



ORU Nouvelle Aquitaine

Version : 1.0

FLUX RPU ETENDU





Veille Sanitaire Nouvelle Aquitaine

Table des matières

1 Objectifs2
2 Organisation2
3 Principes4
4 Procédure5
 4.1 Description Générale5
 4.2 Réalisation des tests unitaires5
 4.3 Description Tension5
5 Définition des formats XML attendus.....7
 5.1 Formulaire TENSION7
6 Définition du format de données attendus9
 6.1 Formulaire TENSION9
7 Sécurisation des échanges via GPG dans le cadre des transferts automatisés14
 7.1 Introduction14
 7.2 Préparation à l'utilisation de GPG – côté Acteurs14
 7.3 Chiffrement avec GPG – côté Acteur15

Rédacteurs	Date de modification
Caroline Ligier	14/06/2023



Veille Sanitaire Nouvelle Aquitaine

1 Objectifs

Procédure de transmission automatisée des RPU étendus à destination du serveur de « veille sanitaire » du ROR Nouvelle Aquitaine.

2 Organisation

L'ORU NA collecte **quotidiennement** les données OSCOUR ou RPU.

En complément de ces données et pour se rapprocher du décret du 24 Juillet 2013, les établissements de la région Nouvelle Aquitaine ont accepté lors de l'AG de l'ORU NA du 8 décembre 2016 de mettre en place un flux de RPU plus fréquent.

Le ROR (outil de l'ORU PACA) permettant la collecte de ses données



3 Procédure

3.1 Description Générale

Chaque acteur doit mettre en place un module capable :

- d'extraire de son SIH, les données requises dans les formulaires qui lui sont attribués ;
- générer un fichiers ASCII normalisé au format XML selon les recommandations du GCS ORU Nouvelle Aquitaine ;
- crypter individuellement les fichiers XML ;
- transmettre ces fichiers sur le serveur ftp régional ;

Pour obtenir un accès ftp il vous faut faire une demande d'identifiant à cie@oruna.fr avec les éléments suivants :

- Nom de l'établissement ;
- Plage d'adresses ip publiques qui enverront les fichiers ;
- Mail gpg afin d'échanger l'adresse IP du serveur FTP et le couple login/mot de passe pour s'y connecter ou numéro de téléphone portable ou adresse de messagerie sécurisé ;

Chaque acteur souhaitant transmettre ses indicateurs par ce biais recevra, par les soins de l'ORU Nouvelle Aquitaine :

- une clé publique de cryptage ;
- un identifiant ;
- une clé d'authentification à intégrer dans chacune de ses transmissions ;

3.2 Réalisation des tests unitaires

Afin de vous aider dans la démarche d'envoi au serveur de veille sanitaire, vous pouvez prendre contact avec l'informaticien de l'ORU Nouvelle Aquitaine Abderrahmen SAHLI au 06 18 37 23 29 ou abderrahmen.sahli@oruna.fr et cie@oruna.fr qui vous précisera les différentes étapes du protocole.



Veille Sanitaire Nouvelle Aquitaine

3.3 Description Tension

Les indicateurs d'**hôpital en tension** doivent être transmis **au fil de l'eau (toutes les 10 minutes)** lorsque les valeurs des éléments concernés sont disponibles

Le flux du formulaire TENSION requiert en effet des envois en temps réel selon les critères suivants :

- toutes les 10 minutes : tous les passages des 48 dernières heures (obligatoire)
- une fois par jour : tous les passages de J-7 à J-2 (optionnel)
- une fois par semaine : tous les passages des 30 derniers jours (optionnel)

Chaque fichier envoyé contiendra donc les données de plusieurs passages. A l'intégration, les données sont entièrement remplacées par période de dates.

Concrètement, la règle suivante est appliquée : tout ensemble de passages envoyé entre une date d'entrée t1 et t2 ANNULE ET REMPLACE toutes données précédentes entre les dates d'entrée t1 et t2 pour le service d'urgences concerné (couple Finess+UF).

Note : pour un fichier transmis, les dates d'entrée t1 et t2 correspondent respectivement à la date d'entrée du patient le plus ancien et à la date d'entrée du patient le plus récent.

