



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-2010/03**

Dispositif d'échange sécurisé d'informations sans  
interconnexion réseau (DESIIR)

**DESIIR 1.0**

*Paris, le 12 avril 2010*

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

Patrick Pailloux  
[ORIGINAL SIGNE]



## 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 présumées 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](mailto:certification.anssi@ssi.gouv.fr)

La reproduction de ce document sans altération ni coupure est autorisée.

<i>Référence du rapport de certification</i>	<b>ANSSI-CSPN-2010/03</b>
<i>Nom du produit</i>	<b>Dispositif d'échange sécurisé d'informations sans interconnexion réseau (DESIIR)</b>
<i>Référence/version du produit</i>	<b>Version 1.0</b>
<i>Conformité à un profil de protection</i>	
<i>Critères d'évaluation et version</i>	<b>CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN, Phase expérimentale)</b>
<i>Développeur(s)</i>	<b>EDF R&amp;D – Département SINETICS 1 avenue du Général de Gaulle – BP408 92141 CLAMART CEDEX France</b>
<i>Commanditaire</i>	<b>EDF R&amp;D – Département SINETICS 1 avenue du Général de Gaulle – BP408 92141 CLAMART CEDEX France</b>
<i>Centre d'évaluation</i>	<b>AQL Groupe Silicomp 1 rue de la châtaigneraie, CS 51766, 35513 Cesson Sévigné Cedex, France Tél : +33 (0)2 99 12 50 00, mél : cesti@aql.fr</b>

## 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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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](http://www.ssi.gouv.fr).

# Table des matières

<b>1</b>	<b>LE PRODUIT .....</b>	<b>6</b>
1.1	PRESENTATION DU PRODUIT .....	6
1.2	DESCRIPTION DU PRODUIT EVALUE .....	7
1.2.1	<i>Catégorie du produit .....</i>	7
1.2.2	<i>Identification du produit.....</i>	7
1.2.3	<i>Services de sécurité .....</i>	7
1.2.4	<i>Configuration évaluée .....</i>	8
<b>2</b>	<b>L’EVALUATION .....</b>	<b>9</b>
2.1	REFERENTIELS D’EVALUATION .....	9
2.2	CHARGE DE TRAVAIL PREVUE ET DUREE DE L’EVALUATION.....	9
2.3	TRAVAUX D’EVALUATION .....	9
2.3.1	<i>Fonctionnalités, environnement d’utilisation et de sécurité.....</i>	9
2.3.2	<i>Installation du produit.....</i>	11
2.3.3	<i>Analyse de la conformité .....</i>	12
2.3.4	<i>Analyse de la résistance des mécanismes et des fonctions .....</i>	14
2.3.5	<i>Analyse des vulnérabilités (conception, implémentation.....)</i> .....	14
2.3.6	<i>Analyse de la facilité d’emploi et préconisations .....</i>	15
2.3.7	<i>Accès aux développeurs.....</i>	15
2.4	ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES .....	15
<b>3</b>	<b>LA CERTIFICATION .....</b>	<b>16</b>
3.1	CONCLUSION.....	16
3.2	RESTRICTIONS D’USAGE.....	16
	<b>ANNEXE 1. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>17</b>
	<b>ANNEXE 2. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>18</b>

# 1 Le produit

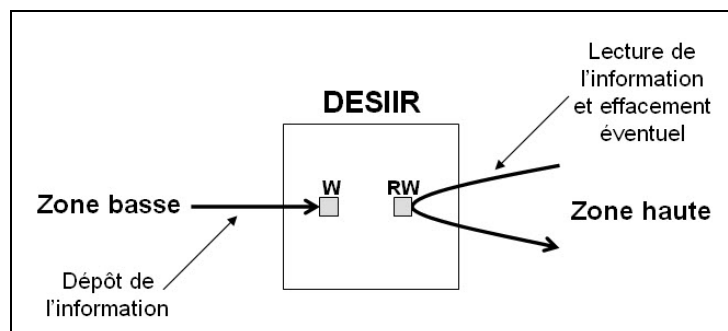
## 1.1 Présentation du produit

Le produit évalué est le « Dispositif d'échange sécurisé d'informations sans interconnexion réseau (DESIIR), Version 1.0 » développé par EDF R&D – Département SINETICS.

Le produit DESIIR (Dispositif d'Échange Sécurisé d'Informations sans Interconnexion Réseau) est un dispositif de filtrage permettant le transfert unidirectionnel de données entre deux machines (pouvant appartenir à deux domaines de confiance différents) via un point de stockage relais avec un filtrage restrictif sur le format des données transférées.



