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-2014/04

DZ-NETWORK
Version 1.0

Paris, le 12 juin 2014

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

[Original signé]

Guillaume POUPARD

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 **ANSSI-CSPN-2014/04**
Nom du produit **DZ-NETWORK**
Référence/version du produit **1.0**
Catégorie de produit **Pare-feu**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **SECLAB-FR** **8 rue Eugène Lisbonne** **34000 Montpellier** **France**
Commanditaire **EDF R&D** **1, avenue du Général de Gaulle** **92141 Clamart** **France**
Centre d'évaluation **AMOSSYS** **4 bis allée du bâtiment,** **35000 Rennes** **France**

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 DZ-NETWORK est un dispositif permettant l'échange d'information entre deux réseaux de niveaux de confiance différents. Il réalise une rupture protocolaire ainsi qu'un filtrage des informations échangées lors des transferts via les protocoles FTP et Modbus-TCP.
Le produit se présente sous forme d'une *appliance*, il est composé de deux systèmes embarqués (nommés « PC haut » et « PC bas »), l'un situé en zone basse (réseau non maîtrisé) et l'autre en zone haute (réseau maîtrisé). Ces systèmes sont reliés par un FPGA (*Field-Programmable Gate Array*) de filtrage et de rupture protocolaire. Son objectif est de protéger la zone haute d'attaques provenant de la zone basse.

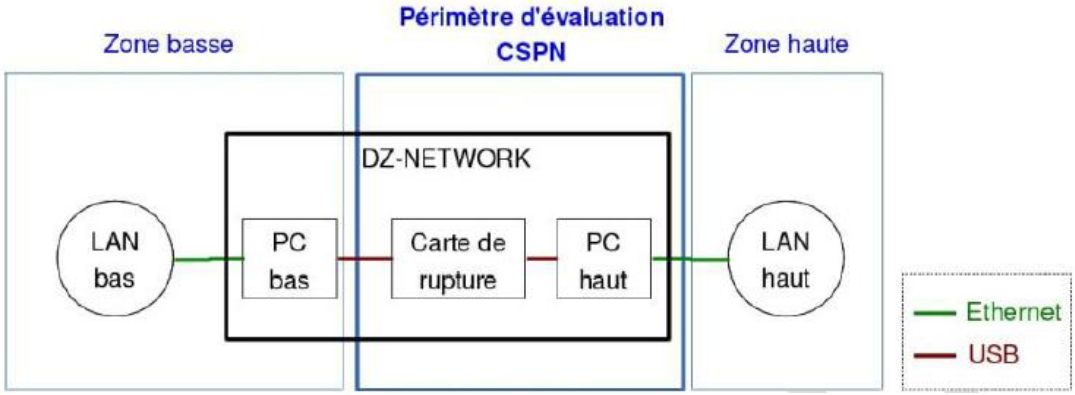

Figure 1- Périmètre de l'évaluation

On distingue donc deux cas de transferts :
- via le protocole FTP ;
- via le protocole Modbus-TCP.

1.1.1. Transfert via le protocole FTP

1.1.1.1 Principes de fonctionnement

Dans le cas du protocole FTP, l'échange d'information est bidirectionnel. Le scénario ci-après décrit un transfert entre la zone basse et la zone haute.
L'utilisateur dépose un fichier sur un serveur *Pure-FTPd* implémenté sur le PC embarqué de la zone basse. Si la carte électronique valide, au regard de sa politique de sécurité, le fichier, ce dernier est transféré automatiquement au PC embarqué de la zone haute qui implémente un serveur *Pure-FTPd* permettant à un utilisateur présent sur le LAN de la zone haute de récupérer les fichiers transférés. Une entrée dans un fichier de journaux distinct pour chacun des serveurs FTP indique si le fichier a été transféré ou bloqué.

