene-informatique.