Le module PRESTO (Outils Régionaux/Activité des Urgences du ROR) vérifie toutes les minutes les fichiers présents sur le dépôt ftp/sftp et calcule ainsi des indicateurs détaillés en annexe (SRVA-IndicateursPRESTO-1.0.pdf de l'ORU PACA qui est l'éditeur du ROR).

4 Définition des formats XML attendus

4.1 Formulaire TENSION

<passages idSite="**Identifiant de l'acteur**" passSite="**Clé Unique attribuée à l'acteur**" idTerminal="**UF d'accueil du service**" capacite="**Nombre de lits installés aux urgences hors UHCD**" >

```
<passage>
  <entree>Date d'entrée </entree>
  <sortie>Date de sortie (si sorti) </sortie>
  <ilp_c>Hash de l'IPP</ilp_c>
  <idpass_c>Hash de l'IDPASS</idpass_c>
  <uf>UF du Patient</uf>
  <is_uhcd>Le patient est UHCD ?</is_uhcd>
  <is_uhcdrepere>Le patient est en UHCD mais présent physiquement aux urgences </is_uhcdrepere>
  <dt_naissance>Date de naissance </dt_naissance>
  <sexe>Sexe</sexe>
  <date_examen>Date d'examen Médicale </date_examen>
  <date_uhcd>Date de passage en UHCD</date_uhcd>
  <mode_admission>Mode d'admission </mode_admission>
  <transport_admission>Mode de transport à l'admission </transport_admission>
  <medecin_urgentiste>Identifiant unique du médecin</medecin_urgentiste>
  <salle_exam>Identifiant unique de la salle(box)</salle_exam>
  <categorie_recours>Thésaurus SFMU</categorie_recours>
  <motif_recours>Thésaurus SFMU</motif_recours>
  <code_recours>Code CIM10 du recours</code_recours>
  <ccmu>Code CCMU</ccmu>
  <dest_souhaitee>Destination souhaitée</dest_souhaitee>
  <dest_attendue>Destination confirmée</dest_attendue>
  <ide>Identifiant unique de l'IDE</ide>
  <moyen_transport>Moyen de transport</moyen_transport>
  <motif_transfert>Motif du transfert</motif_transfert>
  <type_dest>Type de sortie</type_dest>
</actes>
```



Veille Sanitaire Nouvelle Aquitaine

```
<ccam>Code CCAM de l'acte</ccam>
</actes>
<diags>
  <diag is_ppal="1/0">Code CIM10 du diagnostic</diag>
</diags>
</passage></passages>
```

5 Définition du format de données attendus

5.1 Formulaire TENSION

Nom du fichier :

Le nom du fichier généré doit être construit de la façon suivante :

passages.Indentifiant.dateTimeGeneration._v2_.extensionFichier

Il y a bien 2 « . » consécutivement après passages (en PACA un autre identifiant est utilisé ici)

Définition des variables :

- **dateTimeGeneration** : date au format datetime yyyyymmjjhmmss (exemple : 20140903094012)
- **extensionFichier** : .xml si le fichier n'est pas chiffré, .xml.gpg si le fichier est chiffré avec GPG

A titre d'exemple, voilà le nom d'un fichier qui pourrait être transmis :

passages.703.20230603094012._v2_.xml.gpg

Le dépôt dans le répertoire liveTgs du serveur ftp régional doit se faire de la façon suivante :

- transmission du fichier contenant les passages :
 - exemple : passages.703.20230603094012._v2_.xml.gpg
- création et transmission d'un fichier vide nommé de la même façon que précédemment mais en ajoutant l'extension .ok :
 - exemple : passages.703.20230603094012._v2_.xml.gpg.ok

Au final, une fois la transmission terminée, avec notre exemple, il devrait y avoir les fichiers suivants déposés :

- passages.703.20230603094012._v2_.xml.gpg
- passages.703.20230603094012._v2_.xml.gpg.ok



Veille Sanitaire Nouvelle Aquitaine

En tête du fichier xml :