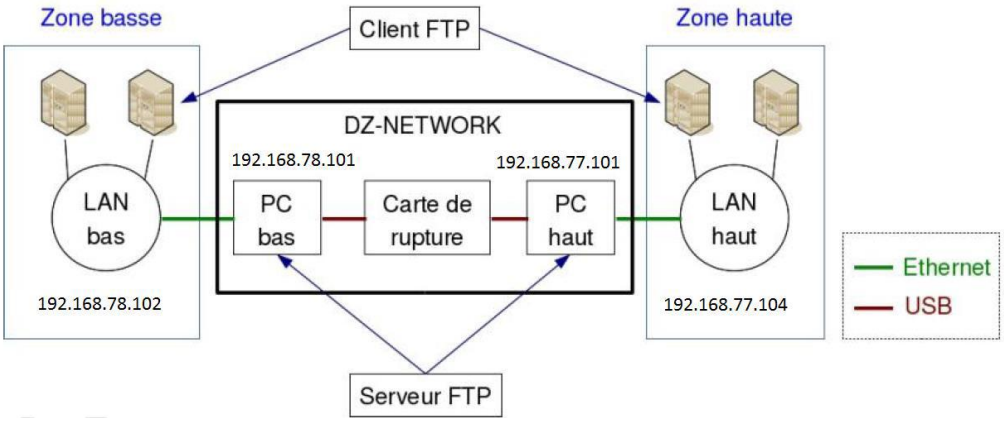

Figure 2 - Schéma d'utilisation de DZ-NETWORK via le protocole FTP

Pour transférer un fichier, il suffit à l'utilisateur de s'authentifier sur le serveur FTP de la zone basse, puis de déposer le fichier dans le dossier « /to-send ». Le fichier est ensuite transféré dans le dossier « /queue » où les paramètres de filtrage sont appliqués.

Deux possibilités existent suivant le résultat de ce filtrage :

- si le fichier respecte les règles, une copie est enregistrée dans le dossier « /sent » et le fichier est transféré vers la zone haute dans le dossier « /incoming »;
- si le fichier ne respecte pas les règles, il est directement déplacé dans le dossier « /errors » de la zone basse.

Dans les deux cas, une entrée est ajoutée dans le journal des événements « logs.txt » de la zone basse.

1.1.1.2 Règles de filtrage FTP

Le filtrage applicatif consiste à s'assurer du respect des règles suivantes :

- les extensions doivent être en minuscules ;
- les extensions autorisées sont :
  - jpeg ;
  - tpg ;
  - tiff ;
  - tif ;
  - bmp ;
  - png ;
  - pdf ;
  - txt ;
- le nom des fichiers doit contenir uniquement les caractères autorisés suivants :
  - les lettres majuscules ;
  - les chiffres ;
  - les espaces ;
  - les caractères '~', '-', '.' et '_' ;
- la taille maximale des fichiers (quel que soit le type de fichier) est de 10 Mo ;
- les fichiers pdf doivent faire moins de 20 pages ;
- les fichiers txt doivent contenir uniquement les caractères suivants :
  - les caractères encodés sur un octet (Basic Latin) :

- le caractère NUL (0x00) ;
- le caractère tabulation (0x09) ;
- les caractères de retour chariot (0x0A et 0x0D) ;
- les caractères imprimables (entre 0x20 et 0x7E inclus) ;

- les caractères encodés sur deux octets suivant l'extension Latin-1 Supplément1 de l'encodage UTF-8 (codes hexadécimaux compris entre 0xC280 et 0xC2BF, ou entre 0xC380 et 0xC3BF inclus) ;
- les caractères encodés sur deux octets suivant l'extension *Greek* and *Coptic* de l'encodage UTF-8 (codes hexadécimaux compris entre 0xCE80 et 0xCEBF, ou entre 0xCF80 et 0xCFBF inclus).

1.1.2. Transfert via le protocole Modbus-TCP

1.1.2.1 Principes de fonctionnement

Dans le cas du protocole Modbus-TCP, l'échange d'information est à l'initiative du client Modbus présent en zone haute. Le client Modbus présent sur le LAN haut peut émettre une requête au PC haut. Si la requête est légitime, le contenu Modbus de la trame TCP/IP est transféré au PC bas au travers de la carte électronique. Le PC bas émet alors une trame Modbus à destination d'un serveur Modbus présent sur le réseau bas. Si la réponse de ce dernier est valable, elle est transmise par le PC bas au PC haut via la carte électronique. Le PC haut transfère alors les informations au client Modbus.