La figure ci-dessous présente le fonctionnement général du boîtier en mode « Write-Only ».



Le boîtier DESIIR est constitué de deux fiches femelles USB (*Universal Serial Bus*) de type B. L'entrée côté W permet de connecter la zone « basse » (écriture uniquement des

informations du réseau bas à destination du réseau haut) et l'entrée côté RW permet de connecter la zone « haute » (lecture et certaines écritures des informations contenues dans le boîtier). Chacune des entrées est repérée par une étiquette spécifique sur le produit.

La zone haute (aussi appelée le réseau haut) correspond au niveau de confiance le plus élevé et la zone basse (aussi appelée le réseau bas) est celle qui est potentiellement exposée à des malveillances.

Le produit DESIIR fonctionne comme une clé USB et est constitué de trois disques :

- disque « DESIIR » : disque d'échange entre les machines basse et haute ;
- disque « *backup* » : disque de sauvegarde ;
- disque « *debug* » : disque contenant le fichier de journalisation des événements.

Les disques DESIIR et *backup* ont une capacité d'environ 1 Go (giga-octet) et le disque *debug* dispose d'environ 128 Mo (méga-octet).

## 1.2 Description du produit évalué

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

### 1.2.1 Catégorie du produit

1 - détection d'intrusion
2 - anti-virus, protection contre les codes malicieux
<b>3 – pare-feu</b>
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 identifiable par les éléments suivants :

Nom du produit	Dispositif d'échange sécurisé d'informations sans interconnexion réseau (DESIIR)
Version	1.0

### 1.2.3 Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- le transfert unidirectionnel bas vers haut ;

- le filtrage selon un format prédéfini ;
- la protection du format de filtrage prédéfini.

#### ***1.2.4 Configuration évaluée***

Le certificat porte sur la configuration dite « write only » disponible au moment de l'évaluation et référencée ci-dessus.

## 2 L'évaluation

### 2.1 Référentiels d'évaluation

L'évaluation a été menée conformément au référentiel « Certification de Sécurité de Premier Niveau en phase expérimentale ». Les références des documents se trouvent en annexe 2.

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

La charge de travail prévue lors de la demande de certification était conforme à la charge de travail préconisée dans [CSPN] pour un produit ne comportant pas de mécanismes cryptographiques, soit 25 hommes x jours. L'évaluation s'est déroulée au cours du mois de décembre 2009.

### 2.3 Travaux d'évaluation

Ce paragraphe apporte des compléments sur la cible de sécurité [ST] 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 [ST].

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

Les biens sensibles suivants sont identifiés dans la cible de sécurité.

D. MHAUTE	Données présentes sur la machine haute.
D. RESEAU_HAUT	Toutes les données et machines accessibles par rebond du côté de la machine haute.
D. CONFIG_FILTRAGE	Paramètres de configuration et de filtrage du dispositif.
D. TRANSFERT	Données mises à disposition de la machine haute par le dispositif DESIIR

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

Les menaces suivantes sont identifiées dans la cible de sécurité.

M. INTRUSION_BAS>HAUT	Tentative de prise de contrôle de la machine haute depuis la machine basse via le dispositif DESIIR.
M. TRANSFERT_DONNEES_ILLICITES_BAS>HAUT	Transfert de données non autorisées depuis la machine basse vers la machine haute.
M. MODIF_CONFIG_DESIIR	Modification de la configuration du dispositif via les seules interfaces accessibles du dispositif, à savoir le câble USB.
M. TRANSFERT_ILLICITE_HAUT>BAS	Transfert illicite de données depuis la machine haute vers la machine basse.

### 2.3.1.4 Fonctions de sécurité

Les fonctions de sécurité suivantes sont identifiées dans la cible de sécurité.

F. TRANSFERT_UNIDIR	Transfert unidirectionnel de données depuis la machine basse vers la machine haute et interdiction des transferts de données depuis la machine haute vers la machine basse. Cette fonction peut être assimilée à une diode.
F. FILTRAGE_FORMAT	Filtrage du format des données transférées (transferts de fichiers au format texte, ne comportant que des caractères ayant un code ASCII compris entre 0 et 127, avec une longueur de ligne limitée à un nombre maximum de caractères. Ces fichiers de type « texte » ont une taille limitée et une extension contrôlée.)
F. PROTECTION_CONFIG_FILTRAGE	Protection contre les tentatives de modification / altération de la configuration du dispositif via les seules interfaces accessibles du dispositif, à savoir le câble USB.

### 2.3.1.5 Hypothèses sur l'utilisation du produit

Les hypothèses suivantes sont identifiées dans la cible de sécurité.

