



MINISTÈRE DES ARMÉES

## **ANNEXE 4 du CCTP PRECONISATIONS TECHNIQUES V2.1**

### **Acheteur public**

ETAT – MINISTÈRE DES ARMÉES  
Service d'Infrastructure de la Défense (SID) Nord-Est

### **Objet du marché**

**N° DAF : 2024\_001370**

**Maintenance et le déploiement du système de télé relève des compteurs  
d'énergies et fluides au profit des sites dépendant du SID Nord-Est**

# FICHE


## PRECONISATIONS TECHNIQUES :

### COMMUNICATION ENTRE LE SYSTEME DE TELERELEVE ET L'APPLICATION INFORMATIQUE DU SYSTEME OSF DEFENSE

	Grade/Nom	Fonction	Téléphone	Date	Version
Rédaction :	IEF DJOUA	Chef de projet SIC	0137076697	21/11/2011	V1.0
Vérification :	IEF BERNARD	Chef de projet fonctionnel	0139076684	01/12/2011	V1.0
Approbation :	CBA ALLAIRE	Directeur de projet	0139076624	15/12/2011	V1.1


## Historique des modifications

Version	Date	Description et justification de la modification	Rédaction (Nom et fonction)	Validation (Nom et fonction)
1.2	06/01/2012	Modification : (§4.2 et §4.3)	Mme VILBERT Chef de projet STERIA	IEF DJOUA Chef de projet SIC
1.3	22/03/2012	Modifications de toutes les parties et ajout de l'annexe	CBA ALLAIRE Directeur de projet	CBA ALLAIRE Directeur de projet
1.4	25/04/2012	Ajout du chapitre 5 : Réception et traitement des accusé-réception par le fédérateur. Modification de la règle de nommage.	IEF DJOUA Chef de projet SIC	M. Juan MONTILLA Ingénieur d'études STERIA
1.5	22/04/2013	Ajout du §4.4: Autres caractéristiques des fichiers. Suppression de la décomposition du code Immeuble G2D dans le chapitre 3.	IEF DJOUA Chef de projet SIC	IC2 ALLAIRE Directeur de projet
1.6	16/07/2013	Modification de la page 14 : « sensibles non classifiées de défense ne portant pas la mention DR » et précision des références. Modification du § 1.2.	IEF DJOUA Chef de projet SIC IC2 ALLAIRE Directeur de projet	IC2 ALLAIRE Directeur de projet
1.7	17/04/2014	Modification du § 4.4 « Niveau de protection des informations » Modification du § 6.1 « Exigence concernant la sécurisation du fédérateur ». Modifications des §1.1 et §1.2	IEF DJOUA Chef de projet SIC IC2 ALLAIRE Directeur de projet	IC2 ALLAIRE Directeur de projet
1.8	03/06/2014	Modification du §6.1 (prescriptions complémentaires concernant le firewall) demandée par la DC DIRSI	IC2 ALLAIRE Directeur de projet	IC2 ALLAIRE Directeur de projet
1.9	14/10/2014	Ajout du §4.5: nécessité de la prise en compte de la menace tempest pour les équipements situés à proximité de bâtiments confidentiels ou de systèmes classifiés. Ajout du §6.1 : exemples de firewall qualifiés par l'ANSSI et recommandés par le MINDEF.	IEF DJOUA Chef de projet SIC	
1.10	31/03/2015	Renforcement de la protection des équipements de télérelève Ajout du §4.4: Format des courriers électroniques.	IEF DJOUA Chef de projet SIC	IEF JEAN-JOSEPH IMI GODBILLOT IC2 PRIGOT
1.11	06/07/2015	Paragraphe 6.1 : Protection physique du fédérateur Firewall de type Stormshield. Traçabilité des connexions IDS sur le fédérateur	IEF DJOUA Chef de projet SIC	IC2 PRIGOT
1.12	02/10/2020	Paragraphe Introduction de la page 4. Harmonisation des polices page 8 et 14. Ajout liste des erreurs 01 à 12 à la page 16. Modification du paragraphe comportant la gestion des erreurs de la page 16.	TSEF Demay Chargé de projet	IDEF DJOUA Chef de projet SIC
2.1	18/12/2020	Ajout du point 6.3. Exigence concernant les émetteurs	APPR SUDRE Assistant chef de projet SIC	IDEF DJOUA Chef de projet SIC

	<div>Fiche</div> <div>Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense</div>	<div>Version : 2.1 Date : 18/12/2020</div> <div>Page 4/25</div>
---	--	---

## Sommaire

<b>Introduction .....</b>	<b>5</b>
<b>1. L'architecture de télérelevage et impact sur la transmission d'informations.....</b>	<b>6</b>
1.1. Description de l'architecture du système OSF .....	6
1.2. Transmission de l'information .....	7
<b>2. Caractéristiques techniques du fédérateur .....</b>	<b>8</b>
2.1. Récupération des informations après une interruption de communication .....	8
2.2. Redondance .....	9
2.3. Identification des utilisateurs.....	9
2.4. Surveillance système .....	9
<b>3. Le nommage des composants du dispositif de télérelève .....</b>	<b>9</b>
<b>4. Les informations à transmettre à l'OSF .....</b>	<b>10</b>
4.1. Le fichier de codes .....	11
<i>Objectif du fichier de codes : .....</i>	<i>11</i>
<i>Principe de fonctionnement du dispositif de clés : .....</i>	<i>11</i>
4.2. Le fichier de données de consommation .....	12
<i>Contenu du fichier : .....</i>	<i>12</i>
<i>Nommage du fichier : .....</i>	<i>12</i>
4.3. Fichier de données d'alertes .....	12
<i>Contenu du fichier : .....</i>	<i>12</i>
<i>Liste des alertes : .....</i>	<i>12</i>
<i>Nommage du fichier : .....</i>	<i>13</i>
4.4. Format des courriers électroniques.....	13
4.5. Autres caractéristiques des fichiers .....	14
<i>Nommage des fichiers : .....</i>	<i>14</i>
<i>Format des fichiers : .....</i>	<i>14</i>
<i>Contenu des fichiers : .....</i>	<i>15</i>
<i>Changement d'heure : .....</i>	<i>15</i>
<i>Niveau de protection des informations : .....</i>	<i>15</i>
<b>5. Réception et traitement des accusé-réception par le fédérateur .....</b>	<b>16</b>
<i>Cas d'un défaut d'acheminement du message vers SISMELE .....</i>	<i>16</i>
<i>Cas d'une erreur dans le fichier de consommation ou d'alertes .....</i>	<i>17</i>
<i>Sécurité : .....</i>	<i>19</i>
<b>6. Exigences de sécurité.....</b>	<b>19</b>
6.1. Exigences concernant la sécurisation du fédérateur .....	19
6.2. Exigences concernant l'accès à une application installée sur le fédérateur.....	22
<i>Identification et authentification.....</i>	<i>22</i>
<i>Mots de passe. ....</i>	<i>22</i>
<i>Ecran de veille.....</i>	<i>22</i>
<i>Profils. ....</i>	<i>22</i>
6.3. Exigence concernant les émetteurs.....	23
<i>Risque de perturbations électromagnétiques et radioélectriques occasionnées.....</i>	<i>23</i>
6.4. Exigence concernant les agents extérieurs .....	23
<i>Maîtrise des accès physiques.....</i>	<i>24</i>
<i>Habilitations. ....</i>	<i>24</i>
<b>ANNEXE : tableau de synthèse des pas et des unités de mesure à paramétrer dans le système de télérelève .....</b>	<b>25</b>

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 5/25

## Introduction

OSF DEFENSE (Outils de Suivi des Fluides) est un système d'information de gestion des fluides pour assurer, à chaque échelon organisationnel (central et local), la gestion des consommations en eau et en énergie dans ses sites immobiliers.