- **idSite** : identifiant unique de l'établissement (fourni par l'ORU)
- **passSite** : clé unique de l'établissement (fourni par l'ORU)
- **idTerminal** : UF d'accueil du service d'urgences
- **finess** : Finess de l'établissement géographique
- **capacite** : Nombre de lits totaux aux urgences hors UHCD

Avec l'aide des informations cidessus, l'en tête du fichier généré sera de la forme suivante :

```
<passages idSite="idSite" passSite="passSite" idTerminal="idTerminal" finess="finess"  
capacite="capacite" >  
<passage>
```

Les éléments surlignés dans le tableau ci-dessous sont ceux permettant le calcul des indicateurs de Tension (cf Annexe : SRVA-IndicateursPRESTO-1.0.pdf) .

Veille Sanitaire Nouvelle Aquitaine

<i>Balise</i>	<i>Description</i>	<i>Type</i>	<i>Format et observations</i>
<passages	Code du formulaire	Caractères	
idSite	Identifiant de l'acteur	Entier	Fourni par l'ORU
passSite	Clé unique attribuée à l'acteur	Caractères	Fourni par l'ORU
idTerminal	UF d'Accueil du Service	Caractères	Nom de L'UF
finess	Code FINESS du Service	Entier	Fines géographique du Site
capacite	Nombres de lits totaux aux Urgences (hors UHCD)	Entier	Supérieur à 0
<passage>	Code du formulaire	Caractères	
<entree>	Date d'entrée du patient	DateTime	YYYY-MM-JJ HH:MM:SS
<sortie>	Date de sortie (si sorti) du patient	DateTime	YYYY-MM-JJ HH:MM:SS
<ilp_c>	Hash quelconque de l'IPP	Caractères	SHA1,MD5...
<idpass_c>	Hash quelconque de l>IDPASS	Caractères	SHA1,MD5...
<uf>	UF du Patient	Entier	Supérieur ou égal à 0
<is_uhcd>	Le patient est UHCD ? Si oui 1 sinon 0	Binaire	1 / 0 ou vide
<is_uhcdrepere>	Le patient est en UHCD mais présent physiquement aux Urgences.Si oui 1 sinon 0	Binaire	1 / 0 ou vide
<dt_naissance>	Date de naissance du patient	DateTime	YYYY-MM-JJ HH:MM:SS brouillage à 10 % de son âge de manière aléatoire
<sexe>	Sexe du patient	Caractère	M / F / I
<date_examen>	Date du premier examen médical du patient	DateTime	YYYY-MM-JJ HH:MM:SS
<date_uhcd>	Date de passage en UHCD	DateTime	YYYY-MM-JJ HH:MM:SS
<mode_admission>	Mode d'admission du patient 1 : Soins de courte durée (MCO) 2 : Soins de suite ou de réadaptation 3 : Soins de longue durée 4 : Psychiatrie 5 : Raison autre que organisationnelle 8 : Raison organisationnelle	Entier	1 / 2 / 3 / 4 / 5 / 8
<transport_admission>	AMBU : Ambulance publique ou privée PERSO : Moyens personnels VSAB : Véhicule de secours d'aide aux blessés SMUR : Service Mobile d'Urgences et de Réanimation HELI : Hélicoptère FO : Forces de l'ordre	Caractères	AMBU / PERSO / VSAB / SMUR / HELI / FO

