EDF R&D
Département SINETICS

Cible de sécurité CSPN – DESIIR			
Auteurs :	Arnaud TARRAGO, Pascal SITBON, Pierre NGUYEN	***Visa :***	
Référence :	CR-I2D-2009-049 indice 2	***Date :***	2 mars 2010

0. OBJECTIF DU DOCUMENT

Ce document présente la cible de sécurité CSPN du dispositif DESIIR (Dispositif d'Echange Sécurisé d'Informations sans Interconnexion Réseau). Il respecte le formalisme et les rubriques classiques des cibles de sécurité CSPN.

1. IDENTIFICATION DU PRODUIT

Organisation éditrice	EDF R&D
Lien vers l'organisation	http://www.edf.fr
Nom commercial du produit	DESIIR
Numéro de la version évaluée	1.0
Catégorie de produit	Catégorie 6 « Firewall »

2. ARGUMENTAIRE (DESCRIPTION) DU PRODUIT

2.1. DESCRIPTION GENERALE DU PRODUIT

Le produit est un dispositif de filtrage permettant une interconnexion avec transfert unidirectionnel de données entre deux machines, une machine basse et une machine haute. Il permet le passage d'information de la machine basse vers la machine haute via un point de stockage relais, avec des restrictions sur le contenu des données échangées. La zone haute reste à l'initiative du traitement des informations transmises. **La zone haute correspond au niveau de confiance le plus élevé**. **La zone basse est potentiellement exposée à des malveillances**. Les rôles utilisateur de la machine basse et utilisateur de la machine haute sont distincts et un même utilisateur ne peut pas avoir accès aux deux machines.

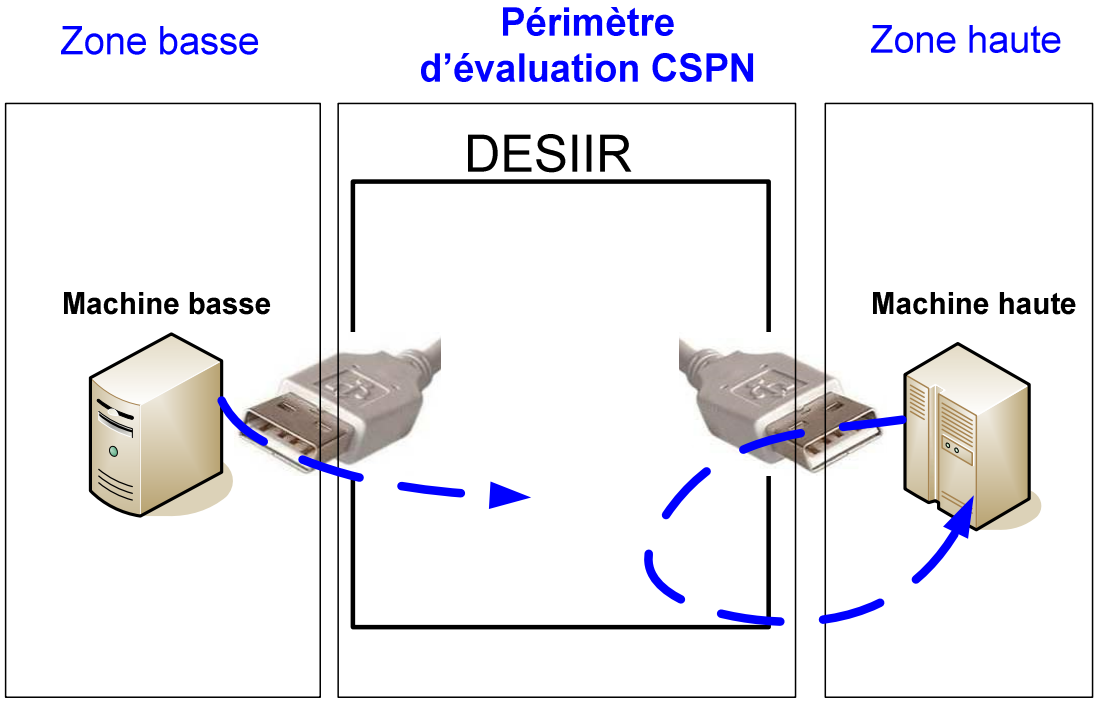

Figure 1. Fonctionnement général du produit et périmètre d'évaluation CSPN

2.2. DESCRIPTION DE LA MANIERE D'UTILISER LE PRODUIT

Le produit fonctionne comme un disque dur USB. L'utilisateur de la machine basse copie les fichiers à transmettre sur le produit de la même manière qu'il le ferait sur un disque dur directement attaché en USB. De même, l'utilisateur de la machine haute lit et efface les fichiers de la même manière qu'il le ferait sur un disque dur directement attaché en USB.

La figure 2 illustre le cas d'usage de la remontée d'informations en provenance de capteurs sans fil (zone basse) vers une salle de supervision (zone haute).