Le fonctionnement de cet outil repose sur l'analyse des mesures de la consommation réelle collectées à partir d'un dispositif de relève à distance (télérelève) des compteurs. Le système OSF est un système de *reporting* (consultation) et non de *monitoring* (commande et contrôle).

Ce document présente les spécifications techniques à suivre pour permettre la communication entre l'infrastructure de télérelève locale et l'application informatique OSF centralisée.


Ces prescriptions traitent du fonctionnement de l'équipement terminal de télérelève, appelé *fédérateur*, assurant la collecte et le transfert de l'ensemble des données de consommations issues des compteurs vers l'OSF.

Ce document abordera les points suivants :

- l'architecture de principe retenue pour l'installation du réseau de communication (Télérelève/OSF) et son impact sur la transmission par le fédérateur des informations à l'OSF ;
- les fonctionnalités techniques du fédérateur attendues pour communiquer avec l'OSF ;
- les règles de nommage des composants du dispositif de comptage par télérelève ;
- le type et le formatage des informations à transmettre ;
- la sécurité de la transmission et la protection du fédérateur.

Les prescriptions de ce document devront être intégrées en substance dans la définition des projets d'installation d'infrastructure de comptage en cours ou en devenir. Elles devront aussi être appliquées dans les systèmes de comptage existants pour permettre une compatibilité totale avec l'OSF.

Ce document s'adresse aux organismes du SID et n'a pas vocation à fournir les descriptions techniques des équipements de télérelève ou de comptage.

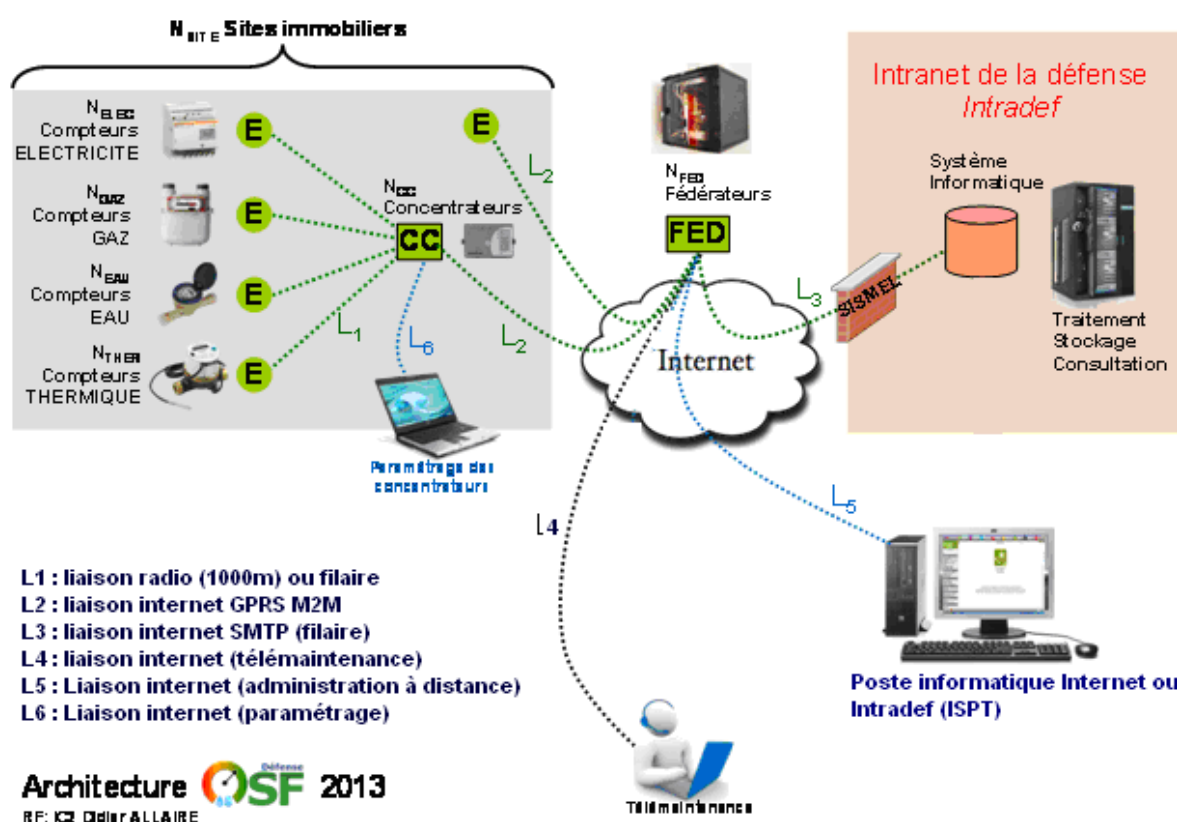
 <p>SID SERVICE D'INFRASTRUCTURE DE LA DÉFENSE</p>	<p>Fiche</p> <p>Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense</p>	<p>Version : 2.1 Date : 18/12/2020</p> <p>Page 6/25</p>
---	--	---

## 1. L'architecture de télérelève et impact sur la transmission d'informations

### 1.1. Description de l'architecture du système OSF


Le système OSF repose sur un dispositif automatique de relève à distance des données de consommation réelle des points de comptage physique (PC).

Le schéma de principe suivant présente l'architecture du système de télérelève en précisant les liaisons :



Il s'agit d'une infrastructure de télérelève fonctionnant sur des réseaux de communication hors Intradef comme Internet et dont l'architecture se compose de trois composants élémentaires :

- Les **émetteurs (E) (ou modules émetteurs)** connectés aux PC (compteur, jauge, intégrateur, capteur...) qui collecte des signaux d'impulsion (index) ou des données physiques (puissance, intensité...) pour les transmettre (liaison L<sub>1</sub> ou L<sub>2</sub>) à des concentrateurs ou directement à des fédérateurs ;
- Le **concentrateur (CC)** qui correspond à un équipement physique intermédiaire paramétrable (similaire à un automate) recevant et traitant directement les trames d'informations des émetteurs pour les retransmettre (liaison L<sub>2</sub>) au fédérateur ;
- Le **fédérateur (FED)** qui correspond à un concentrateur évolué terminal équipé d'une application informatique capable de formater les données en fichiers type csv et de les

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 7/25

envoyer par messagerie Internet vers l'Intradef via la passerelle SISMEL (liaison L<sub>3</sub>) afin d'être exploitée par une application informatique centralisée hébergée sur Intradef.

L'emploi des répéteurs (équipements intermédiaires relayant la transmission radioélectrique) est interdit.

Le protocole non propriétaire de communication radioélectrique du système (L<sub>1</sub>) est le Wireless M-bus BF 169 MHz répondant à la norme européenne NF EN 13757-4:2011. Les canaux de la bande de fréquence 169 Mhz sont ceux autorisées par la décision de la commission de l'Union européenne 2005/928/CE.

La communication bidirectionnelle est autorisée uniquement dans le cadre d'une synchronisation de l'émission pour l'horodatage des données et éviter toute dérive temporelle. Le mode réception des modules émetteurs ne doit pas, dans ce cas, remettre en question la sécurité du système (SSI) en donnant la possibilité de modifier à distance la fonction première des modules. Le paramétrage à distance se limitera à la synchronisation de l'horodatage, la périodicité des communications, l'enregistrement des données et l'actualisation du firmware. La possibilité d'actualiser les *firmware* pourra être immédiatement interdite à distance et réactivée uniquement après une action physique sur chaque émetteur.