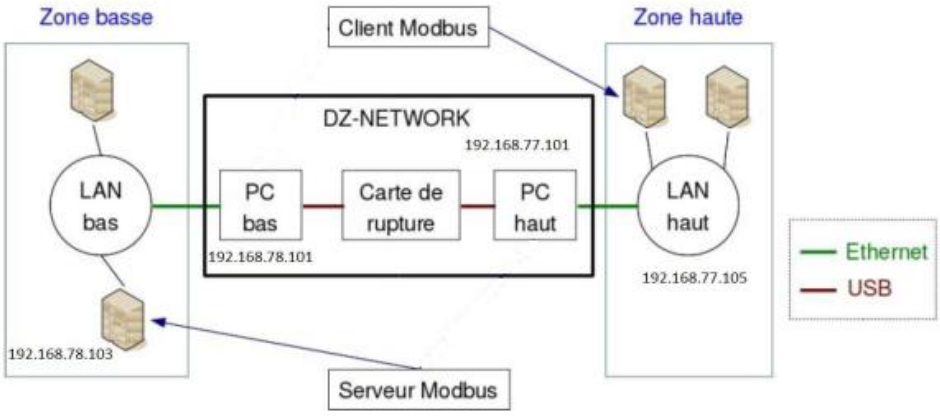

Figure 3 - Schéma d'utilisation de DZ-NETWORK via le protocole Modbus

1.1.2.2 Règles de filtrage Modbus-TCP

Les commandes du client Modbus autorisées par DZ-NETWORK sont les suivantes :

- READ COILS (code 0x01) ;
- READ DISCRETE Inputs (0x02) ;
- READ HOLDING REGISTER (0x03) ;
- READ INPUT REGISTER (0x04) ;
- WRITE SINGLE COIL (0x05) ;
- WRITE SINGLE REGISTER (0x06).

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

Nom du produit	DZ-NETWORK
Numéro de version analysée	1.0

La version certifiée du produit est identifiable par les éléments du tableau ci-dessus. Ces derniers sont visibles à tout moment par un administrateur authentifié de deux manières différentes :

- en utilisant un câble USB A/B pour se connecter au port console de la carte de rupture ;
- dans le journal des événements `logs.txt` présent en zone basse et en zone haute.

1.2.3. Services de sécurité évalués

Les principaux services de sécurité fournis par le produit sont :

- le filtrage du format des données transférées ;
- la protection contre l'accès direct au réseau haut depuis le réseau bas (rupture protocolaire) ;
- la protection contre les tentatives de modification et d'altération de la configuration de filtrage du dispositif via les interfaces accessibles du dispositif.

1.2.4. Configuration évaluée

Les deux configurations, FTP et Modbus-TCP, ont été évaluées.

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 lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit ne comportant pas de mécanismes cryptographiques, soit 25 hommes x jours.

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 « argumentaire (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 que le produit doit protéger»).

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 3.6 « description des utilisateurs typiques concernes (utilisateurs finaux, administrateurs, experts…) et de leur rôle particulier dans l'utilisation du produit »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Les plates-formes de test suivantes ont été déployées par l'évaluateur pour tester respectivement l'utilisation de DZ-NETWORK via le protocole FTP et via Modbus.