Hypothèses	Descriptions
H. SEC_PHYSIQUE	Le dispositif DESIIR doit être utilisé dans un environnement considéré comme physiquement sûr (local à accès contrôlé, de même niveau de confiance que la zone haute) au niveau du produit et de la machine haute. Ainsi, le produit ne prend pas en compte de sécurité particulière au niveau de malveillances matérielles et/ou utilisant un accès physique au produit.
H. INIT	Le dispositif DESIIR est entièrement installé et configuré lors de sa fabrication, donc avant sa livraison. Les fonctions du produit sont figées et ne sont plus modifiables par la suite.

H. PRECAUTIONS_EMPLOI	Les utilisateurs respectent les précautions d'emploi définies dans la documentation utilisateur.
H. NON_COLLUSION	L'utilisateur de la machine haute est considéré de confiance. De ce fait, l'attaquant situé côté machine basse ne peut pas disposer de complice ayant accès à la machine haute.

### 2.3.1.6 Utilisateurs typiques

La cible de sécurité n'identifie que deux types d'utilisateurs :

- les utilisateurs du niveau bas ;
- les utilisateurs du niveau haut.

La notion d'administrateur DESIIR n'existe pas puisque le produit n'est pas configurable.

Cependant, deux autres types d'utilisateurs sont identifiés :

- l'administrateur des machines du niveau bas ;
- l'administrateur des machines du niveau haut.

Ces administrateurs ont la charge du paramétrage (voir paragraphe 2.3.2) des machines de leur niveau, afin qu'elles puissent fonctionner avec le dispositif DESIIR.

### 2.3.2 Installation du produit

Le produit DESIIR s'installe comme une clé de stockage USB.

#### 2.3.2.1 Plate-forme de test

Le produit DESIIR a été testé dans un environnement comportant une machine haute et une machine basse. Une machine est un PC sous Windows XP SP2 mis à jour et l'autre un PC sous Ubuntu 9.04.

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

Le produit DESIIR ne nécessite aucune installation de logiciel mais des paramétrages particuliers des environnements sont à effectuer.

La documentation utilisateur [MANUEL] détaille les étapes nécessaires au paragraphe « Installation d'un dispositif WriteOnly ».

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

Le produit DESIIR ne comporte pas d'option d'installation.

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

Le produit DESIIR s'installe conformément au manuel d'installation.

#### 2.3.2.5 Durée de l'installation

Le produit DESIIR s'installe en moins d'une demi-journée.

#### 2.3.2.6 Notes et remarques diverses

Sans objet.

### 2.3.3 Analyse de la conformité

#### 2.3.3.1 Analyse de la documentation

Les documents constituant le référentiel documentaire sont clairs et bien structurés.

La documentation utilisateur [MANUEL] du dispositif DESIIR « *WriteOnly* » est constituée des éléments suivants :

- présentation (description générale et cas d'usage) ;
- branchement et fonctionnement (installation, fonctionnement, filtrage sur les contenants et contenus) ;
- procédure d'utilisation (par les utilisateurs, par scripts et procédure de redémarrage) ;
- dépannage (messages d'erreurs systèmes, fichier de *debug*, procédures de dépannage).

Le document [MANUEL] contient également en annexe des scripts en langage Python fournissant des exemples d'utilisations automatisées.

#### 2.3.3.2 Revue du code source

Aucun code source n'est disponible pour le produit DESIIR. De plus, lors de sa fabrication, les fonctions du produit sont figées et ne sont plus modifiables par la suite (hypothèse H. INIT).

#### 2.3.3.3 Fonctions testées

Le tableau ci-dessous reprend les tests menés lors de l'évaluation ainsi que les verdicts associés (*Réussite*, *Échec* ou *Non Conclusif*).

Tests	Descriptions	Verdicts / Commentaires
<i>Test-transfert</i>	Vérification du transfert unidirectionnel	<i>Réussite</i>
<i>Test-filtrage-1</i>	Vérification du filtrage sur des fichiers de type texte	<i>Réussite</i>
<i>Test-filtrage-2</i>	Vérification du filtrage sur des fichiers de type texte avec des extensions non interdites	<i>Réussite</i>
<i>Test-filtrage-3</i>	Vérification du filtrage sur des fichiers avec les extensions explicitement interdites	<i>Réussite</i>
<i>Test-filtrage-4</i>	Vérification du filtrage sur des fichiers ayant le même nom mais suffixés différemment	<i>Réussite</i>
<i>Test-filtrage-5</i>	Vérification du filtrage sur des fichiers ayant de longues extensions	<i>Réussite</i>
<i>Test-restrictions-1</i>	Test des restrictions sur la création et modification de répertoires	<i>Réussite</i>
<i>Test-restrictions-2</i>	Premier test des restrictions sur le nombre maximal de fichiers pouvant être déposés	<i>Réussite</i>
<i>Test-restrictions-3</i>	Second test des restrictions sur le nombre maximal de fichiers pouvant être déposés	<i>Réussite</i>