L'ouverture, pour chaque fédérateur, d'un accès physique et logique à Internet est une prestation de service assurée par la DIRISI (marché unique ministériel de fourniture d'accès à Internet).

## 1.2. *Transmission de l'information*

Il existe deux types de données à produire :


- les données de consommation horodatées (et non pas des index de consommation) qui fournissent une information sur la quantité de fluide consommée pendant un temps donné ;
- les données d'alertes qui fournissent une information sur l'état fonctionnel des équipements (compteurs, concentrateurs et fédérateur).

Les fichiers seront envoyés par le fédérateur via le réseau Internet à partir d'un compte de messagerie fourni par la DIRISI. Le rapatriement des fichiers dans le réseau Intradef s'effectuera en utilisant la passerelle ministérielle SISMEL (pare-feu Intradef/Internet). L'utilisation du réseau Internet et de la passerelle SISMEL impose de choisir un format de fichier *csv*.

Le fédérateur formate les données sous la forme de deux fichiers *csv* distincts :

- un fichier de consommation (données horodatées) ;
- un fichier d'alertes (état des équipements).

Ces fichiers sont envoyés périodiquement (fréquence paramétrable) sous la forme de pièces jointes, par messagerie Internet, à une adresse technique unique dans l'environnement Intradef. ([gtp.osf.tec@intradef.gouv.fr](mailto:gtp.osf.tec@intradef.gouv.fr))

 <p>SID SERVICE D'INFRASTRUCTURE DE LA DÉFENSE</p>	<p>Fiche</p> <p>Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense</p>	<p>Version : 2.1 Date : 18/12/2020</p> <p>Page 8/25</p>
---	--	---

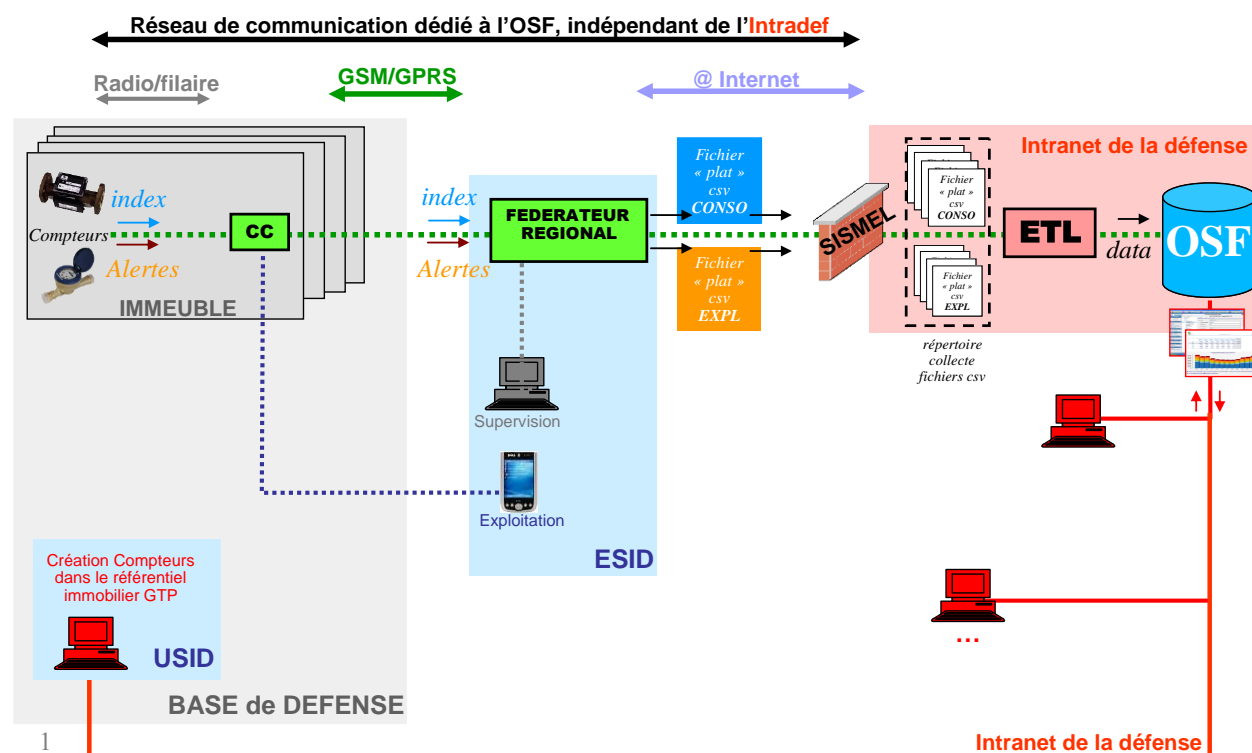
Le logiciel OSF extrait les fichiers de données stockés dans un répertoire dédié existant sur Intradef.

La figure suivante présente le schéma général du système:

ESID : établissement du SID (entité régionale)

USID : unité de soutien de l'infrastructure de la défense (entité de proximité)

ETL : *Extract – Transform - Load*




Dans le cadre d'une télémaintenance, le fédérateur communiquera avec le serveur tiers de maintenance via une connexion sécurisée (§6.1). Par ailleurs, l'ouverture de la connexion entre le fédérateur et le serveur de maintenance sera soumise à une autorisation du SID.

## 2. Caractéristiques techniques du fédérateur

### 2.1. *Récupération des informations après une interruption de communication*

Les données relevées ne doivent pas se perdre. Le fédérateur doit donc pouvoir mémoriser et envoyer en temps différé les fichiers en cas d'anomalie ou de rupture temporaire du réseau. Le système devra intégrer un moyen de conservation des données émises et disposer d'une fonctionnalité de renvoi des mails afin de réduire l'indisponibilité des données. Pour ce faire, une conservation chronologique des informations dans un système de gestion de base de

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 9/25

données (mysql,...) peut être prévue conjointement à une conservation chronologique dans des fichiers déclarés dans une unité de stockage (disque dur, ....)

## 2.2. Redondance

Chaque fédérateur doit intégrer une architecture redondante afin de pallier une panne matérielle (disque ou autre) qui entraînerait une perte de données potentielle.

Les données doivent être automatiquement archivées sur un support physique informatique d'une **capacité minimale de 6 mois d'enregistrement** avant écrasement par des valeurs plus récentes pour ce qui concerne leur émission vers l'application centrale de l'OSF.

## 2.3. Identification des utilisateurs

Si le fédérateur propose des interfaces utilisateurs, celles-ci doivent être sécurisées par mot de passe fort. Tous les identifiants de connexion seront nominatifs.

## 2.4. Surveillance système

Le fédérateur transmet à l'OSF des informations sur l'état des équipements du système dans le cadre de l'analyse des consommations afin de pouvoir distinguer les données de consommation aberrantes des anomalies de télérelève. Ces informations doivent permettre de publier des statistiques de disponibilité du système ou d'initier des actions de maintenance.

## 3. Le nommage des composants du dispositif de télérelève


Chaque point de comptage est identifié **de manière unique et définitive** à partir d'un code (*identifiant*) composé des éléments suivants :

- un identifiant d'immeuble G2D (9 chiffres+ 1 lettre) ;
- un code composant (4 chiffres) ;
- un code niveau (1 lettre + 2 chiffres) ;
- un code local (5 chiffres) ;
- un type de compteur (trigramme) ;
- un numéro de compteur (2 chiffres).