Veille Sanitaire Nouvelle Aquitaine

<i>Balise</i>	<i>Description</i>	<i>Type</i>	<i>Format et observations</i>
<medecin_urgentiste>	Identifiant unique (quelconque) du médecin urgentiste	Caractères	Nom du médecin hashé ou non
<salle_exam>	Identifiant uniquement (quelconque) de la salle	Caractères	Nom ou Numéro de la salle
<categorie_recours>	Catégorie du motif de recours	Caractères	SFMU
<motif_recours>	Libellé du motif de recours aux urgences	Caractères	SFMU
<code_recours>	Code CIM10 du recours	Caractères	SFMU
<ccmu>	Code de la CCMU	Entier	1 / 2 / 3 / 4 / 5
<dest_souhaitee>	Destination souhaitée pour le patient	Caractères	
<dest_attendue>	Destination confirmée pour le patient	Caractères	
<ide>	Identifiant unique (quelconque) de l'IDE	Caractères	Nom de l'IDE hashé ou non
<moyen_transport>	Moyen de transport à la sortie du patient (utilisé lorsque la destination confirmée de type transfert vers un autre établissement)	Caractères	Ambulance privée Ambulance de l'établissement Moyen personnel Hélicoptère autre Hélicoptère SAMU SMUR SAMU VSAB
<motif_transfert>	Motif de transfert du patient	Caractères	Carence de lit Convenance personnelle Défaut plateau technique
<type_dest>	Type de sortie du patient : H : Mutation : le malade est hospitalisé vers une autre unité médicale de la même entité juridique T : Transfert : le malade est hospitalisé dans une autre entité juridique E : Externe (domicile) 6 : Hospitalisation à domicile (assimilé domicile) 7 : Structure d'hébergement médico-social (assimilé domicile) F : Fugue (assimilé domicile) S : Sortie contre avis médical (assimilé domicile) P : Partie sans attendre une prise en charge (assimilé domicile) R : Réorientation directe sans soins (assimilé domicile)	Caractère	H / T / E / 6 / 7 / F / S / P / R / D



Veille Sanitaire Nouvelle Aquitaine

<i>Balise</i>	<i>Description</i>	<i>Type</i>	<i>Format et observations</i>
	D : Décès		
<actes><ccam></ccam>	Code CCAM de l'acte	Caractères	Thésaurus CCAM
<diags is_ppal="1 si diag principal ou 0 ">	Code CIM10 du diagnostic	Caractères	Thésaurus CIM10
</passage></passages>			

6 Sécurisation des échanges via GPG dans le cadre des transferts automatisés

6.1 Introduction

Les fichiers amenés à être transmis par messagerie électronique seront préalablement chiffrés.

L'outil utilisé pour le chiffrement des fichiers est le logiciel GnuPG dans sa dernière version stable.

Ce logiciel est la version gratuite et libre du standard de cryptographie forte OpenPGP.

Les guides d'utilisation, FAQ, sources et binaires du logiciel sont disponibles sur le site <http://www.gnupg.org> et sur de nombreux miroirs référencés depuis cette même adresse.

Une paire de clé privée/publique sera générée par la veille ARS. La veille ARS détiendra la clé privée et fournira sa clé publique aux entités ayant à lui transmettre des fichiers.

6.2 Préparation à l'utilisation de GPG – côté Acteurs

Du côté « émetteur des fichiers – utilisateur de la clé publique » deux opérations sont nécessaires :

- importation de la clé publique
- trust de cette clé

Importation de la clé publique

On doit importer la clé publique fournie par la veille ARS dans le trousseau de clés de GPG

Pour cela on va indiquer à GPG de récupérer la clé depuis le fichier texte qui aura été fourni.

```
gpg --import "pubkey-veille-arh.txt"
```

Une fois la clé importée avec succès, on pourra afficher son fingerprint pour vérifier que l'on a bien importé la bonne clé .

```
gpg --fingerprint vs-arh@sante-aquitaine.org
```



Veille Sanitaire Nouvelle Aquitaine

Trust de la clé

A l'utilisation de GPG pour chiffrer avec une clé publique non trustée le message suivant s'affiche :

*« It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.
Use this key anyway ?) »*

On doit donc déclarer la clé importée comme « de confiance » afin d'éviter les messages d'avertissement à chaque utilisation de cette clé :

```
gpg --edit-key vs-arh@sante-aquitaine.org  
Command> trust
```

Choisir de faire confiance complètement à cette clé : Yes

6.3 Chiffrement avec GPG – côté Acteur

Chiffrement d'un fichier avec la clé publique veille ARH

Exemple : Nous allons chiffrer le fichier fichier-test.pdf :

```
gpg -r vs-arh@sante-aquitaine.org --encrypt fichier-test.pdf
```

Nous récupérons le fichier chiffré avec une double extension fichier-test.pdf.gpg