<i>Test-restrictions-4</i>	Test des restrictions sur des fichiers dont les noms n'utilisent pas les caractères ASCII	<b>Echec</b> Le dispositif DESIIR ne filtre pas correctement les noms de fichiers composés de caractères compris entre les octets 0x80 et 0xFF (en valeur décimale, entre 128 et 255).
<i>Test-montage</i>	Un utilisateur bas va chercher à accéder aux disques <i>backup</i> et <i>debug</i>	<b>Réussite</b>
<i>Test-formatage</i>	Un utilisateur bas va chercher à formater les disques <i>backup</i> et <i>debug</i>	<b>Réussite</b>
<i>Test-full</i>	Test sur la capacité de stockage	<b>Réussite</b>
<i>Test-copie-backup</i>	Test sur le comportement implémenté suivant le répertoire du disque DESIIR	<b>Réussite</b>
<i>Test-backup</i>	Manipulation de la procédure <i>backup</i>	<b>Réussite</b>
<i>Test-eraseall</i>	Manipulation de la procédure <i>eraseall</i>	<b>Réussite</b>
<i>Test-debug-1</i>	Vérification de la protection de la configuration du dispositif	<b>Réussite</b>
<i>Test-debug-2</i>	Vérification des événements tracés par le dispositif	<b>Inconclusive</b> Les différentes actions menées ne sont pas toutes tracées (création de dossier à la racine par exemple)

#### 2.3.3.4 Fonctions non testées

Toutes les fonctions ont été testées.

#### 2.3.3.5 Synthèse des fonctions testées et non testées

Le produit DESIIR fonctionne comme un disque dur USB. Il permet un échange de flux entre deux réseaux différents :

##### - Réseau haut

L'écriture sur les disques DESIIR et *debug* est impossible, ainsi que la suppression (par exemple, la touche « Suppr » du clavier ne fonctionne pas). Un utilisateur haut peut seulement lire (et copier sur un disque local) les données des disques DESIIR et *debug*. Ce même utilisateur peut également écrire des données dans le disque *backup* (disque non accessible au réseau bas).

##### - Réseau bas

Seule une copie sur le disque DESIIR est possible ainsi que la suppression du fichier copié. Un utilisateur du réseau bas ne peut accéder aux disques *backup* et *debug* :

- sous Windows, ils sont vus comme non formatés ;
- sous Linux, ils sont détectés mais ne peuvent être montés.

La déconnexion puis la reconnexion du dispositif DESIIR lance une procédure de backup : les fichiers du disque DESIIR sont transférés sur le disque backup.

Un filtrage sur les fichiers déposés sur le dispositif est réalisé automatiquement. Le filtrage concerne les extensions, le contenu ainsi que les noms des fichiers déposés.

Pour finir, deux procédures sont aussi accessibles afin de piloter le dispositif DESIIR :

- la procédure « *eraseall* » qui est initiée en copiant un fichier portant le nom « *eraseall* » à la racine du « disque » DESIIR. Cela déclenche un effacement de toutes les données contenues sur tous les disques (données des trois disques, données de debug comprises). Cette fonctionnalité n'est disponible qu'à partir du côté *ReadWrite* (RW) ;
- la procédure « *backup* » qui est initiée en copiant un fichier portant le nom « *backup* » à la racine d'un des disques de « DESIIR » déclenche une copie des données présentes sur le « disque » DESIIR vers le disque de *backup*. Cette commande est accessible à la fois du côté *WriteOnly* (W) et du côté *ReadWrite* (RW).

Toutes les fonctions de sécurité du produit ont été testées.

Les tests ont cependant fait apparaître des incohérences mineures dans la documentation utilisateur.

### **2.3.3.6 Avis d'expert sur le produit**

Le dispositif DESIIR fonctionne comme une diode et il n'a pas été possible de faire transiter de l'information du réseau haut vers le réseau bas lors de l'évaluation. L'architecture interne de l'appareil renforce la conviction sur l'efficacité de cette fonctionnalité.