Immeuble G2D	Composant	Niveau		Local	Type de compteur	N°compteur
Code G2D de l'immeuble	4 chiffres	1 lettre	2 chiffres	5 chiffres	3 alphanumériques	2 chiffres
9 chiffres + 1 lettre	0000..9999	S ou E	00..99	00000..99999	trigramme	01..99
370261003V	0007	E	00	00010	CEL	01
490007003X	0001	S	01	00001	CGZ	01
...	...	...	...	...	...	...

Le code niveau est constitué d'une lettre (S ou E) et de 2 chiffres.

« S » =sous-sol et « E » = étage.

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 10/25

Exemple : S01 (sous-sol niveau -1)  
E02 (local 2<sup>ème</sup> étage)

Le tableau suivant établit la liste des trigrammes associés aux différents points de comptage physique :

Composants	Domaine	Abréviation (éléments REELS)
Compteurs	électricité	CEL
Compteurs	gaz	CGZ
Compteurs	thermique	CTH
Compteurs	fioul	CFL
Compteurs	eau froide	CEA
Compteurs	eau technique	CET
Compteurs	eau ECS	CEC
Sonde	T°C chauff/refroid	STH
Sonde	T°C extérieur	STX
Sonde	T°C ECS	STE
Capteur	intensité	SEL
Capteur	occupation du local	SOC
jauge	fioul	SFL
jauge	gaz	SGZ
jauge	eau	SEA
concentrateur	filaire/radio	CON
fédérateur	filaire/radio	FED
répéteur	onde radio	REP
		code couleur destiné à la supervision locale (présence éventuelle d'IHM)

#### Particularités

Pour identifier un point de comptage situé à l'extérieur d'un composant, mettre E00 dans la rubrique « Niveau » et 00000 dans la rubrique « Local »

Exemple : 490007003X0001E0000000CGZ01

Pour identifier un point de comptage non attaché à un composant, mettre 0000 dans Code Composant, mettre E00 dans la rubrique « Niveau », 00000 dans la rubrique « Local »

Exemple : 490007003X0000E0000000CGZ01


## 4. Les informations à transmettre à l'OSF

Le fédérateur transmettra à l'OSF trois types de fichier :

- Un « fichier de codes » assurant le niveau de sécurité de la communication.
- Un « fichier de données » de consommation ;
- Un « fichier de données » d'alertes.

Les trois fichiers seront au format csv.

Les deux fichiers de données sont envoyés à un rythme minimal de **deux fois par jour** qui doit être paramétrable.

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 11/25

## 4.1. *Le fichier de codes*

### **Objectif du fichier de codes :**

L'application informatique OSF doit pouvoir identifier le nom du fichier envoyé par tout fédérateur pour vérifier la validité de la source pour des raisons de sécurité informatique.

Un dispositif de clés, sous la forme de codes, doit être mis en place entre le fédérateur et l'OSF pour garantir l'intégrité des données transmises par le fédérateur à l'OSF.

Le fichier de codes permet de réaliser l'échange des clés entre le fédérateur et l'OSF.

### **Principe de fonctionnement du dispositif de clés :**

Avant l'envoi du premier fichier de données, le fédérateur doit générer une suite de 1000 codes de 4 caractères dans un fichier au format *csv* (un code par ligne) et le transmettre à l'OSF.

Ces codes ou clés sont une suite aléatoire de chaînes de 4 caractères alphanumériques pris dans l'ensemble {[A-Z][0-9]}.

Ces clés participeront au nommage des fichiers de données de consommations et d'alertes.

Chaque code sera associé au nommage d'un fichier de données. La liste des codes sera classée de manière chronologique selon l'ordre d'envoi des fichiers de données :

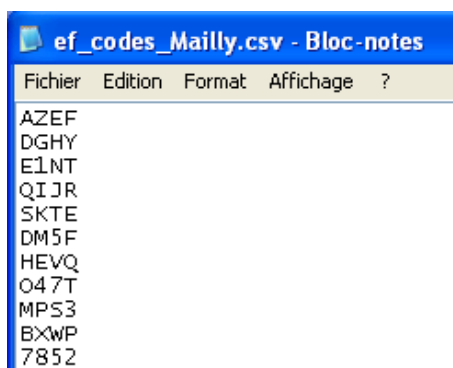
- Le 1<sup>er</sup> code du fichier code sera utilisé pour le nommage du 1<sup>er</sup> fichier de données ;
- Le 2<sup>ème</sup> code servira au nommage du 2<sup>ème</sup> fichier de données ;
- Le N<sup>ème</sup> code pour le N<sup>ème</sup> fichier ;


Le fichier « code » sera nommé **ef\_codes\_NomSite.csv**.

« NomSite » est le nom donné au site (exemple : Mailly).

Dès que tous les 1000 codes du fichier sont utilisés, le fédérateur génère immédiatement une autre suite de codes et l'intègre dans un nouveau fichier de même nom. Ce fichier est aussitôt envoyé à l'OSF afin d'éviter les rejets de fichiers de données au prochain envoi (délais de 12h00). L'opération doit s'exécuter en moins de 10 minutes.

Exemple :



	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 12/25

## 4.2. *Le fichier de données de consommation*

### Contenu du fichier :

Chaque ligne de ce fichier est constituée des données suivantes :

- L'identification du point de comptage : *identifiant* (Cf. §3);
- La date de début de consommation : <jj>/<mm>/<aaaa> ;
- La durée de la consommation : « 10 minutes », « heure », « jour », « mois », « année » ;
- La valeur de la consommation : réel ; il s'agit de la valeur réelle de consommation (différence entre deux index) ;
- [Rubrique facultative] l'équivalent kilowatts : réel ;
- [Rubrique facultative] l'équivalent euros : réel ;

### Nommage du fichier :

Ce fichier sera nommé :

**ef\_consommations\_NomSite\_<aaaa>-<mm>-<jj>\_<[« AAAA ».. « ZZZZ »]> .csv**

Avec :

<aaaa>, <mm>, <jj> : l'année, mois et jour de la date courante

<[« AAAA ».. « ZZZZ »]> : le prochain code à 4 caractères non utilisé dans le fichier **ef\_codes\_NomSite.csv**

Exemple : ef\_consommations\_Mailly\_2011-11-08\_BDA1.csv

```
id_cp;bd;p;val;eq_kwh;eq_eu
370261003V0007E0100006CEL01;01/05/2011 00:00;10 minutes;100;;
370261003V0007E0100006CEL01;01/06/2011 00:00;heure;665;;
370261003V0007E0100006CEL01;01/07/2011 00:00;jour;6321;;
370261003V0007E0100006CEL01;01/08/2011 00:00;mois;311;;
370261003V0007E0100006CEL01;01/09/2011 00:00;année;3644;;
```

## 4.3. *Fichier de données d'alertes*

### Contenu du fichier :


Les données de ce fichier sont :

- L'identification du point de comptage : *identifiant* (Cf. §3);
- La date à laquelle l'alerte a été générée : <jj>/<mm>/<aaaa> <hh>:<MM>;
- Le type d'alerte : « COMCO » ou « COMPC » ;
- La description de l'alerte : texte libre (200 caractères maximum) ;

### Liste des alertes :

« COMPC » lorsque l'équipement concerné est un compteur.

« COMCO » lorsque l'équipement concerné est un concentrateur ou un fédérateur ;

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 13/25

### Exemples de descriptions d'alertes liées au point de comptage ou au concentrateur :

Type d'alerte	Texte libre (exemple)
COMPC	Connexion au point de comptage impossible
COMPC	Batterie faible_Emetteur
COMCO	Connexion au concentrateur impossible
COMCO	Batterie faible_Fédérateur
COMCO	Batterie faible_Concentrateur
COMCO	Défaut récepteur_Concentrateur
COMCO	Défaut récepteur_Fédérateur
COMCO	Défaut liaison_Téléphonie
COMCO	Défaut émission vers l'OSF
COMCO	Dérangement Présence tension

### Nommage du fichier :

Ce fichier sera nommé :

**ef\_systemalerts\_\_NomSite\_<aaaa>-<mm>-<jj>-<[« AAAA ».. « ZZZZ »] >.csv**

Exemple : ef\_systemalerts\_Mailly\_2011-11-08\_BDA1.csv

```
id_eqpt;alert_date;alert_type;alert_desc
370261003V0007E0100006CEL01;01/05/2011 00:00;COMPC;Connexion au point de comptage impossible
370261003V0007E0100006CEL01;02/05/2011 00:00;COMCO;Connexion au concentrateur impossible
```


## 4.4. Format des courriers électroniques

Les courriels par la PFE via la passerelle SISMEL doivent respecter une certaine structure. Les courriels envoyés par les différents sites, doivent respecter la RFC 2822 sur le format des messages texte ainsi que ses extensions sur le format MIME (RFC 2045 à 2049).

Celles-ci sont disponibles en anglais aux adresses suivantes :

- <https://www.ietf.org/rfc/rfc2822.txt>
- <https://www.ietf.org/rfc/rfc2045.txt>
- <https://www.ietf.org/rfc/rfc2046.txt>
- <https://www.ietf.org/rfc/rfc2047.txt>
- <https://www.ietf.org/rfc/rfc2048.txt>
- <https://www.ietf.org/rfc/rfc2049.txt>

Voici un exemple de la structure d'un courriel attendu :

	<div>Fiche</div> <div>Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense</div>	<div>Version : 2.1 Date : 18/12/2020</div> <div>Page 14/25</div>
---	--	--

```

ID: MDCSIDCW06hm8Ua8d9E0000038f@mdcsid.servinfra.def
FROM: aaaa.bbbb@intradef.gouv.fr
TO: aaaa.bbbb@intradef.gouv.fr;cccc.dddd@intradef.gouv.fr
CC:
SUBJECT: Rapport EXPL de MAILLY-LE-CAMP
SendDate: 20/03/2015
SendHour: 13:01:42
MIME-Version: 1.0
AttachmentFiles: ef_systemalerts_Mailly_2015-03-20_87X8.csv
Content-Type: multipart/mixed; boundary="boundary"

Content:
--boundary
Content-Type: text/plain

>Report journalier des alarmes présentes sur le site de MAILLY LE CAMP

--boundary
Content-Type: application/octet-stream; name="ef_systemalerts_Mailly_2015-03-20_87X8.csv"
Content-Disposition: attachment; filename="ef_systemalerts_Mailly_2015-03-20_87X8";
Content-Transfer-Encoding: base64

Contenu de la pièce jointe

--boundary--

```

Les textes surlignés en vert sont les variables.

## 4.5. Autres caractéristiques des fichiers

### Nommage des fichiers :

Le champ « NomSite » dans les noms des fichiers ne peut pas contenir les caractères suivants :


- Des caractères accentués (à, é, î ...),
- Des espaces,
- Le caractère « \_ ».

### Format des fichiers :

Les fichiers envoyés à SISMELE sont des fichiers CSV encodés comme suit :

Encodage	UTF8
Saut de ligne	Caractère LF (0x0A)

- Les enregistrements sont de longueur variable, chaque champ est séparé du suivant par le caractère « ; » (code 0x3B). Un champ vide est représenté par 2 séparateurs accolés,
- Chaque enregistrement se termine par le caractère de fin de ligne : <champ1> ;<champ2> ;... ;<champN><LF> ,
- Si le caractère « ; » est utilisé dans un champ texte, il doit être remplacé par la chaîne « % % » ,

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 15/25

- Les champs texte ne doivent pas contenir de caractères d'échappement (notamment pas de saut de ligne),
- Pour les valeurs numériques, le caractère décimal est le point, il n'y a pas de séparateur des milliers,
- La 1ère ligne contient les noms des colonnes et suit le même format que les lignes de données (séparateur « ; » entre chaque nom de colonne),
- Un fichier sans donnée contient uniquement la ligne d'entête et aucune ligne de données.

### **Contenu des fichiers :**

Les fichiers de consommation ne doivent jamais être vides ou contenir des lignes en doublon. A l'inverse d'un fichier de consommation, un fichier de données d'alertes peut être vide ; dans ce cas, il ne doit pas être transmis à l'OSF, aucun équipement concerné par la télérelève ne présentant de défaut.

### **Changement d'heure :**


Les changements d'heure (passage à l'heure d'été ou d'hiver) doivent être répercutés sur l'ensemble des équipements participant au télérelevage. Dans tous les cas, les heures figurant dans les fichiers de consommation (heures locales) doivent être valides.

### **Niveau de protection des informations :**

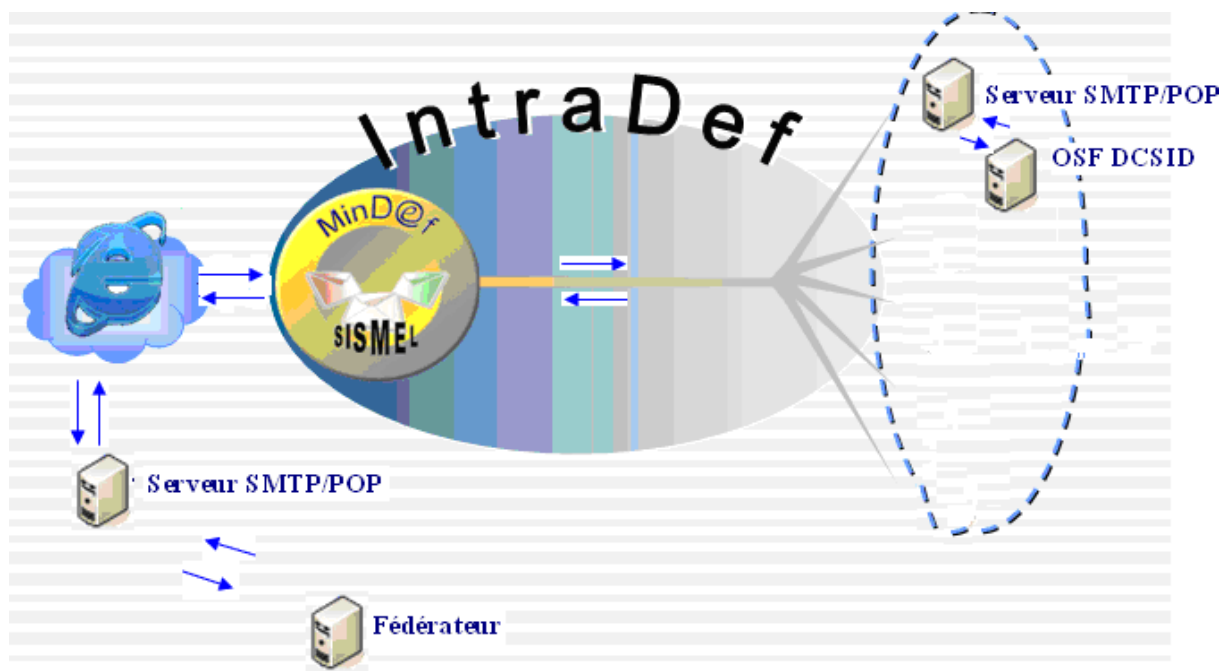
**Les données de consommation collectées par télérelève sont considérées comme des données non sensibles n'ayant pas vocation à être diffusées dans le domaine public.** Ces données vont permettre de connaître la consommation des installations, des équipements et des bâtiments qui sont liées ou non à une activité classifiée sans pour autant révéler une information classifiée. Ce périmètre correspond à la quasi-totalité du parc immobilier de la défense. Des précautions particulières doivent être prises lors de l'installation d'équipements de télérelève (compteurs, concentrateurs, ...) à proximité des bâtiments classés « confidentiels » ou de systèmes d'information classifiés. Des consignes relatives à la prise en compte de la menace tempest, indiquées dans le dossier de sécurité du site, doivent être respectées.

L'infrastructure de télérelève est organisée pour permettre la collecte, le stockage, le traitement sommaire et la transmission d'informations non sensibles. En aucun cas, ce dispositif ne peut recevoir des données portant la mention diffusion restreinte (DR) au sens de l'IGI 1300. Aucune information sensible classifiée (ISC) ne doit transiter ou être stockée dans le système OSF.

**L'acheminement peut s'effectuer par Internet sous réserve d'appliquer les mesures adaptées :** leur confidentialité, leur disponibilité et leur intégrité ne procèdent pas du secret de la défense nationale tel que défini par les articles L413-9 à L413-12 du code pénal et le décret 98-608, mais des dispositions spécifiques prévues dans la loi, notamment l'atteinte au secret professionnel (Code pénal L226-13 à L226-14), les atteintes aux droits de la personne résultant des fichiers et des traitements informatiques (Code pénal L226-16 à L226-24), et d'autres obligations légales ou contractuelles.

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 16/25

## 5. Réception et traitement des accusé-réception par le fédérateur



Le fédérateur de chaque site doit avoir un compte de messagerie afin de recevoir et de permettre le traitement des accusé-réception émis par l'OSF.

### **Cas d'un défaut d'acheminement du message vers SISMEL :**


Le fédérateur doit être configuré de manière à utiliser un serveur SMTP/POP (site) pour l'envoi des messages via Internet. La passerelle SISMEL filtre et contrôle ces messages et les envoie sur l'environnement Intradef vers un serveur SMTP/POP (MINDEF). En cas de défaut d'acheminement d'un message vers l'Intradef, une notification sera retransmise vers le fédérateur.

Le fédérateur doit être doté d'une interface conviviale permettant à un exploitant « autorisé » de visualiser les notifications d'erreurs et offrir les moyens nécessaires lui permettant de la traiter.

Sur cette interface doit apparaître de manière lisible tous les messages envoyés à destination du fédérateur.

Dans certains cas détaillés plus loin, un traitement automatique du message par le fédérateur sera réalisé.

L'ensemble des messages, les traitements associés et réalisés, seront conservés et classés de manière chronologique.

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 17/25


## **Cas d'une erreur dans le fichier de consommation ou d'alertes**

La passerelle SISMEL ne détecte pas les erreurs liées à la qualité ou la quantité des fichiers de consommation ou d'alertes.

Dans ce cas, L'OSF adresse une notification d'erreur au fédérateur pour signaler un problème à la réception d'un mail. L'OSF adresse également une notification aux exploitants qui sont en copie des mails du fédérateur et qui sont autorisés à recevoir des mails de l'extérieur.

Liste des erreurs (codes, descriptions) notifiées par l'OSF :

Codes	Descriptions
<b>SI-01</b>	« Il a été impossible de récupérer la pièce jointe dans votre mail du <jj/mm/aaaa>. Veuillez envoyer un nouveau mail en vérifiant la présence de votre fichier OSF avec le même code. »
<b>SI-02</b>	« Le fichier que vous avez envoyé le <jj/mm/aaaa> n'a pas la structure d'un fichier à destination de l'OSF car le fichier est corrompu ou le nom ne respecte pas la forme : « ef_consommations_NomSite_aaaa-mm-jj_Code.csv » Ou « ef_systemalerts_NomSite_aaaa-mm-jj_Code.csv » Ou « ef_codes_NomSite.csv » Veuillez vérifier le nom et le type de votre fichier OSF avant de l'envoyer à nouveau par mail avec un nouveau code »
<b>SI-03</b>	« Le fichier que vous avez envoyé le <jj/mm/aaaa> n'a pas le format d'un fichier à destination de l'OSF. Veuillez consulter le fichier log ci-joint, afin de corriger votre fichier OSF avant de l'envoyer à nouveau par mail avec un nouveau code. »
<b>SI-04</b>	« Le fichier que vous avez envoyé le <jj/mm/aaaa> est associé à un site inexistant. Veuillez corriger le nom du site et choisissez le code suivant disponible pour le nom de votre fichier OSF avant de l'envoyer à nouveau par mail avec un nouveau code. ».
<b>SI-05</b>	« Le fichier que vous avez envoyé le <jj/mm/aaaa> est associé à un code inexistant pour le site : <Code du fichier traité>. Veuillez vérifier que vous n'avez déjà envoyé ce fichier OSF dans un autre mail. Si ce n'est pas le cas, veuillez corriger le code de votre fichier OSF pour un code disponible avant de l'envoyer à nouveau par mail avec un nouveau code.
<b>SI-06</b>	« Le fichier que vous avez envoyé le <jj/mm/aaaa> est associé à un code non disponible pour le site : <Code du fichier traité>. Veuillez corriger le code de votre fichier OSF pour un code disponible avant de l'envoyer à nouveau par mail avec un nouveau code. »

	<div>Fiche</div> <div>Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense</div>	<div>Version : 2.1 Date : 18/12/2020</div> <div>Page 18/25</div>
---	--	--

<b>SI-07</b>	« Le fichier que vous avez envoyé le <jj/mm/aaaa> est associé à un code disponible mais non attendu pour le site : <Code du fichier traité> au lieu du : <Code attendu par la PFE>. Veuillez envoyer le fichier OSF associé au code attendu par mail afin de relancer le traitement des fichiers pour votre site. »
<b>SI-08</b>	« Le fichier que vous avez envoyé le <jj/mm/aaaa> contient des données incohérentes. Veuillez consulter le fichier log ci-joint, afin de connaître la liste d'erreurs à corriger dans l'outil GTP. »
<b>SI-09</b>	« En raison d'un problème de communication avec l'outil GTP, le fichier que vous avez envoyé le <jj/mm/aaaa> n'a pas été intégré. Il le sera automatiquement sans aucune action de votre part ultérieurement »
<b>SI-10</b>	« Le fichier de consommation que vous avez envoyé le <jj/mm/aaaa> est vide et le traitement des autres fichiers de consommation pour votre site restent en attente. Veuillez corriger le fichier de consommation en erreur avant de l'envoyer à nouveau par mail avec le même code. »
<b>SI-12</b>	« Le fichier que vous avez envoyé le <jj/mm/aaaa> contient des compteurs inexistantes. Veuillez consulter le fichier log ci-joint, afin de connaître la liste d'équipements à créer dans l'outil GTP. Vous n'avez pas besoin de l'envoyer à nouveau le fichier »

Le traitement des erreurs est géré par l'exploitant de façon manuelle ou automatique si une interface de paramétrage existe.


Le fédérateur peut faire des vérifications et réémettre un mail en cas d'erreur mais dans certains cas, il faut une analyse voire une expertise d'un exploitant ayant accès au fédérateur.

Le corps du message de chaque mail contient les lignes suivantes :

Ligne	Valeur
1	Date : <Date d'envoi du mail traité au format jj/mm/aaaa>
2	Heure : <Heure d'envoi du mail traité au format hh:mm>
3	Objet : <Objet du mail traité>
4	Code d'erreur : <Code>
5	Libellé : <Description de l'erreur>
6	<Balise de fin>

Exemple du corps du mail dans la notification de l'erreur « SI-05 » :

Date : 01/08/2012

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 19/25

Heure : 15:29  
 Objet : Fichier de consommations  
 Code d'erreur : SI-05  
 Libellé : Code inexistant pour le site : 0ef1.  
 [ENVOYE PAR INTERNET]

### **Sécurité :**

Le fédérateur doit être configuré de telle manière à n'accepter que les balises des accusé-réception provenant de SISMELE ou de l'OSF, et refuser toutes autres balises ou fichiers.

## **6. Exigences de sécurité**

### ***6.1. Exigences concernant la sécurisation du fédérateur***

#### **Protection physique du fédérateur**

Les équipements de télérelève sont hébergés dans des locaux du ministère de la défense. Le fédérateur, en particulier, doit se trouver dans un local fermé à accès contrôlé et être équipé d'un onduleur. L'ensemble des équipements du fédérateur doit être séparé de l'internet par un dispositif de pare-feu, afin de constituer un bastion (ou DMZ).


Le fédérateur ne doit être physiquement accessible qu'aux administrateurs du système.

#### **Séparation des serveurs**

Le fédérateur doit se composer d'au moins deux serveurs physiques : Le serveur de transfert de fichier sécurisé gérant les communications avec les concentrateurs doit être distinct du serveur de base de données.

#### **Firewall**

Le fédérateur doit être protégé par un firewall qualifié par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) et homologué par le MINDEF (de type Stormshield) pour sécuriser les communications entrantes et sortantes. Le firewall doit être à jour, administré et entretenu. Les logs doivent être régulièrement audités de manière à pouvoir détecter et expliquer tout comportement anormal.

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 20/25

### **Protocole sécurisé entre le concentrateur et le fédérateur**

Un protocole de sécurité standard, non propriétaire (FTPS, SCP, HTTPS, ...) assurera la transmission des données entre les concentrateurs et le fédérateur. Ce protocole sera installé sur un serveur distinct du serveur de base de données.

L'utilisation du GPRS (General Packet Radio Service) doit permettre de réaliser le transfert de données à partir des dispositifs de sécurité standards liés à cette technologie (Clés d'authentification – carte SIM, chiffrement des données de l'utilisateur).

### **Antivirus**

Un anti-virus sera installé sur chaque serveur (du type *Kaspersky*), ainsi que sur les postes « client » (du type *Trend-Micro*) et les passerelles (du type *Sophos*).

### **Mise à jour des systèmes de protection**

Une mise à jour régulière sera assurée concernant les moteurs anti-virus et les définitions ainsi que des correctifs concernant le système d'exploitation.

Les mises à jour des applications concernent toutes les applications utilisées dans le fonctionnement du fédérateur : serveur de messagerie, base de données, ... L'installation des correctifs est réalisée sous l'autorité du RSSI-A.

### **Traçabilité des connexions, imputabilité**

Un serveur de *logs* sera obligatoirement utilisé pour archiver les connexions pendant 1 an. Un export automatique des fichiers *logs* vers ce serveur doit être prévu.


Une politique d'identification renforcée doit être mise en place sur le serveur de transfert de fichier sécurisé du fédérateur pour assurer la reconnaissance des équipements émetteurs pour contrer notamment toute utilisation malveillante de l'adresse du constructeur.

Par ailleurs seuls les services utiles au fonctionnement, à la sécurité et à la supervision des systèmes d'information hébergés sur le fédérateur doivent être activés. Cela implique que les autres services doivent être désactivés.

Le système doit mettre en œuvre des mécanismes de protection des événements de sécurité contre la lecture, les modifications non autorisées et l'effacement en cas de dysfonctionnement.

Les événements de sécurité qui doivent être journalisés sur le fédérateur sont au minimum :

- Le démarrage (y compris le redémarrage) et l'arrêt (automatique ou manuel, y compris les échecs) d'un serveur ou d'un service ;
- L'authentification, l'échec d'authentification et la fermeture de session auprès d'un serveur ou d'un service ;
- La création, la suppression et la modification (y compris les échecs) des journaux de sécurité des serveurs ou des services ;
- Les événements liés à la gestion des journaux de sécurité (rotation, archivage, purge...) du serveur ou des services ;
- L'accès/modification de données système ;
- L'échec lors d'un accès à une ressource (fichier système, objet, réseau, etc.) ;
- L'application des correctifs de sécurité ;
- Les actions d'administration et de prise de main à distance ;

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 21/25

- Les journaux du logiciel antivirus (activation/désactivation, détection de codes malveillants, etc).

Les évènements de sécurité qui doivent être journalisés sur l'application installée sur le fédérateur sont au minimum :

- Connexion à l'application (succès et échec)
- Fermeture de session sur le SI
- La création, la suppression et la modification (y compris les échecs) des journaux de sécurité du système d'information
- Les actions liées à la gestion des journaux de sécurité (rotation, archivage, purge...) du système d'information
- La modification de droits sur le système d'information
- La création, la modification et la suppression de comptes.

### Système de détection d'intrusion

Un système de détection d'intrusion (IDS : Intrusion Detection System) du monde libre devra être, si possible, installé afin de repérer des activités anormales ou suspectes sur le fédérateur et avoir une connaissance sur les tentatives réussies ou échouées des intrusions.

### Administration à distance du fédérateur par des utilisateurs

L'administration à distance du fédérateur via Internet s'effectuera au moyen d'un protocole sécurisé type HTTPs, d'un dispositif d'authentification et d'un système de gestion des droits d'accès différenciant les profils (utilisateur, administrateur).

Par cet accès, il sera possible de consulter à distance les informations de consommation.

Les profils devront être nominatifs et individuels. La gestion des profils de connexion devrait être réalisée en local sur le fédérateur (création, suppression, modification des droits,...).

### Télémaintenance du fédérateur


En cas de télémaintenance, la liaison de télémaintenance doit être sécurisée de bout en bout. Une authentification forte de l'organisme chargé de la télémaintenance et une journalisation protégée des opérations de maintenance doivent être mises en œuvre. En outre, un accord écrit du MINDEF est requis avant toute modification de données. La liaison de télémaintenance n'est pas permanente et n'est activée qu'en cas de besoin avéré, sous la responsabilité de l'administrateur système et sous le contrôle de l'utilisateur connecté. Dans tous les cas, le lien de maintenance ne doit être « actif » que pendant le créneau prévu et pour une durée limitée. Le matériel auquel le fédérateur sera connecté devra être fixe et formellement identifié.

Les identifiants de connexion devront être nominatifs afin de tracer les interventions et de responsabiliser les intervenants.

L'exploitation opérationnelle du système doit être suspendue pendant les opérations de maintenance. La procédure de désactivation/réactivation de l'exploitation devra être clairement décrite. A cet effet, une procédure d'exploitation de sécurité (PES) générique sera établie par la direction centrale du SID. Celle-ci devra être adaptée localement (PES locale) et comportera l'ensemble des procédures à suivre pour que le système fonctionne en toute sécurité.

En outre, une documentation locale comportant les informations ci-dessous, devra être établie:

- Liste complète des actions à faire en cas d'incidents,

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 22/25

- Liste des points d'accès des équipements de télérelève (compteur, concentrateur, fédérateur).

## ***6.2. Exigences concernant l'accès à une application installée sur le fédérateur***

### **Identification et authentification.**

L'accès à tout poste de travail et à tout système d'information ne doit se faire qu'après une identification nominative.

Les droits de l'application doivent être restreints au strict minimum nécessaire à son fonctionnement.

### **Mots de passe.**

Quand l'authentification au système d'information et de communication est réalisée par un mot de passe, ses caractéristiques seront les suivantes :

- composé au minimum de 9 caractères (14 pour les administrateurs) dont au moins trois des catégories suivantes : caractères alphanumériques, chiffres arabes (0 à 9), caractère spécial (@, !, ?, /, é, ;, :, à, î, (, {, [, %, ...), mélange de majuscules et minuscules (sous réserve que le système d'exploitation le permette) ;
- ne doit pas contenir tout ou partie de l'identifiant, du nom de l'utilisateur, de son rôle ou de son grade ;
- a une durée de validité fixée à 45 jours pour les administrateurs et trois mois dans les autres cas ;
- a une durée de vie minimale de 7 jours ;
- ne peut être identique aux 6 derniers mots de passe utilisés.

Par ailleurs, le seuil d'avertissement de l'obligation de changer de mot de passe est fixé à 14 jours.

Après 6 tentatives de connexion infructueuses, un compte doit se verrouiller pour une durée minimale de :

- 60 mn pour les administrateurs,
- 30 mn dans les autres cas (avec remontée d'alarme auprès des administrateurs).


Le déverrouillage du compte, avant l'expiration du délai, doit nécessiter une action de l'administrateur.

### **Ecran de veille.**

Un écran de veille, associé à un mot de passe ayant les mêmes caractéristiques que celles prévues pour l'accès au poste de travail, doit systématiquement être activé en cas de non utilisation.

Le délai de non utilisation est variable selon l'importance des données et selon l'environnement. En tout état de cause, il ne pourra être supérieur à 10 minutes.

### **Profils.**

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 23/25

L'accès aux ressources informatiques est accordé par l'autorité hiérarchique et mis en place par l'administrateur compte tenu des missions de l'utilisateur, de son habilitation et de son besoin d'en connaître. La règle d'accès au moindre privilège doit être suivie dans l'attribution des droits à un utilisateur.

Des mécanismes permettant la gestion des différents profils des utilisateurs doivent être fournis. Une procédure de retrait des droits d'accès doit être prévue afin de ne pas voir subsister des comptes pour des utilisateurs qui ne sont plus présents. Notamment, pour les accès à distance qui doivent être supprimés dès que l'intervenant cesse ses activités.

### **6.3. Exigence concernant les émetteurs**

#### **Risque de perturbations électromagnétiques et radioélectriques occasionnées**


Les fiches techniques décrivant les équipements de télérelève montrent que le risque de perturbation radioélectrique et électromagnétique vis-à-vis des équipements existants a une vraisemblance très faible actuellement.. Les tests réalisés dans la base aérienne N°133 à Nancy-Ochey ont permis de confirmer ce résultat dans la pratique. Les équipements fonctionnent sur une bande de fréquence fixe publique (BF 169Mhz) à une puissance de 500mW maximum (limitation réglementaire).

Toutefois, s'il est admis que le risque de perturbation est extrêmement faible, certaines préconisations de principes seront suivies pour les installations ou équipements classifiés (PSSI-A PSD.53, II 920, DIR 485) au sujet des émetteurs radio et GPRS:

- Les émetteurs seront installés à plus de deux mètres de tout équipement classifié (poste classifié, réseau informatique classifié) ;
- Ils ne seront pas mis en place à l'intérieur d'une zone réservée, ni dans un local sécurisé, ni dans une salle de réunion ;
- Si l'émetteur est placé à proximité d'un mur, le local situé de l'autre côté ne doit pas contenir de matériel classifié ;
- L'émetteur ne devra pas être fixé à proximité d'un chemin de câbles.

La mise en place d'un équipement de télérelève à proximité d'un bâtiment « Confidentiel » ou à proximité de systèmes d'information classifiés doit se faire en respectant les consignes relatives à la protection par rapport à la menace TEMPEST. Ces consignes doivent être indiquées dans le dossier de sécurité du site.

### **6.4. Exigence concernant les agents extérieurs**

	Fiche	Version : 2.1 Date : 18/12/2020
	Préconisations techniques : interface de communication entre le système télérelève et l'application informatique OSF Défense	Page 24/25

### **Maîtrise des accès physiques.**

L'accès aux Zones Protégées, Zones Réservées ou locaux à accès restreint (accès par digicode ou badge) est strictement interdit à toute personne non autorisée.

Tout visiteur devant pénétrer dans des Zones Protégées, Zones Réservées ou locaux à accès restreint, doit obligatoirement être accompagné par une personne habilitée à pénétrer dans les locaux et à renseigner le registre « Visiteurs » pour les locaux techniques et du chiffre.

### **Habilitations.**

La société ainsi que les agents extérieurs doivent avoir fait l'objet d'une habilitation au niveau requis.

**ANNEXE : tableau de synthèse des pas et des unités de mesure à paramétrer dans le système de télérelève**

Type de fluides	Compteurs ou capteurs	Pas de la mesure relevée au point de comptage	Unités de mesure de la donnée collectée au fédérateur	Conversion		Unités à disposition de l'utilisateur de l'application OSF	Pas minimal de la mesure disponible sur l'OSF	Précision sur la mesure
				Type de conversion	Coefficient de conversion (paramétrable)			
EAU	Compteur principal	1h	m <sup>3</sup>	m <sup>3</sup>	1	m <sup>3</sup>	1h	1l
	Compteur forage	1h	m <sup>3</sup>	m <sup>3</sup>	1	m <sup>3</sup>	1h	1l
	Compteur château d'eau	1h	m <sup>3</sup>	m <sup>3</sup>	1	m <sup>3</sup>	1h	1l
	Compteur de secteur	1h	m <sup>3</sup>	m <sup>3</sup>	1	m <sup>3</sup>	1h	1l
	Compteur entrée bâtiment	1h	m <sup>3</sup>	m <sup>3</sup>	1	m <sup>3</sup>	1h	1l
	Compteur divisionnaire	1h	/	l → m <sup>3</sup> (1)	0,001	m <sup>3</sup>	1h	1l
ELECTRICITE	Compteur principal	10 minutes	/	l → m <sup>3</sup> (1)	0,001	m <sup>3</sup>	1h	1l
	Compteur entrée bâtiment	10 minutes	kWh	kWh	1	kWh	10 minutes	0.1kWh
	Compteur divisionnaire	10 minutes	kWh	kWh	1	kWh	10 minutes	0.1kWh
GAZ	Compteur principal	1h	m <sup>3</sup> (2)	m <sup>3</sup>	1	m <sup>3</sup>	1h	1m3
	Compteur entrée bâtiment	1h	m <sup>3</sup>	m <sup>3</sup>	1	m <sup>3</sup>	1h	1m3
	Compteur divisionnaire	1h	m <sup>3</sup>	m <sup>3</sup>	1	m <sup>3</sup>	1h	1m3
FOD	Compteur principal	1h	/ (1)	l → m3	0,001	m <sup>3</sup>	1h	1l
Thermique	Compteur principal	1h	kWh	kWh	1	kWh	1h	0.1kWh
	Compteur entrée bâtiment	1h	kWh	kWh	1	kWh	1h	0.1kWh
	Compteur divisionnaire	1h	kWh	kWh	1	kWh	1h	0.1kWh

(1) Le fédérateur aura à sa charge la conversion des valeurs unitaires qui remonteront des compteurs pour les rendre compatible avec le progiciel OSF.  
 Ex : Le compteur transmet une valeur en l/h vers le fédérateur. Le fédérateur transforme cette valeur en m3/h et la transmet vers l'OSF.  
 (2) Les données collectées au niveau du compteur de gaz situés au point de livraison doivent correspondre aux données de référence pour la facturation (Ex : compteur T3; données impulsionsnelles en sortie du convertisseur)