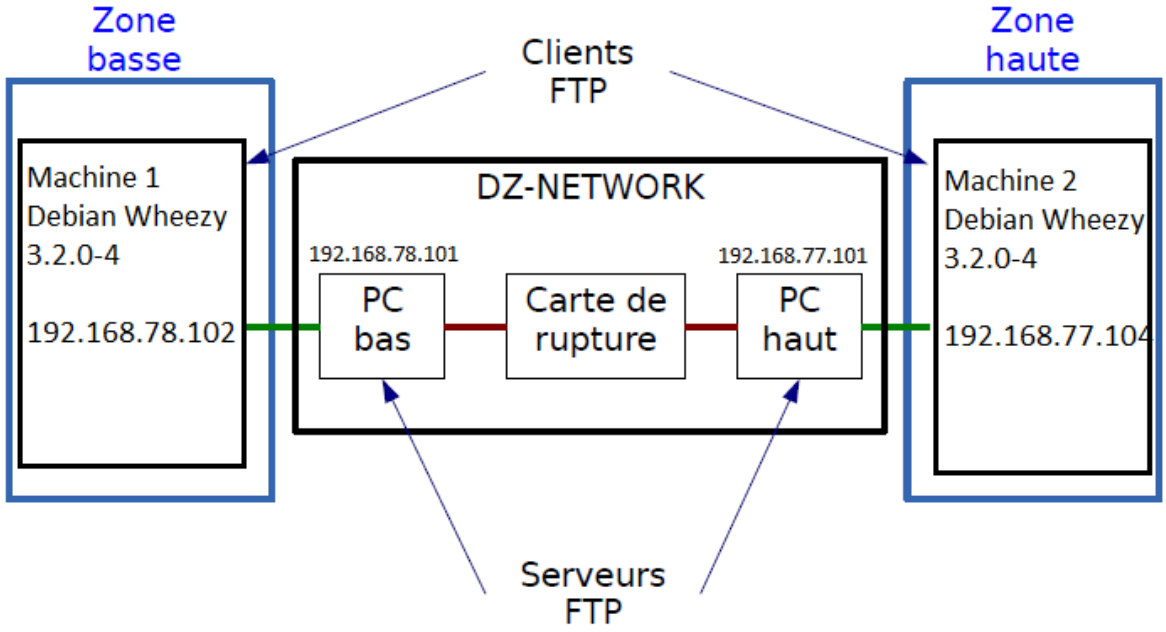

Figure 4 - Plate-forme de test FTP

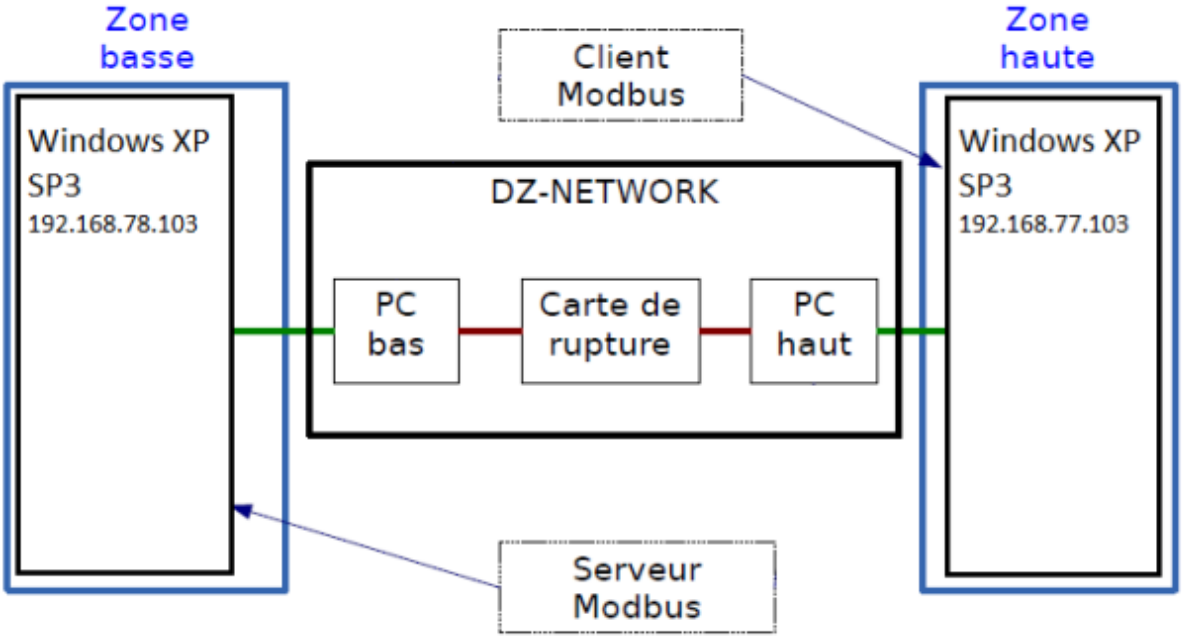

Figure 5 - Plate-forme de test Modbus

2.3.2.2. Particularités de paramétrage de l'environnement

Les PC embarqués haut et bas ne supportent pas IPV6.

2.3.2.3. Options d'installation retenues pour le produit

Aucune option d'installation n'est disponible.

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

L'installation consiste à brancher et démarrer l'*appliance* puis configurer l'environnement réseau. Pour paramétrer le serveur FTP, les adresses des PC haut et bas sont obtenues automatiquement via la fonction DHCP (*Dynamic Host Configuration Protocol*) de l'interface d'administration de DZ-NETWORK. Pour paramétrer le client et le serveur Modbus, l'adresse et le port d'écoute doivent être modifiés via les deux interfaces d'administration, conformément à la documentation.
DZ-NETWORK doit être le seul point d'entrée entre la zone basse et la zone haute. Il convient également de s'assurer que le dispositif DZ-NETWORK est installé dans un environnement adapté au niveau de sensibilité le plus élevé (c.à.d. que le dispositif doit être physiquement installé dans la zone haute).

2.3.2.5. Durée de l'installation

La mise en service s'effectue en moins de dix minutes.