Il n'y a aucun moyen de modifier la configuration du dispositif DESIIR car celle-ci est figée en usine afin d'éviter les erreurs de configuration ou de modification éventuelles. La robustesse du produit est ainsi renforcée.

Les données pouvant circuler à travers le produit DESIIR doivent être formatées de façon particulière comme indiqué au paragraphe « Filtrage sur les contenants du dispositif *WriteOnly* » du manuel utilisateur [MANUEL]. En cas de non respect des règles de filtrage, le produit DESIIR est conçu pour ne signaler aucune erreur à l'utilisateur.

## **2.3.4 Analyse de la résistance des mécanismes et des fonctions**

### **2.3.4.1 Liste des fonctions testées et résistance**

Les fonctions testées sont celles citées au paragraphe 2.3.1.4.

### **2.3.4.2 Avis d'expert sur la résistance des mécanismes**

Les trois fonctions de sécurité du produit objet de l'évaluation (cf. paragraphe 2.3.1.4) s'avèrent robustes et n'ont pu être mises en défaut. L'architecture interne de l'appareil renforce la conviction sur le fait que ces fonctions sont efficaces et non contournables.

On notera que l'évaluateur n'a pas testé la présence éventuelle de canaux cachés.

## **2.3.5 Analyse des vulnérabilités (conception, implémentation...)**

### **2.3.5.1 Liste des vulnérabilités connues**

Aucune vulnérabilité publique n'est recensée sur cette version du produit DESIIR.

### **2.3.5.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert**

Les principales vulnérabilités potentielles concernent des attaques physiques, d'où l'importance de l'hypothèse H.SEC\_PHYSIQUE.

Le produit est sensible à une attaque par nom de fichier mal formé, qui peut entraîner un reformatage du disque DESIIR, et donc un effacement des fichiers présents. Toutefois, la fonction principale (diode) du produit n'est pas remise en cause.

### ***2.3.6 Analyse de la facilité d'emploi et préconisations***

#### **2.3.6.1 Cas où la sécurité est remise en cause**

Il n'a pas été identifié de cas où la sécurité est ambiguë (à part, éventuellement, l'inversion des câbles USB).

#### **2.3.6.2 Recommandations pour une utilisation sûre du produit**

Les fichiers transitant par DESIIR doivent respecter les formats de données décrits dans le manuel utilisateur [MANUEL]. En cas de non respect des règles de filtrage, aucune erreur n'est signalée à l'utilisateur.

L'hypothèse H.SEC\_PHYSIQUE doit être impérativement respectée.

Le produit DESIIR n'a pas pour vocation de s'assurer de l'innocuité des fichiers qu'il transfère. C'est aux processus côté « haut » de s'assurer de ce point.

#### **2.3.6.3 Avis d'expert sur la facilité d'emploi**

Le produit est simple d'emploi. Il ne nécessite aucune configuration. Il n'a pas été identifié de risque d'erreur dans l'utilisation.

### ***2.3.7 Accès aux développeurs***

L'évaluateur a pu contacter facilement les développeurs. Ils se sont montrés coopératifs et ont répondu clairement aux questions de l'évaluateur.

## **2.4 Analyse de la résistance des mécanismes cryptographiques**

Le produit évalué ne comporte pas de mécanismes cryptographiques.

## **3 La certification**

### **3.1 Conclusion**

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

Ce rapport de certification de sécurité de premier niveau atteste que le produit « Dispositif d'échange sécurisé d'informations sans interconnexion réseau (DESIIR), Version 1.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST].

### **3.2 Restrictions d'usage**

Dans le respect des hypothèses d'utilisation formulées par le développeur, aucune restriction d'usage n'est identifiée pour le produit Dispositif d'échange sécurisé d'informations sans interconnexion réseau (DESIIR).

## Annexe 1. Références documentaires du produit évalué

[ST]	Cible de sécurité CSPN – DESIIR <i>Référence</i> : CR-I2D-2009-049 indice 2 <i>Date</i> : 2 mars 2010
[MANUEL]	Documentation utilisateur DESIIR Dispositif « en écriture uniquement » (WriteOnly) Version DESIIR 1. 0 Documentation V1. 8. 6
[RTE]	Rapport Technique d'Évaluation Certification de Sécurité de Premier Niveau DESIIR EDF317-RTE-CSPN version 1.02 du 23/02/2010

## Annexe 2. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CSPN-CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI, disponible sur <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>
[CSPN]	<p>Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 2. 4, phase expérimentale, n° 915/SGDN/DCSSI/SDR/CCN du 25 avril 2008.</p> <p>Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1.4.</p> <p>Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1.3.</p> <p>Documents disponibles sur <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a></p>