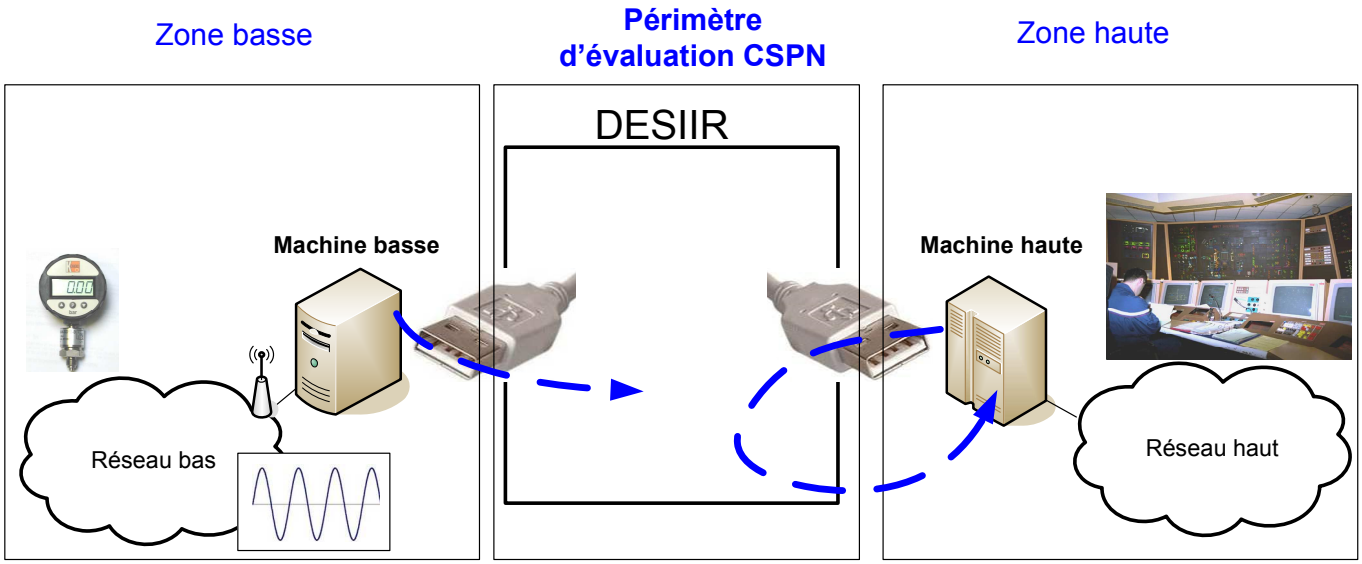

Figure 2. Cas d'usage du produit

2.3. DESCRIPTION DE L'ENVIRONNEMENT PREVU POUR SON UTILISATION

L'environnement est considéré comme physiquement sûr 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.

L'utilisation concerne uniquement des transferts de fichiers au format texte, ne comportant que des caractères d'un intervalle défini (caractères dont le code ASCII est compris entre 0 et 127), avec une longueur de ligne limitée à un nombre maximum de caractères. Ces fichiers, de type « texte », ont aussi une taille limitée et ne peuvent pas utiliser n'importe quelle extension. Le **contenu de ces fichiers n'est pas confidentiel**.

2.4. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Les attaques nécessitant un accès physique au produit ne sont pas prises en compte par hypothèse (cf. §2.3).

[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.

Les seules actions de l'administrateur sont le raccordement des interfaces USB et la mise sous tension du dispositif. Les deux rôles distincts existant sont donc le rôle utilisateur côté machine basse et le rôle utilisateur côté machine haute.

[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.

2.5. DESCRIPTION DES DEPENDANCES PAR RAPPORT A DES MATERIELS, DES LOGICIELS ET/OU DES MICROPROGRAMMES DU SYSTEME QUI NE SONT PAS FOURNIS AVEC LE PRODUIT

Pas de dépendance particulière, les systèmes validés sont spécifiés dans la documentation utilisateur, *a minima* Windows XP SP3 et Linux noyau 2.6 à partir du 2.6.31.

2.6. DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNES (UTILISATEURS FINAUX, ADMINISTRATEURS, EXPERTS…) ET DE LEUR ROLE PARTICULIER DANS L'UTILISATION DU PRODUIT

Lors de la fabrication, les fonctions du produit sont figées et ne sont plus modifiables par la suite. Les deux rôles existants sont donc les rôles utilisateur côté machine basse et utilisateur côté machine haute.

2.7. DEFINITION DU PERIMETRE DE L'EVALUATION, A SAVOIR LES CARACTERISTIQUES DE SECURITE DU PRODUIT CONCERNEES PAR L'EVALUATION

Le périmètre de l'évaluation couvre la totalité du dispositif DESIIR, considéré en « boîte noire » sous l'angle de ses deux interfaces USB, une côté machine basse et une côté machine haute (cf. Figure 1).

L'objectif principal de sécurité du dispositif DESIIR consiste à protéger l'accès à la machine haute depuis la machine basse, tout en offrant une interconnexion entre ces deux machines, limitée à un transfert de données unidirectionnel depuis la machine basse vers la machine haute, avec un filtrage restrictif sur le format des données transférées.

3. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DANS LEQUEL LE PRODUIT DOIT FONCTIONNER

3.1. MATERIEL COMPATIBLE OU DEDIE

Présence d'un contrôleur USB disponible sur les machines basse et haute.

3.2. SYSTEME D'EXPLOITATION COMPATIBLE : TYPE, VERSION, CORRECTIFS…

Windows XP SP3 ou Linux noyau 2.6 à partir du 2.6.31 gérant l'USB Mass Storage.

4. DESCRIPTION DES BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER

Le produit est conçu pour protéger les biens sensibles suivants :

- **[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

On considère (cf. §2.2.1) que les données en provenance de la machine basse ne sont pas des biens sensibles.

5. DESCRIPTION DES MENACES

L'agent menaçant est tout utilisateur pouvant se connecter sur la machine basse ou à la place de la machine basse.

Les menaces contre lesquelles protège le dispositif DESIIR sont les suivantes :

- **[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 (cf. §6, F.FILTRAGE_FORMAT) 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

6. DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT

Les fonctions de sécurité du produit sont les suivantes :

- **[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 caractéristique.)
- **[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.