2.3.2.6. Notes et remarques diverses

L'installation du produit est simple et consiste en une rapide configuration réseau du boitier une fois ce dernier branché et démarré. Les règles de filtrage sont figées lors de la production du boitier et ne sont pas modifiables. La procédure d'installation, détaillée dans [GUIDE], est claire et précise.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès au guide d'utilisation du produit [GUIDE]. La documentation est claire, complète et suffisante pour une bonne utilisation du produit. Le développeur a fait en sorte que l'utilisateur final saisisse le fonctionnement et les enjeux du produit. La documentation fournie permet d'installer et d'utiliser correctement le produit. Aucune non-conformité n'a été relevée.

2.3.4. Fonctionnalités testées

Les fonctions suivantes ont été soumises à des tests de conformité :

Fonctionnalité	Résultat
Filtrage du format des données	**Réussite**
Rupture protocolaire	**Réussite**
Protection de la configuration de filtrage	**Réussite**

2.3.5. Fonctionnalités non testées

Néant.

2.3.6. Synthèse des fonctionnalités testées / non testées et des non-conformités

Les fonctionnalités testées sont conformes à ce qui est décrit dans la cible de sécurité [CDS].

2.3.7. Avis d'expert sur le produit

Le produit est fonctionnellement conforme à sa cible de sécurité.

2.3.8. Analyse de la résistance des mécanismes et des fonctions

2.3.8.1. Liste des fonctions et des mécanismes testés

Les mécanismes de sécurité mis en œuvre par DZ-NETWORK sont des mécanismes de filtrage.

Fonction et mécanisme de filtrage
Blocage d'un fichier texte dont le contenu n'est pas conforme
Blocage d'un fichier texte dont le nom n'est pas conforme
Blocage d'un fichier dont la taille n'est pas conforme
Blocage d'un fichier dont le format n'est pas conforme
Blocage d'un fichier PDF dont le nombre de pages n'est pas conforme
Rupture protocolaire entre les machines de la zone haute et celles de la zone basse
Non interprétation des requêtes Modbus non autorisées
Non interprétation des réponses Modbus non autorisées

2.3.8.2. Avis d'expert sur la résistance des mécanismes

L'ensemble des tests menés n'a pas permis d'exploiter les vulnérabilités théoriques, connues ou spécifiques au produit, dans le temps imparti et avec les moyens matériels correspondant à une analyse de premier niveau. Le produit est sensible à une attaque par déni de services depuis la zone basse, qui rend le guichet bas indisponible. Ce déni de service nécessite un redémarrage et une suppression manuelle des fichiers impliqués mais ne permet pas le transfert de fichiers non autorisés.

2.3.9. Analyse des vulnérabilités (conception, construction…)

2.3.9.1. Liste des vulnérabilités connues

Des vulnérabilités connues ont été identifiées sur certaines bibliothèques de DZ-NETWORK. Cependant aucune n'est exploitable dans le contexte d'emploi visé.

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

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

2.3.10. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement aux questions posées.

2.3.11. Analyse de la facilité d'emploi et préconisations

2.3.11.1. Cas où la sécurité est remise en cause

Néant.

2.3.11.2. Recommandations pour une utilisation sûre du produit

Le produit doit être déployé dans un environnement sécurisé correspondant au niveau de sensibilité du réseau le plus élevé. L'utilisation du produit doit se faire par des utilisateurs formés et de confiance conformément à ce qui est décrit dans le guide utilisateur. En particulier les utilisateurs devront s'assurer que la taille du nom du fichier soumis sur le guichet bas est bien conforme au guide utilisateur.

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

Moyennant le respect des recommandations évoquées en 2.3.11.2, 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.

2.3.11.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

Sans objet.

2.5. Analyse du générateur d'aléas

Sans objet.

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 « DZ-NETWORK, version 1.0 » 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, notamment assurer la protection physique du produit.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN – DZ-NETWORK 1.2 ;* Référence : *CR-I2D-2013-029 ;* Version : *1.2*; Date : *09/04/2014.*
[RTE]	*Rapport Technique d'Évaluation CSPN – DZ-NETWORK version 1.0 ;* Référence : *CSPN-RTE-DZNETWORK-1.02* ; Version : *1.02* ; Date : *14/04/2014.*
[GUIDE]	*Documentation utilisateur DZ-NETWORK ;* Référence : *DZ-NETWORK-RW-RW-V1.0_Documentation_Utilisateur_V1.0.1 ;* Version : *1.0 RW/RW.*

Annexe 2. Références liées 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. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr.