AGENCE
DU NUMÉRIQUE
EN SANTÉ

Volet Transport Synchrone pour Client Lourd

CI-SIS – Février 2021

Statut : Validé | *Classification : Publique* | *Version : 1.8*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1. POSITIONNEMENT DANS LE CADRE D'INTEROPERABILITE

Ce volet spécifie la couche Transport pour :

- un système cible offrant un service auquel il est possible de se connecter de façon synchrone ;
- un système initiateur bénéficiant d'un « client lourd » (c.à.d. un logiciel spécialisé intégrant les interfaces décrites dans ce volet) se connectant au service de façon synchrone.

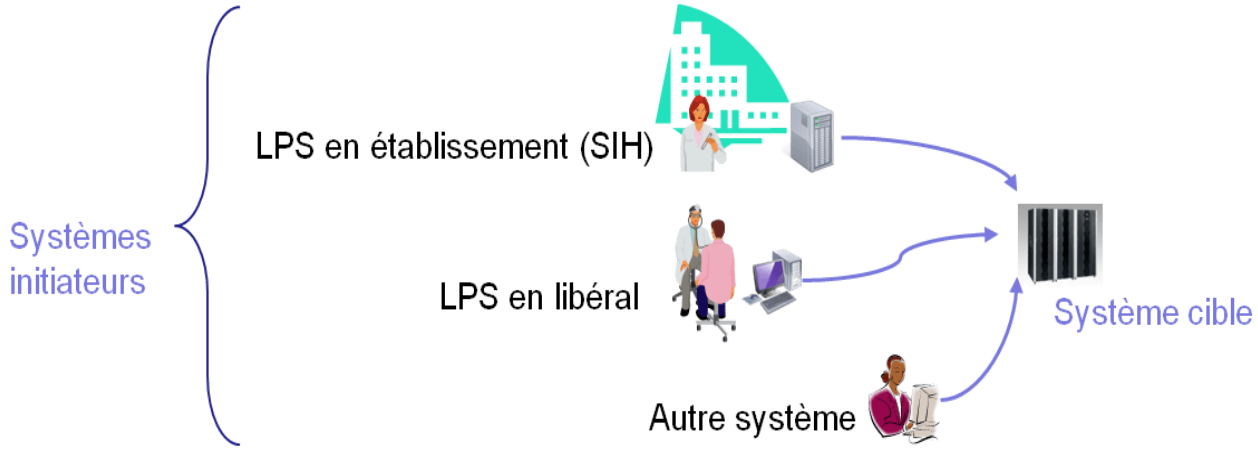

Figure 1 : Rôles des systèmes

Ce volet est utilisé par le volet partage de documents médicaux.

Nota :

Les spécificités d'implémentation des standards utilisés présentées dans ce volet seront validées et approfondies dans le cadre de la réalisation de systèmes de santé majeurs tels que le DMP V1.

Certaines solutions restant à valider feront l'objet d'implémentations de test.

Cet aspect est particulièrement sensible pour la configuration « Libérale », pour laquelle la mise en œuvre de la carte CPS présente des limitations techniques qui nécessitent de faire des choix présentant un compromis acceptable entre sécurité et performance.

2. PRE-REQUIS

Pour être conforme au présent volet, les systèmes initiateurs et cibles doivent pouvoir s'appuyer sur des certificats émis par une IGC autorisée par les référentiels d'authentification de la PGSSI-S que ceux-ci soient associés à des personnes physiques (ex. CPS personnelle et nominative) ou à des personnes morales (ex. certificat de personne morale, certificat serveur).

3. SPECIFICATIONS

3.1. Références

Le choix de la pile protocole pour ce volet est présenté ci-dessous. Il est basé sur l'annexe V du tome 2x du cadre technique ITI d'IHE et le profil d'implémentation XUA :

Les échanges se font sur le protocole **http 1.1** encapsulé dans une connexion sécurisée **TLS**.

SOAP 1.2 est utilisé et permet de spécifier le format du message ainsi que les informations sur le message lui-même permettant son acheminement à travers un réseau (de type Internet) et son traitement.

Les flux transportant des documents utilisent en plus les mécanismes d'optimisation du codage et de la transmission des messages SOAP définis dans **MTOM** et **XOP**.

Les services offerts par les systèmes de santé doivent être décrits dans un langage commun exploitable par tout autre système, le standard **WSDL 1.1**.

Enfin, les flux doivent comporter une assertion **SAML 2.0** intégrant des informations d'authentification de l'utilisateur définies en fonction du certificat **X509** utilisé par le système. L'utilisation de l'assertion SAML doit respecter la standardisation **WS-I Basic Security Profile 1.1**, notamment les recommandations **WS-Security SAML Token Profile 1.1** pour ce qui concerne le contenu de l'assertion et son utilisation avec WS-Security.

http 1.1 :

http://www.w3.org/Protocols/rfc2616/rfc2616.html

TLS 1.0 :

http://www.ietf.org/rfc/rfc2246.txt

SOAP 1.2 :

http://www.w3.org/TR/2007/REC-soap12-part0-20070427/

http://www.w3.org/TR/2007/REC-soap12-part1-20070427/

http://www.w3.org/TR/2007/REC-soap12-part2-20070427/

http://www.w3.org/TR/2007/REC-soap12-testcollection-20070427/

MTOM :

http://www.w3.org/TR/soap12-mtom/

XOP :

http://www.w3.org/TR/2005/REC-xop10-20050125/

WSDL 1.1 :

http://www.w3.org/TR/wsdl

SAML 2.0 :

http://saml.xml.org/saml-specifications

Certificat X509 :

http://tools.ietf.org/html/rfc5280

WS-I Basic Security Profile 1.1:

http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html

WS-Security SAML Token Profile 1.1:

http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf

3.2. Messages SOAP

3.2.1. Structure d'un message SOAP avec WS-Addressing

Le protocole SOAP définit une grammaire XML pour décrire le format et la structure du message échangé. Ce paragraphe détaille les principaux éléments d'un message SOAP.

Le message SOAP est obligatoirement composé d'une ***Envelope*** (Enveloppe) qui contient éventuellement un élément **Header** (en-tête) et obligatoirement un élément ***Body*** (corps).

Exemple de la structure d'une enveloppe SOAP :

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope" >
  <env:Header>
     ……..
</env:Header>
 -<env:Body>
     …….
- </env:Body >
<env:Envelope>
```

Le mot clé Enveloppe est suivi obligatoirement d'un espace de nom indiquant la version du protocole SOAP utilisée et éventuellement d'un attribut ***encodingStyle*** permettant de préciser les règles d'encodage du message.

Dans la version SOAP1.2, l'attribut ***xmlns:env*** représente le mot clé ***namespaces*** associé au préfixe "env" qui définit l'enveloppe.

La chaîne de caractères "http://www.w3.org/2003/05/soap-envelope" désigne la version du protocole SOAP utilisée (ici SOAP1.2).

L'élément ***Header*** (en-tête) du message est optionnel et contient les éléments techniques du message (appelés entrées) destinés à être traités par des nœuds intermédiaires et le nœud final.

L'en-tête permet d'étendre les spécifications du message SOAP à d'autres spécifications qui gèrent des fonctionnalités techniques telles que la gestion de l'adressage, la gestion de la sécurité, le caractère requis ou non du traitement du message par le nœud récepteur, etc.

L'en-tête contient donc un ou plusieurs éléments composés chacun d'un espace de nom et de deux attributs réservés à la spécification SOAP1.2 :

- L'attribut ***role*** désigne le destinataire de l'élément de l'en-tête. Lorsqu'il est omis, le destinataire correspond au point final, c'est-à-dire un web-service endpoint du système cible.
- L'attribut ***mustUnderstand*** permet d'indiquer le caractère requis ou non du traitement de l'élément d'en-tête par le destinataire. Ce traitement est obligatoire dans le cas où ***mustUnderstand*** = "true".

Dans le cas des SIS français :

- l'élément **Header** (en-tête) du message SOAP est requis ;
- aucun nœud intermédiaire n'est prévu entre système initiateur et système cible, l'attribut ***role*** est absent de la structure du message SOAP ;
- l'attribut ***mustUnderstand*** est égal à "true" ce qui signifie que le message est adressé au nœud final (services définis dans les volets de la couche Service du cadre d'interopérabilité) et qu'il doit être traité par ce nœud.

Il est possible d'étendre le protocole SOAP en ajoutant des éléments techniques à l'en-tête du message.

Il est notamment possible d'ajouter une entrée WS-Addressing permettant d'indiquer le destinataire du message (élément <To>), l'identifiant du message (élément <MessageID>), l'action à réaliser (élément <Action>) et l'adresse à laquelle le message de réponse doit être envoyé (élément <ReplyTo>).

Exemple de Header SOAP avec une entrée WS-Addressing pour une transaction d'un service de type partage de documents médicaux

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
    <env:Header>
        <a:Action env:mustUnderstand="true">urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b</a:Action>
        <a:MessageID>urn:uuid:6d296e90-e5dc-43d0-b455-7c1f3eb35d83</a:MessageID>
        <a:ReplyTo env :mustUnderstand="true">
            <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
        </a:ReplyTo>
        <a:To>http://localhost:2647/XdsService/IHEXDSRepository.svc</a:To>
    </env:Header>
    <env:Body> ……
    </env:Body>
<env:Envelope>
```

Dans le cas des SIS français, le protocole SOAP1.2 est étendu avec la spécification WS-Addressing, ses caractéristiques sont les suivantes :

- les éléments <Action>, <To>, <MessageID> et <ReplyTo> doivent être présents ;
- l'élément <Action> doit comporter l'attribut mustUnderstand à la valeur "true" ;
- dans le cas d'un message initial, l'élément <ReplyTo> doit comporter l'attribut mustUnderstand à la valeur "true".

L'élément ***Body*** est requis et suit immédiatement l'élément ***Header***. Il est produit par l'émetteur et doit être consommé obligatoirement par le destinataire final.

Il contient un ensemble d'éléments composés chacun par un espace de noms et des attributs portant les données spécifiques à l'application.

Le corps du message peut aussi contenir un élément ***Fault***, qui permet éventuellement de renvoyer vers l'émetteur le type d'erreur intervenu lors du traitement du message par le destinataire.

La figure 2 représente un message SOAP pour le cadre d'interopérabilité des SIS français. Les éléments optionnels sont représentés en pointillé.

La spécification SOAP autorise l'utilisation de plusieurs vocabulaires XML (namespaces ou espaces de nom). Elle définit un espace de nom pour coder les éléments et les attributs propres aux messages SOAP1.2 et autorise l'utilisation d'espaces de nom applicatifs spécifiques. Tous les espaces de nom doivent être déclarés dans l'enveloppe SOAP.

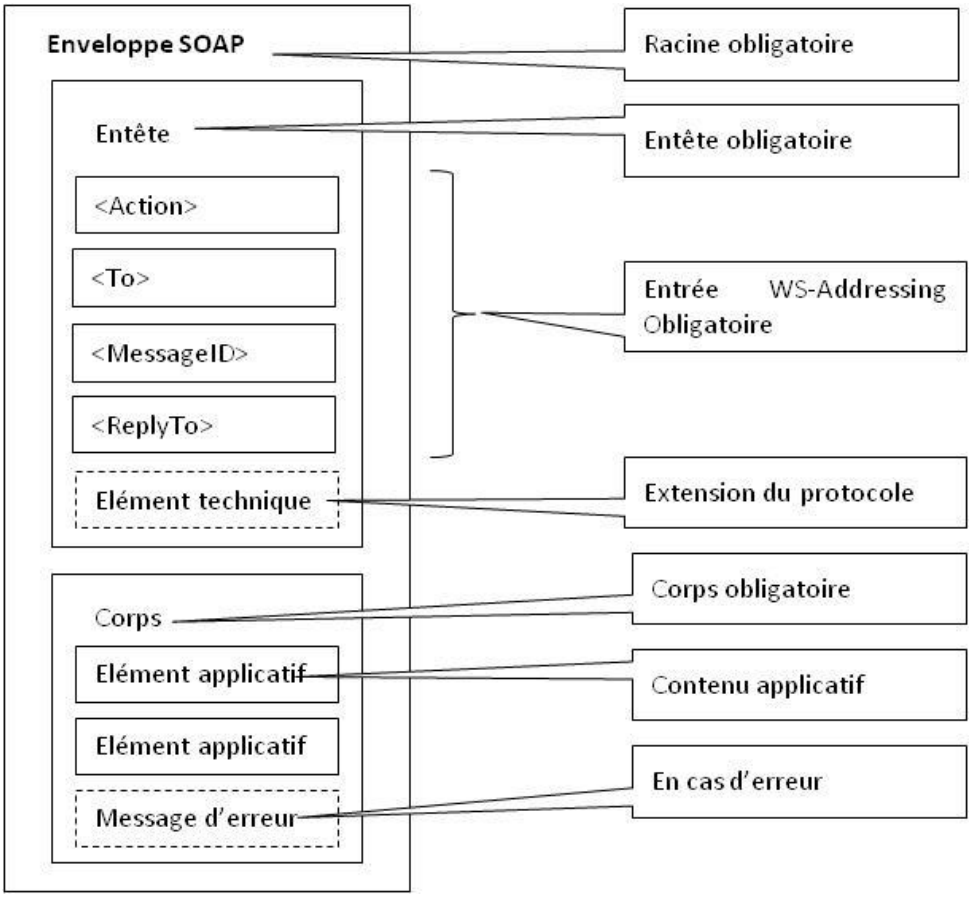

Figure 2 : Structure d'un message SOAP pour le cadre d'interopérabilité des SIS français

Le tableau suivant liste les namespaces qui doivent être utilisés pour les SIS français.

soap12	http://schemas.xmlsoap.org/wsdl/soap12/
wsaw	http://www.w3.org/2006/05/addressing/wsdl
xsd	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance
ihe	urn:ihe:iti:xds-b:2007
rs	urn:oasis:names:tc:ebxml-regrep:xds:rs:3.0
lcm	urn:oasis:names:tc:ebxml-regrep:xds:lcm:3.0
query	urn:oasis:names:tc:ebxml-regrep:xds:query:3.0
HL7 V3	urn:hl7-org:v3

3.2.2. Style et encodage du message SOAP

SOAP permet de définir le codage des données manipulées par les messages et les règles d'encodage/décodage (sérialisation/dé-sérialisation) de ces données par les applications émettrices/réceptrices.

Ce codage et les règles d'encodage/décodage associées sont appelés « styles de codage » (encoding style).

Ce style de codage est porté par l'attribut encodingStyle qui peut apparaître :

- au niveau d'un bloc d'en-tête du message,
- au niveau d'un élément fils du corps du message.

La portée du style d'encodage est limitée à l'élément ou à ses descendants auquel il est rattaché.

Outre le codage des données constituant le message SOAP, il faut aussi considérer le codage des documents véhiculés par le message.

SOAP propose deux styles d'encodage :

- Codage littéral : aucun codage de données particulier n'est appliqué au message. Le contenu du message véhiculé est un document XML. Il est manipulé tel que par les applications qui s'échangent le message SOAP. On parle de style de codage « document ».
- Codage explicite : le style de codage est indiqué explicitement par l'élément encodingStyle et définit la correspondance entre la représentation des données gérées par l'application et celle gérée par le message SOAP. On parle de style de codage RPC (Remote Procedure Call). Dans le cas où le contenu a été codé selon les règles d'encodage SOAP, l'attribut encodingStyle prend la valeur : « http://www/w3.org/2003/05/soap-encoding ». L'absence de valeur pour l'élément encodingStyle indique qu'il n'y a pas de codage particulier.

Pour les SIS français, pour l'échange de documents, le codage littéral doit être utilisé. L'élément encodingStyle n'est pas présent dans le message SOAP.

3.2.3. Styles d'échanges des messages SOAP

SOAP définit deux types d'échanges entre un émetteur SOAP et un récepteur SOAP :

- transmission unidirectionnelle du message,
- transmission de type requête/réponse.

Dans le premier cas, le message SOAP est transmis de l'émetteur vers le récepteur et l'émetteur n'attend pas de réponse de la part du récepteur.

Dans le deuxième cas, le message de requête est suivi d'une réponse. Ce style d'échange requête/réponse s'applique à la fois aux messages utilisant le style de codage explicite (style d'échange RPC) et à ceux utilisant le style de codage littéral (style d'échange Document).

Pour les SIS français, pour l'échange de documents, le style d'échange requête/réponse doit être utilisé.

3.2.4. Liaison avec le protocole de transport ou binding (HTTP 1.1 dans TLS)

Les messages SOAP peuvent être échangés en s'appuyant sur différents protocoles. La description de la façon de transférer un message d'un nœud à un autre en utilisant un protocole particulier est appelée «liaison avec le protocole» ou «protocol binding».

Pour les SIS français, le protocole **HTTP1.1** encapsulé dans une connexion sécurisée **TLS** doit être utilisé.

Un message HTTP correspond soit à une requête d'un client, soit à une réponse du serveur.

Le message de requête HTTP 1.1 est constitué de :

- une ligne de requête qui contient la méthode utilisée (POST) ainsi que l'URL destinatrice,
- champs d'en-tête optionnels du type «champ:valeur»,
- une ligne vide,
- un corps de message MIME optionnel dépendant du type de l'encodage utilisé qui est décrit dans les champs Content-Type et Content-Encoding.

Exemple d'un message HTTP de requête pour une transaction d'un service de type partage de documents médicaux

```
POST <!—Volontairement non spécifié--> HTTP/1.1
Content-Type: multipart/related;
boundary=MIMEBoundaryurn_uuid_806D8FD2D542EDCC2C1199332890718;
type="application/xop+xml"; start="0.urn:uuid:806D8FD2D542EDCC2C1199332890719@example.org";
start-info="application/soap+xml"; action="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b"
User-Agent: <!—Volontairement non spécifié-->
Host: localhost:9085

--MIMEBoundaryurn_uuid_806D8FD2D542EDCC2C1199332890718
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:806D8FD2D542EDCC2C1199332890719@example.org>

<?xml version='1.0' encoding='UTF-8'?>
<env:Envelope xmlns:env=http://www.w3.org/2003/05/soap-envelope
   xmlns:wsa="http://www.w3.org/2005/08/addressing">
   <env:Header>
      ……
   </env:Header>
   <env:Body>
      ……
   </env:Body>
</env:Envelope>
--MIMEBoundaryurn_uuid_806D8FD2D542EDCC2C1199332890718
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:806D8FD2D542EDCC2C1199332890776@example.org>

< !—Emplacement du document codé en binaire-->

      ……..

--MIMEBoundaryurn_uuid_806D8FD2D542EDCC2C1199332890718--
```

Le message de réponse HTTP 1.1 est constitué de :

- une ligne de statut qui contient la version HTTP utilisée, un code de réponse numérique ainsi que la description textuelle du statut,
- champs d'en-tête optionnels du type « champ:valeur »,
- une ligne vide,
- un corps de message MIME optionnel dépendant du type de l'encodage utilisé qui est décrit dans les champs Content-Type et Content-Encoding.

Exemple d'un message HTTP de réponse pour une transaction d'un service de type partage de documents médicaux

```
HTTP/1.1 200 OK
Server: <!—Volontairement non spécifié-->/1.1
Content-Type: application/soap+xml; action="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-
bResponse";charset=UTF-8
Date: Thu, 03 Jan 2008 04:01:37 GMT

<?xml version='1.0' encoding='UTF-8'?>
<env:Envelope xmlns:env=http://www.w3.org/2003/05/soap-envelope
   xmlns:wsa="http://www.w3.org/2005/08/addressing">
   <env:Header>
      …..
   </env:Header>
   <env:Body>
      <rs:RegistryResponse xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
         status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"/>
   </env:Body>
</env:Envelope>
```

Pour les SIS français, pour le transport de documents, la méthode HTTP1.1 POST doit être utilisée.

À noter que l'utilisation de la valeur « urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b » dans l'élément Action de l'entête des messages SOAP n'est pas obligatoire. Ceci s'applique à l'ensemble des exemples dans ce document utilisant cette valeur.

3.2.5. Transport de documents avec MTOM et XOP

La spécification MTOM (SOAP Message Transmission Optimization Mechanism) décrit un mécanisme abstrait d'optimisation du codage et de la transmission des messages SOAP, permettant d'encoder d'une façon optimisée les portions du message SOAP codées en base64.

Le protocole XOP (XML-binary Optimized Packaging) implémente concrètement MTOM pour encoder l'enveloppe SOAP de façon optimisée, utilisant le format XOP et un packaging de type MIME Multipart/Related.

Les éléments de type base64 sont extraits de l'infoset XML, ré-encodés en binaire et placés dans un package de type MIME Multipart/Related.

L'exemple suivant décrit la structure de l'enveloppe SOAP sans optimisation du codage et du transfert du document.

Exemple de l'utilisation de MTOM pour une transaction d'un service de type partage de documents médicaux

```
MIME-Version: 1.0
Content-Type: type=text/xml
Content-Description: exemple XDS.b utilisant MTOM

<?xml version='1.0' ?>
<env:Envelope
xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
<env:Body>
<!—Description des métadonnées -->
...
<ExtrinsicObject id="monDocument" />
...
<Document id="monDocument">contenu du document encodé en base64</Document>
...

</env:Body>
</env:Envelope>
```

L'enveloppe SOAP contient un élément <Document> qui contient le document codé en base64. Ce mode de codage est adapté aux documents peu volumineux.

L'exemple suivant décrit la structure de l'enveloppe SOAP sérialisée en utilisant un package XOP.

Exemple de l'utilisation de MTOM/XOP pour une transaction d'un service de type partage de documents médicaux.

```
MIME-Version: 1.0
Content-Type: Multipart/Related; boundary=MIME_boundary;
  type="application/xop+xml";
  start="<monmessage.xml@example.org>"
  start-info="application/soap+xml;action="urn:ihe:iti:2007:ProvideAnd
RegisterDocumentSet-b"
Content-Description: exemple MTOM/XOP

--MIME_boundary
Content-Type: application/xop+xml;
        charset=UTF-8;
        type="application/soap+xml;action="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b"
Content-Transfer-Encoding: 8bit
Content-ID: monmessage.xml@example.org

<?xml version='1.0' ?>
<env:Envelope
xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
xmlns :xmlmime="http://www.w3.org/2004/11/xmlmime">
<env:Body>

<!—Description des métadonnées -->
...
<ExtrinsicObject id="monDocument" />
...
<Document xmlmime:content"Type=text/xml" id="monDocument">
<xop:Include xmlns:xop=http://www.w3.org/2004/08/xop/include
   href="cid:1.urn:uuid:BC47538ED684E0A2D41194546709563@example.org"/>
</Document>
...

</env:Body>
</env:Envelope>

--MIME_boundary
Content-Type: text/xml
Content-Transfer-Encoding: binary
Content-ID: cid:1.urn:uuid:BC47538ED684E0A2D41194546709563@example.org

//ici, Encodage binaire des contenus de documents
--MIME_boundary—
```

Les éléments <ExtrinsicObject> et <Document> placés dans les métadonnées ont tous les deux la même valeur d'attribut id.

L'élément <Document> a un élément fils <Include> qui référence l'identifiant de la partie MIME qui contient le document codé en binaire.

Ce mode de codage est adapté aux documents volumineux.

Pour les SIS français, le codage et le transfert des documents doit être optimisé en utilisant le protocole MTOM/XOP.

La transaction métier (constitution du document et de ses attributs définis selon le service utilisé) est réalisée au niveau applicatif. Elle est transmise à la couche d'infrastructure de message qui construit le message SOAP, en accord avec les règles définies dans le fichier de description du web service (cf description d'un service web (WSDL) ci-dessous).

3.2.6. Description d'un service Web (WSDL)

WSDL1.1 est une spécification qui permet de décrire, sous la forme d'un fichier XML, les interfaces et les modalités d'interaction avec un web service.

WSDL permet de spécifier non seulement l'interface abstraite, mais aussi les types de données utilisés, le format de message, les conventions de codage et les protocoles de transport utilisés.

La spécification WSDL décrit un service comme un ensemble de points finaux de communication (ports) qui s'échangent des messages.

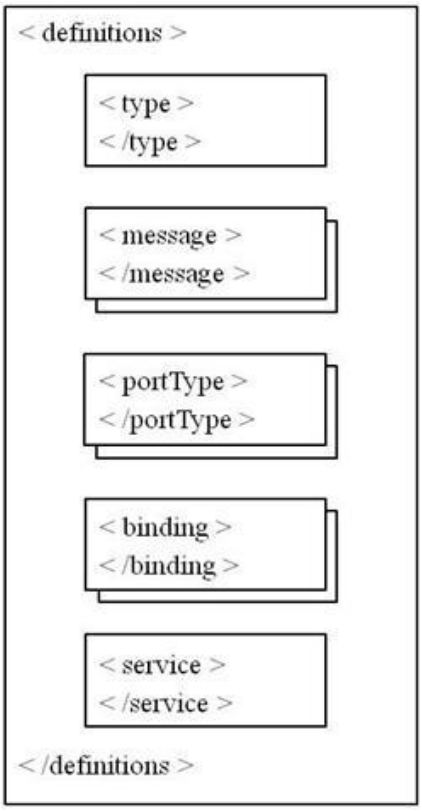

Figure 3 : Structure d'un fichier WSDL

Un document WSDL peut être présenté schématiquement de la manière suivante :

1. Le premier bloc permet de définir les types de données qui seront utilisés dans les messages. En général, la spécification XML Schéma est utilisée pour définir ces types.
2. Le second bloc permet de définir de manière abstraite les messages qui seront échangés entre les nœuds de communication. Un message est un acte de communication unique entre le client et le prestataire (requête) ou le prestataire et le client (réponse). On associe à ces messages des parties logiques (balise part) qui correspondent aux informations véhiculées par le message.
3. Le troisième bloc permet de définir des types de port et des opérations associées. Un type de port est un ensemble d'opérations abstraites. Pour chaque opération abstraite, les messages impliqués dans

l'opération sont précisés. Ce sont souvent un message de requête et un message de réponse associés éventuellement à plusieurs messages d'erreur.

4. Le quatrième bloc permet de définir les liaisons entre les opérations définies dans un type de port et les protocoles de transport et formats de messages qui prendront en charge les échanges.
5. Le dernier bloc permet de définir le service. Un service contient un ou plusieurs ports. Un port est un point de terminaison identifié de manière unique par la combinaison d'une adresse Internet et d'une liaison. Chaque port permet d'associer à une liaison (ou un binding) la localisation du service.

Un document WSDL peut donc être découpé en 3 parties :

- une partie de définition des types de données utilisés (bloc 1) ;
- une partie de définition abstraite des opérations qui contient les blocs <message>…</message> et <portType>…</portType> (blocs 2 et 3) ;
- une partie décrivant l'implémentation concrète du service, constituée des blocs <binding>…</binding> et <service>…</service> (blocs 4 et 5).

Les deux premières parties définissent l'interface abstraite. Celle-ci définit, de manière abstraite et indépendante du langage, l'ensemble des opérations et des messages qui peuvent être transmis vers et à depuis un service web donné. La troisième partie définit l'implémentation concrète des messages.

Ce découpage permet, entre autres, d'avoir une même définition abstraite pour plusieurs implémentations concrètes.

Chaque interface de service est associée à un type de port abstrait WSDL :

- Un portType regroupe un ensemble d'opérations abstraites :

  Exemple pour une transaction d'un service de type partage de documents médicaux

```
<portType name="DocumentRepository_PortType">
  <operation name="DocumentRepository_ProvideAndRegisterDocumentSet-b">
    …….
  </operation>
  <operation name="DocumentRepository_RetrieveDocumentSet">
    …….
  </operation>
</portType>
```

- Pour chaque opération, le message de requête et de réponse est défini en entrée et en sortie de l'opération :

  Exemple pour une transaction d'un service de type partage de documents médicaux

```
<portType name="DocumentRepository_PortType">
   <operation name="DocumentRepository_ProvideAndRegisterDocumentSet-b">
     <input message="ihe:ProvideAndRegisterDocumentSet-b_Message"
wsaw:Action="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b"/>
     <output message="ihe:ProvideAndRegisterDocumentSet-bResponse_Message"
wsaw:Action="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-bResponse"/>
   </operation>
</portType>
```

À noter que l'utilisation de la valeur « urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b » dans l'élément Action de l'entête des messages SOAP n'est pas obligatoire. Ceci s'applique à l'ensemble des exemples dans ce document utilisant cette valeur.

- Pour chaque message utilisé dans une opération, un élément <message> est défini. Cet élément référence un message du protocole de requête ou de réponse, conformément au schéma XML de l'interface de service utilisée par le système cible :

  Exemple pour une transaction d'un service de type partage de documents médicaux

```
<message name="ProvideAndRegisterDocumentSet-b_Message">
  <documentation>Provide and Register Document Set</documentation>
  <part name="body" element="ihe:ProvideAndRegisterDocumentSetRequest"/>
</message>
<message name="ProvideAndRegisterDocumentSet-bResponse_Message">
  <documentation>Provide And Register Document Set Response</documentation>
  <part name="body" element="rs:RegistryResponse"/>
</message>
```

- Chaque PortType fait l'objet d'une implémentation concrète sur un protocole de message et un protocole de transport ;
  Le style d'encodage littéral est précisé pour les paramètres d'entrée et de sortie de chaque opératio
  Pour le transport de document, le style d'encodage «document» indique que les requêtes/réponses au format SOAP sont traitées comme un document XML et non pas comme un appel RPC :

  Exemple pour une transaction d'un service de type partage de documents médicaux avec transport de document

```
<binding name="DocumentRepository_Binding_Soap12"
type="ihe:DocumentRepository_PortType">
<soap12:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <operation name="DocumentRepository_ProvideAndRegisterDocumentSet-b">
  <soap12:operation soapAction="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b"/>
    <input>
      <soap12:body use="literal"/>
    </input>
    <output>
      <soap12:body use="literal"/>
    </output>
  </operation>
</binding>
```

- Définition du service et de ses points d'accès :

Exemple pour une transaction d'un service de type partage de documents médicaux

```
<service name="DocumentRepository_Service">
  <port name="DocumentRepository_Port_Soap11"
binding="ihe:DocumentRepository_Binding_Soap11">
    <soap:address location="http://servicelocation/DocumentRepository_Service"/>
  </port>
  <port name="DocumentRepository_Port_Soap12"
binding="ihe:DocumentRepository_Binding_Soap12">
    <soap12:address location="http://servicelocation/DocumentRepository_Service"/>
  </port>
</service>
```

Dans le cas des SIS français, chaque système cible offrant des services doit publier les WSDL correspondant aux services offerts en suivant le standard WSDL 1.1.

4. DISPOSITIONS DE SECURITE

4.1. Confidentialité

La confidentialité des échanges au niveau du transport est gérée par l'encapsulation du flux dans une connexion sécurisée TLS.

4.2. Intégrité

L'intégrité des échanges au niveau du transport est gérée par l'encapsulation du flux dans une connexion sécurisée TLS.

4.3. Identification et authentification

Les échanges se font entre :

- le système initiateur, qui fournit les informations d'identification et d'authentification des utilisateurs nécessaires au contrôle d'accès ;
- le système cible, qui met en œuvre le contrôle d'accès (ex. détermination des autorisations d'accès en fonction des droits accordés à l'utilisateur localement) en fonction des informations transmises par le système initiateur.

La transmission de l'identification et de l'authentification se fait par l'utilisation d'une assertion formalisée nommée VIHF[1] décrite ci-dessous

L'authentification d'un utilisateur peut être gérée :

- de façon décentralisée ; chaque système cible est alors responsable de l'authentification des utilisateurs se connectant depuis un système initiateurs ;
- de façon centralisée avec un portail d'authentification qui valide l'identité et les données complémentaires des utilisateurs des systèmes initiateurs puis diffuse au système cible les éléments nécessaires à la mise en œuvre du contrôle d'accès.

Ces deux types d'architecture d'authentification s'appuient sur des modes d'utilisation de SAML différents et donc sur des types de VIHF différents décrits spécifiquement dans les sections suivantes ; section 4.3.1.1 à section 4.3.1.7 pour l'authentification gérée de façon décentralisée et section 4.3.1.8 et suivantes pour l'authentification gérée de façon centralisée.

4.3.1. VIHF

Le Vecteur d'Identification et d'Habilitation Formelles (VIHF) présente un modèle organisationnel et technique définissant les standards, formats et protocoles applicables pour la sécurisation des échanges de données avec les SIS.

Ce document présente la seconde version du VIHF : le VIHF 2.0.

Celui-ci a pour objectif de présenter une standardisation des moyens techniques pour accéder aux données, tout en prenant en compte la diversité des politiques de sécurité applicables, des environnements techniques des utilisateurs, des architectures d'authentification et des contextes d'utilisation.

Dans le modèle du VIHF 2.0, le système cible effectue les contrôles d'accès en fonction de règles et de droits définis localement.

Les prochaines versions du VIHF répondront à d'autres besoins comme, par exemple, la centralisation des droits des utilisateurs des SISP.

[1] Vecteur d'Identification et d'Habilitation Formelles

Le VIHF tient compte du profil IHE XUA dans sa version complète incluant l'extension d'attribut XUA++. Cependant, pour des raisons opérationnelles et en particulier de performance, il ne met pas en œuvre l'intégralité des spécifications XUA, en particulier en ce qui concerne la signature de l'assertion. Afin d'aider les développeurs de produits mettant en œuvre ce volet à atteindre la conformité à XUA, les prérequis XUA sont signalés dans la description du VIHF et l'annexe 3 dans la section 0 en présente une synthèse.

4.3.1.1. Les configurations possibles pour les systèmes initiateurs utilisant le VIHF en architecture d'authentification décentralisée

Les configurations possibles pour le système initiateur utilisant le VIHF en architecture d'authentification décentralisée sont les suivantes :

- une configuration « authentification indirecte » :
  Le système initiateur est hébergé au sein d'une personne morale et s'authentifie auprès du système cible.
  L'utilisateur final s'authentifie localement au sein de la personne morale pour le compte de laquelle il intervient, selon des modalités définies par celle-ci. La personne morale s'authentifie sur le système cible et lui transmet les traits d'identité de l'utilisateur final qu'elle a authentifié.
- Une configuration « authentification directe » :
  Un dispositif d'authentification est utilisé pour authentifier directement l'utilisateur humain auprès du système cible, quel que soit l'endroit effectif où se trouve l'utilisateur.
- Une configuration « authentification déléguée » :
  Le système initiateur est hébergé au sein d'une personne morale à qui le système cible a délégué la responsabilité de l'authentification de l'utilisateur final.
  L'utilisateur final s'authentifie auprès de la personne morale selon des modalités fixées par le système cible. La personne morale s'authentifie sur le système cible et lui transmet les traits d'identité de l'utilisateur final qu'elle a authentifié. L'utilisateur n'intervient pas forcément pour le compte de la personne morale responsable de l'authentification qui peut être un prestataire technique.

Remarque pour les contextes d'utilisation concernant des professionnels de santé

On parle de configuration et non de situation d'exercice. En effet, ces configurations dépendent des technologies employées pour les mécanismes d'authentification et non d'une situation d'exercice pour un professionnel de santé. Ainsi, par exemple, un utilisateur exerçant au sein d'une structure de soin peut être :

- en configuration « authentification directe », s'il utilise sa CPS pour se connecter directement à un système cible ;
- en configuration « authentification indirecte », s'il s'authentifie localement et que la connexion au système cible est réalisée à partir d'un certificat serveur de la structure ;
- en configuration « authentification déléguée », s'il s'authentifie localement avec sa CPS, que la connexion au système cible est réalisée à partir d'un certificat serveur de la structure et si le système cible a délégué l'authentification à la structure avec comme contrainte d'authentifier localement les utilisateurs avec leurs CPS.

4.3.1.2. Fonctionnement général des échanges intégrant le VIHF en architecture d'authentification décentralisée

Le principe de fonctionnement est le suivant :

- les connexions entre le système initiateur et le système cible sont sécurisées par des connexions TLS pour assurer la confidentialité des échanges SOAP ;
- chaque requête SOAP émise par le système initiateur est accompagnée d'un VIHF sous la forme d'une assertion SAML ; cette assertion contient l'identité de l'utilisateur et les éléments nécessaires à la détermination des habilitations par le système cible, pour chacune des requêtes applicatives ;
- les mécanismes d'authentification sont différenciés selon la configuration :
- en configuration « authentification indirecte », l'authentification est effectuée par le système cible à partir de l'utilisation d'un dispositif d'authentification lié à la personne morale responsable du système initiateur ;
- en configuration « authentification directe », l'authentification est effectuée par le système cible à partir d'un dispositif d'authentification lié à la personne physique utilisant le système initiateur ;
- en configuration « authentification déléguée », l'authentification est effectuée par le système cible à partir de l'utilisation d'un dispositif d'authentification lié à la personne morale à laquelle il a délégué l'authentification de la personne physique utilisant le système initiateur.

4.3.1.2.1. Fonctionnement pour la configuration « authentification indirecte »

Dans cette configuration, l'utilisateur final s'authentifie au sein du système d'information de la personne morale dont il utilise le système d'information.

Les échanges réalisés avec le système cible sont réalisés par des applications hébergées au sein de la personne morale à laquelle l'utilisateur a délégué la responsabilité des échanges.

Cette responsabilité est matérialisée par l'utilisation d'un dispositif d'authentification assigné à la personne morale, pour assurer l'authentification et la sécurisation des échanges.

La sécurisation des échanges avec le système cible peut se faire sur deux plans présentés ci-dessous. Le choix des mécanismes de sécurité à mettre en œuvre et des configurations à utiliser pour chacun est de la responsabilité du système cible, en fonction de son analyse de risques, de sa politique de sécurité en découlant et des caractéristiques de « l'authentification indirecte ».

1) Sur le plan des connexions entre le système d'information de la personne morale et le système cible

Les connexions sont établies entre le système d'information de la personne morale et le service cible en TLS. Le système cible définit la version de TLS à utiliser en fonction de son analyse de risques, sa politique de sécurité en découlant et suivant les besoins en confidentialité et d'imputabilité identifiés et les caractéristiques de « l'authentification indirecte ».

Ces connexions sont utilisées pour tous les échanges applicatifs entre la personne morale et le système cible. Selon la politique de sécurité du système cible, elles peuvent être ré-utilisées pour les échanges applicatifs de plusieurs utilisateurs, voire de plusieurs applications.

2) Sur le plan des échanges applicatifs

Les échanges entre le système initiateur et le système cible s'effectuent sur SOAP. Tous les échanges identifient un utilisateur final, qui est identifié dans un jeton VIHF contenant son identifiant (local ou national), l'identifiant de la personne morale pour laquelle il intervient, ainsi que des données complémentaires dont le détail est donné dans les différents profils du VIHF décrites dans la section 4.3.1.5.

En fonction de ses besoins, le système cible peut réaliser son contrôle d'accès en partie ou totalement sur :

- tout ou partie des informations du jeton VIHF,
- le service appelé et la politique d'accès associée.

En fonction de son analyse de risques, de la politique de sécurité en découlant et des caractéristiques de « l'authentification indirecte », le système cible peut identifier des mécanismes de sécurité complémentaires à mettre en œuvre (ex. profil WS-Security avec ou sans signature).

La figure 4 résume la cinématique présentée.

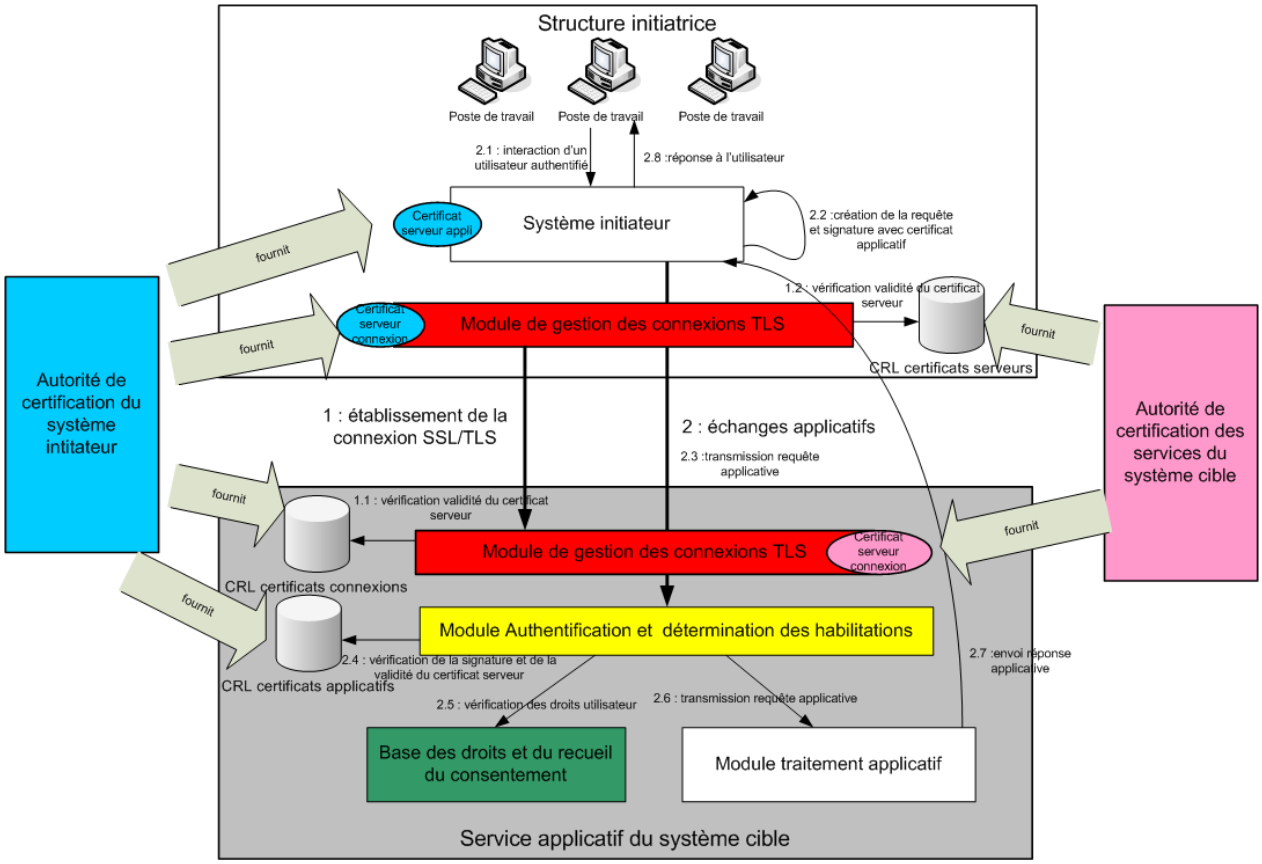

Figure 4 : Cinématique d'échange en authentification indirecte

4.3.1.2.2. Fonctionnement pour la configuration « authentification directe »

Dans cette configuration, l'utilisateur final s'identifie et s'authentifie directement sur le système cible. par l'intermédiaire du VIHF.

La sécurisation des échanges avec le système cible peut se faire sur deux plans présentés ci-dessous. Le choix des mécanismes de sécurité à mettre en œuvre et des configurations à utiliser pour chacun est de la responsabilité du système cible, en fonction de son analyse de risques, sa politique de sécurité en découlant et des caractéristiques de « l'authentification directe ».

1) Sur le plan des connexions entre le système d'information de l'utilisateur final et le système cible

Les connexions sont établies entre le système d'information de l'utilisateur final et le service cible en TLS. Le système cible définit la version de TLS à utiliser en fonction de son analyse de risques, sa politique de sécurité en découlant suivant les besoins en confidentialité et d'imputabilité identifiés et les caractéristiques de « l'authentification directe ».

2) Sur le plan des échanges applicatifs

Les échanges entre le système initiateur et le système cible s'effectuent sur SOAP. Tous les échanges identifient un utilisateur final, qui est identifié dans un jeton VIHF contenant son identifiant (local ou national), le cas échéant l'identifiant de la personne morale pour laquelle il intervient, ainsi que des données complémentaires décrites dans la section 4.3.1.5.

En fonction de ses besoins en contrôle d'accès, le système cible peut baser ses décisions d'accès en partie ou totalement sur :

- tout ou partie des informations du jeton VIHF,
- le service appelé et la politique d'accès associée.

En fonction de son analyse de risques, de la politique de sécurité en découlant et des caractéristiques de « l'authentification directe », le système cible peut identifier des mécanismes de sécurité complémentaires à mettre en œuvre (ex. profil WS-Security avec ou sans signature).

4.3.1.2.3. Fonctionnement pour la configuration « authentification déléguée »

Dans cette configuration, l'utilisateur final s'authentifie sur le système d'information d'une personne morale à laquelle le système cible a délégué l'authentification de l'utilisateur final. Les dispositifs utilisables pour cette authentification sont définies par le système cible.

La sécurisation des échanges avec le système cible peut se faire sur deux plans présentés ci-dessous. Le choix des mécanismes de sécurité à mettre en œuvre et des configurations à utiliser pour chacun est de la responsabilité du système cible, en fonction de son analyse de risques, de sa politique de sécurité en découlant et des caractéristiques de « l'authentification déléguée ».

1) Sur le plan des connexions entre le système d'information de la personne morale et le système cible

Les connexions sont établies entre le système d'information de la personne morale et le service cible en TLS. Le système cible définit la version de TLS à utiliser en fonction de son analyse de risques, sa politique de sécurité en découlant et suivant les besoins en confidentialité et d'imputabilité identifiés et les caractéristiques de « l'authentification déléguée ».

Ces connexions sont utilisées pour tous les échanges applicatifs entre la personne morale et le système cible. Selon la politique de sécurité du système cible, elles peuvent être ré-utilisées pour les échanges applicatifs de plusieurs utilisateurs, voire de plusieurs applications.

2) Sur le plan des échanges applicatifs

Les échanges entre le système initiateur et le système cible s'effectuent sur SOAP. Tous les échanges identifient un utilisateur final, qui est identifié dans un jeton VIHF contenant son identifiant, l'identifiant de la personne morale pour laquelle il intervient[2], ainsi que des données complémentaires décrites dans la section 4.3.1.5.

En fonction de ses besoins, le système cible peut réaliser son contrôle d'accès en partie ou totalement sur :

- tout ou partie des informations du jeton VIHF,
- le service appelé et la politique d'accès associée.

En fonction de son analyse de risques, de la politique de sécurité en découlant et des caractéristiques de « l'authentification déléguée », le système cible peut identifier des mécanismes de sécurité complémentaires à mettre en œuvre (ex. profil WS-Security avec ou sans signature). Il peut également conditionner la délégation de l'authentification à la mise en œuvre d'objectifs de sécurité par la personne morale à laquelle il délègue l'authentification. Les conditions de mise en œuvre d'une authentification déléguée sont détaillées dans le référentiel d'authentification des acteurs de santé [6].

[2] qui peut être différente de la personne morale à qui a été déléguée l'authentification.

4.3.1.3. Section laissée vide intentionnellement

4.3.1.4. Section laissée vide intentionnellement

4.3.1.5. Contenu du jeton VIHF en architecture d'authentification décentralisée

Un jeton VIHF (assertion de sécurité sous la forme d'un jeton SAML 2.0) est émis à chaque requête du système initiateur vers le système cible, pour transmettre des informations nécessaires à la validation de l'authentification et à la détermination de ses droits d'accès.

Le contenu du jeton VIHF est dépendant de la configuration utilisée (directe, indirecte ou déléguée), du contexte d'utilisation et du dispositif d'authentification utilisé pour authentifier l'utilisateur final. Le contenu du jeton VIHF est également dépendant des choix de la politique de sécurité du service cible qui peut compléter les spécifications présentées dans ce document par des contraintes complémentaires en termes d'éléments à intégrer dans le VIHF ou de valeurs admises pour chacun de ces éléments. En particulier, le système cible peut imposer ou non la présence d'une signature du jeton conforme au standard SAML 2.0[3].

En plus des champs SAML standards, des profils applicatifs VIHF spécifiques sont définis pour véhiculer les informations nécessaires à la mise en œuvre du contrôle d'accès. Ces informations peuvent être issues :

- du dispositif d'authentification utilisé ;
- du SI qui émet l'assertion ;
- de l'utilisateur directement.

Les éléments sur lesquels un système cible peut se baser pour effectuer les contrôles d'accès diffèrent selon le périmètre du système cible. Par exemple, un système cible implémentant un dossier médical a besoin de l'identifiant du patient pour déterminer si un professionnel de santé est habilité ou non à consulter le dossier, en revanche, un système cible implémentant un annuaire de professionnels de santé n'a pas besoin d'identifiant patient pour déterminer les droits d'accès.

Afin de refléter ces différences, un profil générique de VIHF est fourni. Ce profil est ensuite instancié par contexte d'utilisation afin de le restreindre aux éléments spécifiques à chaque contexte d'utilisation.

Les contextes d'utilisation identifiés dans la présente version de ce volet sont :

- dossier médical ;
- annuaire.

Cette liste n'est pas exhaustive et d'autres contextes d'utilisation pourront être identifiés dans des versions ultérieures du présent volet. Chaque contexte donnera lieu à un profil spécifique du VIHF décrit dans la section suivante.

Le profil générique décrit une assertion SAML qui doit être acceptée par tout SIS cible mettant en œuvre ce volet (i.e. ne pas générer d'erreur même s'il ne traite pas certains champs du VIHF). Dans les sections suivantes, il est instancié par contexte d'utilisation portant des contraintes supplémentaires.

[3] Il est également à noter que la signature de l'assertion est un prérequis XUA comme rappeler dans l'annexe 3 de la section 0.

Les autres facteurs de variation dans le contenu du VIHF, à savoir :

- la configuration utilisée (indirecte, directe ou déléguée) ;
- le type d'utilisateur final (professionnel de santé, dispositif, personnel administratif ou patient) ;
- le type de dispositif utilisé pour authentifié l'utilisateur final en authentification directe (certificat électronique ou identifiant/mot de passe + OTP[4]) ;

sont présentés, le cas échéant, dans le profil générique ou les instanciations par contexte s'ils induisent des spécificités dans l'alimentation des champs du VIHF.

Afin de faciliter la lecture, les spécificités de contenu sont présentées pour chaque champ sous la forme d'un tableau intégré après la description générique du contenu du champ.

4.3.1.5.1. Champs standards du profil générique

Les attributs de l'objet racine « *Assertion* » requis dans SAML 2.0 doivent être renseignés, en particulier, les attributs *@Version*, *@ID* et *@IssueInstant*.

Les champs SAML standards suivants doivent être renseignés dans l'objet *Assertion* par le système initiateur. Les champs sont tous requis à l'exception du champ *AudienceRestriction*.

4.3.1.5.1.1. /Assertion/Issuer

Ce champ doit contenir l'identité de l'émetteur de l'assertion.

Configuration utilisée	Valeur du champ Issuer et de l'attribut Issuer/@Format
Authentification directe via certificat électronique	DN du certificat électronique de l'utilisateur final. Issuer/@Format = 'urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName'
Authentification directe via identifiant/mot de passe + OTP	Identifiant de l'instance du logiciel utilisé tel que renseigné dans le champ LPS_ID. L'attribut Issuer/@Format n'est pas utilisé.
Authentification indirecte	DN du certificat électronique de la personne morale pour le compte de laquelle intervient l'utilisateur final. Issuer/@Format = 'urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName'
Authentification déléguée	DN du certificat électronique de la personne morale à laquelle le système cible à délégué l'authentification. Issuer/@Format = 'urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName'

Format :

Chaine alphanumérique.

Dans le cas où le champ contient un DN, sa structure doit être conforme à la spécification RFC 2253 « UTF-8 String Representation of Distinguished Names » de Décembre 1997.

Rappel des règles de la RFC 2253 :

- Les RDN (chaînes séparées par des ",") doivent apparaître dans l'ordre inverse du certificat.

[4] Dispositifs d'authentification publique décrits dans le référentiel d'authentification des acteurs de santé [6]. D'autres dispositifs d'authentification pourront être pris en compte en fonction des évolutions de ce référentiel.

- L'ordre des attributs à l'intérieur d'un RDN multi-valué (les chaînes séparées par des "+") est quant à lui indifférent.

Exemple DN d'un PS médecin :
CN=801234567890+SN=DUPONT+GN=JEAN,OU=Médecin,O=GIP-CPS,C=FR

Exemple DN d'un employé d'une personne morale référencé dans FINESS :
CN=3750100125/0001+SN=DUPONT+GN=JACQUES,OU=1750100125,L=Paris (75),O=GIP-CPS,C=FR

Source :

Configuration utilisée	Source du champ Issuer
Authentification directe via certificat électronique	Si le VIHF est signé, prendre le DN présent dans le certificat X509 de signature, sinon prendre le DN issu du certificat X.509 d'authentification ayant initié la connexion TLS.
Authentification directe via identifiant/mot de passe + OTP	A renseigner par le logiciel utilisé
Authentification indirecte	Si le VIHF est signé, prendre le DN présent dans le certificat X509 de signature, sinon prendre le DN issu du certificat X.509 d'authentification ayant initié la connexion TLS.
Authentification déléguée	Si le VIHF est signé, prendre le DN présent dans le certificat X509 de signature, sinon prendre le DN issu du certificat X.509 d'authentification ayant initié la connexion TLS.

4.3.1.5.1.2. /Assertion/Subject/NameID

Ce champ doit contenir l'identifiant de l'utilisateur final envoyé par le système initiateur.

Utilisateur final	Valeur du champ NameID
Professionnel de santé, personnel administratif et dispositif	Identifiant du professionnel constitué selon les principes décrits dans l'annexe [4], sous le nom « **PS_IdNat** ».
Patient	Identifiant du patient au format CX de HL7 v2.5. Pour une connexion à des services de partage de documents de santé, les identifiants utilisables sont définis par le système cible en accord avec le cadre juridique. Les composants 1, 4 et 5 sont requis. Composant 1 - Identifiant Ce composant contient l'identifiant du patient. Composant 4 - Autorité d'affectation Identifiant de l'autorité d'affectation de l'identifiant utilisé : ► 1er sous-composant : Namespace ID (IS) = vide ► 2ème sous-composant : Universal ID (ST) : valeur de l'OID de l'autorité d'affectation de l'identifiant (pour l'INS, l'OID à utiliser est à sélectionner dans la liste des OID des autorités d'affectation des INS dans [5]) ► 3ème sous-composant : Universal ID type (ID) = "ISO" Composant 5 – Type d'identifiant Code du type d'identifiant tel que défini dans [5]. « NH » pour les patients identifiés avec leur INS tel que défini dans le cadre juridique. Exemple pour l'INS : 124018852493334^^^&1.2.250.1.213.1.4.8&ISO^NH

Ce champ est obligatoire, à l'exception des échanges initiaux entre le système initiateur et le système cible avant attribution du jeton de session dans le cas d'une authentification directe par identifiants/mot de passe + OTP.

Format :

Chaîne alphanumérique

Source :

Configuration utilisée	Source du champ NameID
Authentification directe via certificat électronique	Lecture du certificat de l'utilisateur final. Les modalités d'accès à cette information pour les cartes CPx sont spécifiées dans l'annexe [4], sous le nom « **PS_IdNat** ». Pour les pharmaciens ne disposant pas de cartes CPS ou CPF mais de cartes CPE, se reporter, pour ce cas particulier au paragraphe 4.3.1.5.4.
Authentification directe via identifiant/mot de passe + OTP	A renseigner par le logiciel utilisé.
Authentification indirecte	A renseigner par le logiciel utilisé.
Authentification déléguée	A renseigner par le logiciel utilisé.

4.3.1.5.1.3. /Assertion/AuthnStatement/AuthnContext/AuthnContextClassRef

Le champ doit référencer la méthode d'authentification de l'utilisateur dans le système qui produit l'assertion SAML (système initiateur), il ne s'agit pas du mode d'authentification sur le système cible.

Configuration utilisée	Valeur du champ AuthnContextClassRef
Authentification directe via carte CPx	*'urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI'*
Authentification directe via certificat électronique logiciel	*'urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI'*
Authentification directe via identifiant/mot de passe + OTP	*'urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered'*
Authentification indirecte	Valeur à sélectionner dans la nomenclature définie pour SAML 2.0 dans le document *saml-authn-context-2.0-os* [5] du standard en fonction de l'authentification locale de l'utilisateur final mise en œuvre. Les valeurs possibles pour ce champ peuvent être restreintes par le système cible en fonction de son analyse de risques et de sa politique de sécurité en découlant.
Authentification déléguée	Valeur à sélectionner dans la nomenclature définie pour SAML 2.0 dans le document *saml-authn-context-2.0-os* [6] du standard en fonction de l'authentification locale de l'utilisateur final mise en œuvre. Les dispositifs d'authentification utilisable pour l'authentification de l'utilisateur final et donc les valeurs possibles pour ce champ sont à lister explicitement par le système cible qui délègue l'authentification.

Format :

Chaîne alphanumérique.

[5] saml-authn-context-2.0-os : http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

[6] saml-authn-context-2.0-os : http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

Source :

A renseigner par le logiciel utilisé.

4.3.1.5.1.4. /Assertion/AuthnStatement@AuthnInstant

Cet attribut doit référencer la date et l'heure exprimée en temps universel coordonné (UTC).à laquelle l'authentification a été réalisée par le système produisant l'assertion SAML (système initiateur).

4.3.1.5.1.5. /Assertion/Conditions/AudienceRestriction

Pour assurer la compatibilité avec la version 1.0 du VIHF, ce champ est optionnel dans le CI-SIS. Il est cependant à noter que le profil « Cross-Enterprise User Assertion » d'IHE dans sa version finale impose l'utilisation de ce champ.

S'il est utilisé, ce champ contient un champ *Audience* qui contient l'URI du service cible pour lequel l'assertion a été élaborée, ses conditions d'usage et les éventuelles contraintes sur le VIHF (ou l'absence de contraintes complémentaires par rapport au CI-SIS).

Format :

URI comportant un OID (i.e. urn :oid :XXX.YYY.ZZZ où XXX.YYY.ZZZ est l'OID de l'objet référencé).

Source :

A renseigner par le logiciel utilisé.

4.3.1.5.1.6. Assertion/Conditions/@NotBefore et Assertion/Conditions/@NotOnOrAfter

L'attribut *NotBefore* contient la date et l'heure exprimées en temps universel coordonné (UTC) de constitution de l'assertion SAML qui correspond à son début de validité.

L'attribut *NotOnOrAfter* contient la date et l'heure exprimées en temps universel coordonné (UTC) de fin de validité de l'assertion.

La différence entre les deux valeurs donne la durée de vie du jeton. Le système cible peut déterminer une durée de vie maximum acceptable, qui peut être éventuellement réduite par le système émetteur.

Si le jeton est signé, alors la valeur de *NotBefore* ne doit pas être postérieure à la date de la signature, la date de signature représentant l'étape finale de constitution de l'assertion.

Format :

xs:dateTime

Source :

A renseigner par le logiciel utilisé.

4.3.1.5.2. Champs complémentaires du profil générique

Les champs complémentaires sont des champs <saml:Attribute> situés dans la balise <saml:AttributeStatement> du jeton SAML. Afin d'aider les développeurs de produits mettant en œuvre ce volet à atteindre la conformité à XUA, les champs issus du profil XUA sont signalés dans la colonne description. En particulier, deux champs provenant du profil XUA ont été ajoutés à la version 2.0 du VIHF pour alignement avec le profil alors que les informations contenues dans ces champs sont également renseignés dans des champs du VIHF version 1.0 qui ont été conservés dans la version 2.0. Les champs non XUA provenant de la version 1.0 seront supprimés dans une version ultérieure du VIHF.

Pour des raisons de compatibilité avec l'existant, les éléments complémentaires ajoutés dans les versions 2.0 et ultérieures du VIHF sont optionnels pour les configurations supportées par la version 1.0 du VIHF (i.e. authentification directe via certificat électronique et authentification indirecte). Pour mémoire, le tableau récapitulatif des optionalités de la V1.0 du VIHF est rappelé en annexe 2. Par ailleurs, la colonne version d'origine du tableau ci-dessous indique à partir de quelle version un champ a été intégré dans le VIHF.

Les champs complémentaires du profil générique sont les suivants :

Champ	Requis /Optionnel	Description	Version d'origine
VIHF_Version	R	Version du VIHF utilisée	1.0
urn:oasis:names:tc:xacml:2.0:subject:role	O	*Champ issu d'une option du profil XUA.* Rôle fonctionnel de l'utilisateur, éventuellement multi-valué	1.0
Secteur_Activite	O	Secteur d'activité dans lequel exerce l'utilisateur	1.0
urn:oasis:names:tc:xacml:2.0:resource:resource-id	O	*Champ issu d'une option du profil XUA.* Identifiant du patient concerné par la requête	1.0
Ressource_URN	R	Ressource visée par l'utilisateur.	1.0
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	O	*Champ issu d'une option du profil XUA.* Mode d'accès demandé par l'utilisateur (normal ou accès exceptionnel[7]). Valeur par défaut = normal	1.0
Mode_Acces_Raison	O	Explication de la raison de l'usage d'un accès exceptionnel	1.0
urn:oasis:names:tc:xspa:1.0:subject:subject-id	O	*Champ issu d'une option du profil XUA.* Identité de l'utilisateur (ex. nom, prénom et/ou service)	1.0
Identifiant_Structure	O	Identifiant de la personne morale depuis le SI de laquelle la requête est émise.	1.0
LPS_Nom	O	Nom du logiciel utilisé	1.0
LPS_Version	O	Version du logiciel utilisé	1.0
LPS_ID	O	Numéro de série ou identifiant de l'installation du logiciel	1.0
Profil_Utilisateur	O	Profil d'accès au système cible	2.0
Profil_Utilisateur_Perimetre	O	Périmètre d'application du Profil_utilisateur	2.0
Authentification_Mode	R en authentification déléguée ou en authentification directe via identifiant / mot de passe + OTP O sinon	Mode d'authentification (directe, indirecte ou déléguée). Si absent, le mode d'authentification est déduit à partir du certificat utilisé pour monter la connexion internet	2.0

[7] Cf. l'assertion pour un contexte d'utilisation « dossier médical patient » pour un exemple d'accès exceptionnel.

Champ	Requis /Optionnel	Description	Version d'origine
JSESSIONID	R en authentification directe via identifiant / mot de passe + OTP O sinon	Identifiant de session utilisé dans le cas d'une authentification directe par identifiant/mot de passe + OTP	2.0
urn:oasis:names:tc:xspa:1.0:subject:npi	O	*Champ issu du profil XUA.* Lorsque l'utilisateur est un professionnel de santé, identifiant du professionnel de santé contenant la même valeur que le champ Assertion/Subject/NameID	2.0
urn:oasis:names:tc:xspa:1.0:subject:organization-id	O	*Champ issu du profil XUA.* Identifiant de la personne morale contenant la même valeur que le champ complémentaire Identifiant_Structure	2.0
VIHF_Profil	O	Profil spécifique utilisé. Si absent, le profil utilisé est le profil pour contexte d'utilisation « accès à un dossier médical »	2.0
PSI_Locale	O	En authentification indirecte ou déléguée : identifiant de la politique de sécurité mise en œuvre dans le cadre de l'authentification locale de l'utilisateur. Non utilisé en authentification directe	3.0
Palier_Authentification	O	Palier du référentiel d'authentification auquel se situe l'authentification locale de l'utilisateur mise en œuvre. Non utilisé en authentification directe	3.0
urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code	O	Restriction d'audience à appliquer aux traces générées par la transaction objet du flux	3.0

4.3.1.5.3. Formats et valeurs des champs complémentaires du jeton VIHF pour le profil générique

4.3.1.5.3.1. VIHF_Version

Numéro de version de la spécification du VIHF. Le numéro de la version courante à utiliser est 3.0.

Format :

Numérique

4.3.1.5.3.2. urn:oasis:names:tc:xacml:2.0:subject:role

Rôle fonctionnel de l'utilisateur final. Le champ « subject :role » peut être multi-valué si un rôle nécessite d'être précisé pour permettre la mise en œuvre des droits d'accès.

Les valeurs possibles pour ce champ doivent être un code provenant d'une des terminologies de référence suivantes :

- TRE_A00-ProducteurDocNonPS, OID : 1.2.250.1.213.1.1.4.6
- TRE_G15-ProfessionSante, OID : 1.2.250.1.71.1.2.7
- TRE_G16-ProfessionFormation, OID : 1.2.250.1.71.1.2.8
- TRE_R01-EnsembleSavoirFaire-CISIS, OID : 1.2.250.1.71.4.2.5
- TRE_G05-SousSectionTableauCNOP, OID : 1.2.250.1.71.4.2.6

Les valeurs possibles peuvent être restreintes en fonction du jeu de valeurs correspondant mis à disposition par le projet.

En l'absence de spécifications complémentaires, le jeu de valeurs JDV_J05-SubjectRole-CISIS peut être utilisé.

Utilisateur final	Valeur du champ « subject :role »
Professionnel de santé	**La première occurrence** doit contenir pour : ► un PS : le code et le displayName de sa profession suivi du codeSystem (OID), ► un PF : le code et le displayName de sa future profession suivi du codeSystem (OID), **La deuxième occurrence** n'est renseignée que pour les médecins et les pharmaciens (absente pour tous les autres subjects), elle doit contenir pour : ► un médecin : le code et le displayName de sa spécialité de qualification ou d'un autre savoir-faire correspondant au contexte au moment de l'élaboration du jeton, suivi du codeSystem (OID), ► un pharmacien : le tableau de pharmacien et le displayName correspondant au contexte au moment de l'élaboration du jeton, suivi du codeSystem (OID).
Personnel administratif, dispositif et patient	**Une seule occurrence** contenant le code et le displayName correspondant au subject (patient, dispositif, secrétariat, ...) suivi du codeSystem (OID)

Format :

Type de donnée CE d'HL7 v3

Source :

Se reporter à la spécification dans l'annexe [4], sous le paragraphe « **subjectRole** ».

Exemple pour un médecin :

```
<saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
    <saml:AttributeValue>
        <Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="10" codeSystem="1.2.250.1.71.1.2.7" displayName="Médecin"/>
    </saml:AttributeValue>
    <saml:AttributeValue>
        <Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="SM54" codeSystem="1.2.250.1.71.4.2.5" displayName="Médecine Générale (SM)"/>
    </saml:AttributeValue>
</saml:Attribute>
```

4.3.1.5.3.3. Secteur_Activite

Secteur d'activité dans lequel exerce l'utilisateur final.

Utilisateur final	Valeur du champ « Secteur_Activite »
Professionnel de santé, personnel administratif, dispositif	Code du secteur d'activité suivi de l'OID de la nomenclature utilisée
Patient	Champ non utilisé

Les valeurs possibles pour ce champ proviennent de la nomenclature « R02 – Secteur d'activité RPPS » dont l'OID est 1.2.250.1.71.4.2.4

Format :

Code^OID

Source :

A renseigner par le logiciel utilisé.

Dans le cas où une carte CPx est utilisée, se reporter à la spécification dans l'annexe [4], sous le paragraphe « **Présence des données dans le SI-CPS** ».

4.3.1.5.3.4. urn:oasis:names:tc:xacml:2.0:resource:resource-id

L'usage de ce champ est issu de la recommandation du supplément au Technical Framework IHE nommé « Cross-Enterprise User Assertion » et concerne l'identification du patient si nécessaire. Se référer aux contextes d'utilisation traitant des données patients pour une description plus détaillée de ce champ.

4.3.1.5.3.5. Ressource_URN

Identification du service utilisé

Format :

URN[8] constitué selon les règles indiquées ci-dessous.

urn:{cible}

où {cible} identifie la ressource cible (le service utilisé).

Pour les services concernant un objet particulier dans la cible :

urn:{cible}:{identifiant objet cible}

4.3.1.5.3.6. urn:oasis:names:tc:xspa:1.0:subject:purposeofuse

Mode d'accès au service en particulier si le service accepte des modes d'accès exceptionnels tels que le mode « bris de glace ».

Les valeurs possibles pour ce champ doivent être un code provenant de la terminologie de référence suivante :

- TRE_R248_ModeAcces, OID : 1.2.250.1.213.1.1.4.336

Les valeurs possibles peuvent être restreintes en fonction du jeu de valeurs correspondant mis à disposition par le projet.

En l'absence de spécifications complémentaires, le jeu de valeurs JDV_J38_ModeAcces-CISIS peut être utilisé.

Si ce champ n'est pas présent dans le VIHF, l'accès se fait en mode « normal ».

Format :

Type de donnée CE d'HL7 v3

4.3.1.5.3.7. Mode_Acces_Raison

Raison invoquée par l'utilisateur final pour l'utilisation d'un mode d'accès exceptionnel (i.e. tout mode d'accès différent du mode « normal ».

Format :

Texte libre

4.3.1.5.3.8. urn:oasis:names:tc:xspa:1.0:subject:subject-id

Identité de l'utilisateur. Ce champ n'est prévu qu'à titre informatif pour la lisibilité des traces. Son contenu est donc informatif et libre en termes de format. Il peut être spécifié par le SI Cible.

Pour un utilisateur humain : Identification explicite de l'utilisateur (ex. nom, prénom, service au sein d'une structure…).

Pour une machine (ex. dispositif de télé-monitoring) : Identification explicite de la machine (ex. nom du logiciel, nom du modèle, service au sein d'une structure…).

Format :

Texte libre

[8] Tel que défini dans la RFC 2141

Exemple :

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">
        <saml:AttributeValue>Joseph Martin – Service de pédiatrie</saml:AttributeValue>
</saml:Attribute>
```

4.3.1.5.3.9. Identifiant_Structure

Identifiant de la structure de l'utilisateur final.

Utilisateur final	Valeur du champ « Identifiant_Structure »
Professionnel de santé, personnel administratif, dispositif	Identifiant de la structure
Patient	Champ non utilisé

La valeur correspond à l'identifiant augmenté d'un préfixe qualifiant le type d'identifiant utilisé. Les préfixes possibles sont identifiés dans le tableau ci-dessous.

Identifiant de la structure
0 + Identifiant cabinet ADELI
1 + FINESS
2 + SIREN
3 + SIRET
4 + Identifiant cabinet RPPS

Note 1 : Dans le tableau, le signe + indique une concaténation du type d'identifiant et de l'identifiant lui-même (sans espace).

Note 2 : Ce composant doit être traité comme un ensemble. Il ne doit pas être interprété par les applications (pour obtenir le n° SIRET par exemple), ni être dissocié en plusieurs champs.

Format :

Chaîne alphanumérique

Source :

Se reporter à la spécification dans l'annexe [4] sous le paragraphe « **Struct_IdNat** ».

4.3.1.5.3.10. LPS_Nom

Nom du logiciel utilisé

Format :

Chaîne alphanumérique

4.3.1.5.3.11. LPS_Version

Version du logiciel utilisé

Format :

Chaîne alphanumérique

4.3.1.5.3.12. LPS_ID

Numéro de série ou identifiant de l'installation du logiciel

Pour un système cible qui en a le besoin, ce champ peut servir à tracer les différentes instances de logiciels qui y accèdent ou faire du contrôle d'accès sur ce champ.

Format :

Chaîne alphanumérique

4.3.1.5.3.13. Profil_Utilisateur

Pour les systèmes cibles le nécessitant, profil utilisateur à utiliser en complément des autres données du VIHF pour déterminer les droits d'accès au service.

Les valeurs possibles pour ce champ sont définies par les systèmes cibles.

Format :

Type de donnée CE d'HL7 v3

4.3.1.5.3.14. Profil_Utilisateur_Perimetre

Pour les systèmes cibles le nécessitant, périmètre du profil utilisateur à utiliser en complément du profil utilisateur pour déterminer les droits d'accès au service.

Les valeurs possibles pour ce champ sont définies par les systèmes cibles.

Format :

Type de donnée CE d'HL7 v3

4.3.1.5.3.15. Authentification_Mode

Indication de la configuration utilisée pour s'authentifier.

Les configurations d'authentification possibles sont définies par le système cible.

Les valeurs possibles pour ce champ doivent être un code provenant de la terminologie de référence suivante :

- TRE_R218-ModeAuthentification, OID : 1.2.250.1.213.1.1.4.323

Les valeurs possibles peuvent être restreintes en fonction du jeu de valeurs correspondant mis à disposition par le projet.

Pour assurer la compatibilité avec la version 1.0 du VIHF, si ce champ est absent, le mode d'authentification est considéré être :

- « authentification directe » si le certificat ayant initié la connexion TLS est le certificat de l'utilisateur final référencé dans le VIHF ;
- « authentification indirecte » si le certificat ayant initié la connexion TLS est un certificat serveur ou un certificat de personne morale.

Note : Ce champs est donc obligatoire dans le cas d'une authentification déléguée ou d'une authentification directe via identifiant/mot de passe + OTP.

Format :

Type de donnée CE d'HL7 v3

Exemple :

Configuration utilisée	Valeur du champ « Authentification_Mode »
Authentification directe	<saml:Attribute Name="Authentification_Mode"> <saml:AttributeValue> <Authentification_Mode xmlns="urn:hl7-org:v3" xsi:type="CE" code="DIRECTE" codeSystem="1.2.250.1.213.1.1.4.323" displayName="Authentification directe"/> </saml:AttributeValue> </saml:Attribute>
Authentification indirecte	<saml:Attribute Name="Authentification_Mode"> <saml:AttributeValue> <Authentification_Mode xmlns="urn:hl7-org:v3" xsi:type="CE" code="INDIRECTE" codeSystem="1.2.250.1.213.1.1.4.323" displayName="Authentification indirecte"/> </saml:AttributeValue> </saml:Attribute>
Authentification déléguée	<saml:Attribute Name="Authentification_Mode"> <saml:AttributeValue> <Authentification_Mode xmlns="urn:hl7-org:v3" xsi:type="CE" code="DELEGUEE" codeSystem="1.2.250.1.213.1.1.4.323" displayName="Authentification déléguée"/> </saml:AttributeValue> </saml:Attribute>

4.3.1.5.3.16. JSESSIONID

Jeton de session utilisé pour faire le lien avec la session d'un utilisateur final authentifié directement via identifiant/mot de passe + OTP.

Ce champ n'est pas à fournir qu'après authentification et uniquement dans une configuration de type authentification directe via identifiant/mot de passe + OTP. La valeur à positionner dans ce champ est fourni par le système cible au cours de la procédure d'authentification.

Format :

Chaine alphanumérique.

4.3.1.5.3.17. urn:oasis:names:tc:xspa:1.0:subject:npi

Si l'utilisateur final est un professionnel de santé, ce champ contient l'identifiant du professionnel tel que renseigné dans le champ Assertion/Subject/NameID.

Si l'utilisateur final n'est pas un professionnel de santé, ce champ n'est pas utilisé.

Ce champ est un champ obligatoire dans le profil XUA lorsque l'identifiant d'un professionnel de santé doit être véhiculé par l'assertion SAML.

Format :

Chaine alphanumérique.

4.3.1.5.3.18. urn:oasis:names:tc:xspa:1.0:subject:organization-id

Ce champ contient l'identifiant de la structure pour le compte de laquelle l'utilisateur final intervient. Les conditions d'utilisation et la valeur de ce champs sont les mêmes que celles du champ Identifiant_Structure. En particulier, ce champ n'est pas utilisé lorsque l'utilisateur final est un patient.

Ce champ est un champ obligatoire dans le profil XUA lorsque l'identifiant de la structure pour le compte de laquelle l'utilisateur final intervient doit être véhiculé par l'assertion SAML.

Format :

Chaine alphanumérique.

4.3.1.5.3.19. VIHF_Profil

Indication du contexte d'utilisation du VIHF.

L'éventuel profil à suivre est défini par le système cible.

Les valeurs possibles pour ce champ correspondent à la nomenclature des profils VIHF dont l'OID est 1.2.250.1.213.1.1.4.312.

Pour assurer la compatibilité avec la version 1.0 du VIHF, si ce champ est absent, le VIHF est considéré comme suivant le profil « accès à un dossier médical ».

Format :

Type de donnée CE d'HL7 v3

Exemple :

Pour un VIHF ne suivant que le profil générique :

```
<saml:Attribute Name="VIHF_Profil">
    <saml:AttributeValue>
        <VIHF_Profil xmlns="urn:hl7-org:v3" xsi:type="CE" code="profil_generique"
codeSystem="1.2.250.1.213.1.1.4.312" displayName="Contexte non spécifié"/>
    </saml:AttributeValue>
</saml:Attribute>
```

4.3.1.5.3.20. PSI_Locale

En authentification indirecte ou déléguée : identifiant sous la forme d'un OID de la politique de sécurité mise en œuvre dans le cadre de l'authentification locale de l'utilisateur.

Format :

Chaine alphanumérique

Exemple :

```
<saml:Attribute Name="PSI_locale">
    <saml:AttributeValue>1.2.250.1.213.1.5.3.456363</saml:AttributeValue>
</saml:Attribute>
```

4.3.1.5.3.21. Palier_Authentification

Palier du référentiel d'authentification auquel se situe l'authentification locale de l'utilisateur mise en œuvre.

Les valeurs possibles pour ce champ doivent être un code provenant de la terminologie de référence suivante :

- TRE_R231-PalierAuthentification, OID : 1.2.250.1.213.1.5.1.1.1

Les valeurs possibles peuvent être restreintes en fonction du jeu de valeurs correspondant mis à disposition par le projet.

En l'absence de spécifications complémentaires, le jeu de valeurs JDV_J21-PalierAuthentificationActeurPP peut être utilisé.

Format :

Type de donnée CE d'HL7 v3

Exemple :

```
<saml:Attribute Name="Palier_Authentification">

    <saml:AttributeValue>

        < xmlns="urn:hl7-org:v3" xsi:type="CE" code="   APPPRIP1" codeSystem="1.2.250.1.213.1.5.1.1.1" displayName="   Palier
1 de l'authentification privée des acteurs sanitaires, médico-sociaux et sociaux personnes physiques "/>
    </saml:AttributeValue>

</saml:Attribute>
```

4.3.1.5.3.22. urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code

Restriction d'audience à appliquer aux traces générées par la transaction objet du flux.

Les valeurs possibles pour ce champ doivent être un code provenant de la terminologie de référence suivante :

- TRE_A07-StatutVisibiliteDocument, OID : 1.2.250.1.213.1.1.4.13

Les valeurs possibles peuvent être restreintes en fonction du jeu de valeurs correspondant mis à disposition par le projet.

En l'absence de spécifications complémentaires, le jeu de valeurs JDV_J22-RestrictionAudienceVIHF-CISIS peut être utilisé.

Format :

Code^OID

Exemple :

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code">
    <saml:AttributeValue>INVISIBLE_REPRESENTANTS_LEGAUX^1.2.250.1.213.1.1.4.13</saml:AttributeValue>
</saml:Attribute>
```

4.3.1.5.4. Cas particuliers

4.3.1.5.4.1. Traitement des cartes Pharmaciens en remplacement exclusif

Les Pharmaciens diplômés et les Pharmaciens en formation qui ne font que des remplacements ou qui sont « multi-employeurs » ne disposent pas de CPS ou CPF. Ils disposent de CPE (PS_TypeCarte = 2) avec un identifiant spécifique commençant par « 3000000001/ » ou « 3000000018/ ».
Ces porteurs de cartes doivent être considérés comme des vrais professionnels, leur profil est déduit de leur identifiant.

Les composants suivants doivent être déduits des données PS disponibles :

- Identification nationale du PS (PS_IdNat) ; l'identifiant du PS à renseigner dans la requête (dans le jeton VIHF) est l'identifiant national PS et non l'identifiant spécifique présent en carte ou certificat,
- Profession (PS_Prof) et Future Profession (PS_FutureProf),
- Spécialités (PS_SpécRPPS) et Tableaux de pharmacie (PS_TabPharm),
- Secteur d'activité (Struct_SectAct).

Pour plus de précisions, se référer à l'annexe [4].

4.3.1.5.5. Profil pour un contexte d'utilisation « accès à un dossier médical »

Cette section décrit les contraintes apportées aux champs du VIHF dans le cas d'une utilisation pour se connecter sur un système cible gérant de données médicales à caractère personnel.

Afin de faciliter la lecture, seuls les champs présentant des contraintes spécifiques au contexte d'utilisation sont repris. En particulier, le tableau des champs complémentaires est repris pour indiquer les optionalités spécifiques au profil « accès à un dossier médical »

4.3.1.5.5.1. Champs standards

Pas de contrainte complémentaire par rapport au profil générique.

4.3.1.5.5.2. Champs complémentaires

Dans le contexte d'utilisation « accès à un dossier médical », il est considéré que la profession, la spécialité et le secteur d'activité renseignés dans le VIHF correspondent à sa situation au sein de la structure émettrice.

Champ	Requis /Optionnel	Description complémentaire par rapport au profil générique
VIHF_Version	R	

Champ	Requis /Optionnel	Description complémentaire par rapport au profil générique
urn:oasis:names:tc:xacml:2.0:subject:role	R	
Secteur_Activite	R si possible[9]	
urn:oasis:names:tc:xacml:2.0:resource:resource-id	R si nécessaire[10]	
Ressource_URN	R	
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	R	
Mode_Acces_Raison	R si bris de glace	Explication de la raison de l'usage du bris de glace.
urn:oasis:names:tc:xspa:1.0:subject:subject-id	O	
urn:oasis:names:tc:xspa:1.0:subject:npi	O	Non utilisé si l'utilisateur final n'est pas un professionnel de santé (ex. patient)
Identifiant_Structure	R si possible[11]	Identifiant de la structure de soin depuis laquelle la requête est émise.
urn:oasis:names:tc:xspa:1.0:subject:organization-id	O	
LPS_Nom	O	
LPS_Version	O	
LPS_ID	O	
Profil_Utilisateur	O	
Profil_Utilisateur_Perimetre	O	
Authentification_Mode	R en authentification déléguée ou en authentification directe via identifiant / mot de passe + OTP O sinon	
JSESSIONID	R en authentification directe via identifiant / mot de passe + OTP Non utilisé sinon	
VIHF_Profil	O	
PSI_Locale	O	Non utilisé en authentification directe

[9] Non utilisé pour un utilisateur final de type patient.

[10] L'élément urn:oasis:names:tc:xacml:2.0:resource:resource-id est nécessaire pour tout flux concernant un patient. Pour les flux génériques ne concernant pas un patient particulier (ex. liste des autorisations, accès aux traces utilisateur…) l'élément urn:oasis:names:tc:xacml:2.0:resource:resource-id n'est pas inclus dans le VIHF .

[11] Non utilisé pour un utilisateur final de type patient

Champ	Requis /Optionnel	Description complémentaire par rapport au profil générique
`Palier_Authentification`	O	Non utilisé en authentification directe
`urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code`	O	Restriction d'audience à appliquer aux traces générées par la transaction objet du flux

4.3.1.5.5.3. Formats et valeurs des champs complémentaires du jeton VIHF

4.3.1.5.5.3.1. urn:oasis:names:tc:xacml:2.0:resource:resource-id

L'usage de ce champ est issu de la recommandation du supplément au Technical Framework IHE nommé « Cross-Enterprise User Assertion » et concerne l'identification du patient.

Ce champ porte l'identifiant du patient. Pour une connexion à un service de partage de documents de santé, les identifiants utilisables sont définis par le système cible en accord avec le cadre juridique.

Les composants 1, 4 et 5 sont requis.

Composant 1 - Identifiant

Ce composant contient l'identifiant du patient.

Composant 4 - Autorité d'affectation

Identifiant de l'autorité d'affectation de l'identifiant utilisé :

- 1er sous-composant : Namespace ID (IS) = vide
- 2ème sous-composant : Universal ID (ST) : valeur de l'OID de l'autorité d'affectation de l'identifiant (pour l'INS, l'OID à utiliser est à sélectionner dans la liste des OID des autorités d'affectation des INS dans [5])
- 3ème sous-composant : Universal ID type (ID) = "ISO"

Composant 5 – Type d'identifiant

Code du type d'identifiant tel que défini dans [5]. « NH » pour les patients identifiés avec l'INS tel que défini dans le cadre juridique.

Format :

Format CX de HL7 v2.5.

Exemple :

```
<Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">
   <AttributeValue>124018852493334^^^&amp;1.2.250.1.213.1.4.8&amp;ISO^NH</AttributeValue>
</Attribute>
```

4.3.1.5.5.3.2. Ressource_URN

Dans le cas d'un système de gestion de dossiers médicaux qui indexerait des objets par des identifiants de patients, l'identifiant objet cible ne doit pas être interprété pour obtenir l'identifiant de patient.

L'identifiant du patient est à renseigner dans le champ *urn:oasis:names:tc:xacml:2.0:resource:resource-id*.

4.3.1.5.5.3.3. VIHF_Profil

Le profil utilisé est le profil « accès à un dossier médical ».

Pour assurer la compatibilité avec la version 1.0 du VIHF, si ce champ est absent, le VIHF est considéré comme suivant le profil « accès à un dossier médical ».

Exemple :

```
<saml:Attribute Name="VIHF_Profil">
   <saml:AttributeValue>
      <VIHF_Profil xmlns="urn:hl7-org:v3" xsi:type="CE" code="profil_dossier_medical" codeSystem="1.2.250.1.213.1.1.4.312"
displayName="Accès à un dossier médical"/>
   </saml:AttributeValue>
</saml:Attribute>
```

4.3.1.5.6. Profil pour un contexte d'utilisation « accès à un annuaire »

Cette section décrit les contraintes apportées aux champs du VIHF dans le cas d'une utilisation pour se connecter sur un système cible gérant un annuaire dans le secteur santé.

Afin de faciliter la lecture, seuls les champs présentant des contraintes spécifiques au contexte d'utilisation sont repris. En particulier, le tableau des champs complémentaires est repris pour indiquer les optionalités spécifiques au profil « accès à un annuaire »

4.3.1.5.6.1. Champs standards

Pas de contrainte complémentaire par rapport au profil générique.

4.3.1.5.6.2. Champs complémentaires

Dans le contexte d'utilisation « accès à un dossier médical », il est considéré que la profession, la spécialité et le secteur d'activité renseignés dans le VIHF correspondent à sa situation au sein de la structure émettrice.

Champ	Requis /Optionnel	Description complémentaire par rapport au profil générique
VIHF_Version	R	
urn:oasis:names:tc:xacml:2.0:subject:role	O	
Secteur_Activite	O	
urn:oasis:names:tc:xacml:2.0:resource:resource-id	N/A	Non utilisé dans le contexte d'utilisation « accès à un annuaire »
Ressource_URN	R	
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	O	
Mode_Acces_Raison	O	
urn:oasis:names:tc:xspa:1.0:subject:subject-id	O	
urn:oasis:names:tc:xspa:1.0:subject:npi	O	Non utilisé si l'utilisateur final n'est pas un professionnel de santé
Identifiant_Structure	R si nécessaire	Cf. la section détaillant ce champ
urn:oasis:names:tc:xspa:1.0:subject:organization-id	O	
LPS_Nom	O	
LPS_Version	O	
LPS_ID	O	
Profil_Utilisateur	R	
Profil_Utilisateur_Perimetre	O	
Authentification_Mode	R en authentification déléguée ou en authentification directe via identifiant / mot de passe + OTP O sinon	
JSESSIONID	R en authentification directe via identifiant / mot de passe + OTP Non utilisé sinon	
VIHF_Profil	R	
PSI_Locale	O	Non utilisé en authentification directe
Palier_Authentification	O	Non utilisé en authentification directe

4.3.1.5.6.3. Formats et valeurs des champs complémentaires du jeton VIHF

4.3.1.5.6.3.1. urn:oasis:names:tc:xacml:2.0:resource:resource-id

Ce champ ne concerne que les requêtes manipulant des données médicales à caractère personnel, il n'est pas utilisé dans un contexte « accès à un annuaire ».

4.3.1.5.6.3.2. Identifiant_Structure

L'identifiant de la personne morale est requis pour une authentification indirecte.

Il est par ailleurs requis s'il permet de caractériser le profil utilisateur. Par exemple, dans le cas d'un profil de type représentant légal d'une personne morale, ce champ est requis pour identifier la personne morale en question.

La liste des profils utilisateurs nécessitant la présence de ce champ est à définir par le système cible.

4.3.1.5.6.3.3. VIHF_Profil

Le profil utilisé est le profil « accès à un annuaire ».

Exemple :

```
<saml:Attribute Name="VIHF_Profil">
    <saml:AttributeValue>
        <VIHF_Profil xmlns="urn:hl7-org:v3" xsi:type="CE" code="profil_annuaire_PS" codeSystem="1.2.250.1.213.1.1.4.312"
displayName="Accès à un annaire"/>
    </saml:AttributeValue>
</saml:Attribute>
```

4.3.1.6. Exemple de jeton VIHF

L'exemple ci-dessous doit être précisé et validé par des implémentations de test.

```
<!-- exemple de VIHF généré pour un PS médecin généraliste en situation libérale en authentification directe pour un contexte d'usage de type accès à un dossier médical
   Les valeurs concernant l'émetteur ou le système cible sont imaginaires, pour illustration-->
<Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:assertion http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-2.0.xsd"
   ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
   IssueInstant="2009-09-09T00:46:02Z"
   Version="2.0">
   <!-- émetteur imaginaire.  -->
   <Issuer Format="urn:oasis:names:tc:SAML:1.1:namid-format:X509SubjectName">
      CN=801234567890+SN=DUPONT+GN=Jean,OU=Médecin,L=Paris(75),O=GIP-CPS,C=FR
   </Issuer>
   <!-- identité Issuer contenue dans le certificat. Dans le cas présent cela correspond à l'utilisateur identifié dans
         l'attribut subject:subject-id, mais cela pourrait être aussi l'identifiant de la structure -->
   <Subject>
      <NameID >
         801234567890
      </NameID>
   </Subject>
   <Conditions NotBefore="2009-09-09T00:46:02Z"  NotOnOrAfter="2009-09-09T01:46:02Z" >
      <!-- indique les dates de validité de l'assertion -->
      <AudienceRestriction> <!-- indique le service cible -->
         <Audience> urn:oid:1.2.250.1.554.999.111.777 </Audience> <!-- valeur imaginaire -->
      </AudienceRestriction>
   </Conditions>
   <AuthnStatement AuthnInstant="2009-09-09T00:46:02Z">
      <AuthnContext>
         <!-- exemple avec authentification par carte CPS -->
         <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:SmartCardPK</AuthnContextClassRef>
      </AuthnContext>
   </AuthnStatement>
   <AttributeStatement>
      <Attribute Name="VIHF_version">
         <AttributeValue3.0</AttributeValue>
      </Attribute>
      <Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
         <!-- contient profession et éventuellement spécialité -->
         <AttributeValue> <!-- profession -->
            <Role xmlns="urn:hl7-org:v3" xsi:type="CE"
               code="10"  codeSystem="1.2.250.1.71.1.2.7" codeSystemName="G15" displayName="Médecin"/>
         </AttributeValue>
         <AttributeValue> <!-- Spécialité qualification -->
            <Role xmlns="urn:hl7-org:v3" xsi:type="CE"
               code="SM54"  codeSystem="1.2.250.1.71.4.2.5" codeSystemName="R01" displayName="Médecine générale (SM)"/>
         </AttributeValue>
      </Attribute>
      <Attribute Name="Secteur_Activite">
         <AttributeValue>SA07^1.2.250.1.71.4.2.4</AttributeValue>
      </Attribute>
      <Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">
         <AttributeValue>124018852493334^^^&amp;amp; 1.2.250.1.213.1.4.8&amp;amp;ISO^NH</AttributeValue> <!-- INS imaginaire -->
      </Attribute>
      <Attribute Name="Ressouce_URN">
         <AttributeValue>urn:monsystemecible</AttributeValue> <!-- URN imaginaire à titre d'exemple -->
      </Attribute>
      <Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
         <AttributeValue>
            <purposeOfUse xmlns="urn:hl7-org:v3" xsi:type="CE" code="normal" codeSystem="1.2.250.1.213.1.1.4.248"/>
         <AttributeValue>
      <Attribute>
```

```
      <Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">
        <AttributeValue>Jean DUPONT</AttributeValue> <!-- Dans cet exemple, la valeur est celle du certificat -->
      </Attribute>
      <Attribute Name="Identifiant_Structure">
        <AttributeValue>401234567890005 </AttributeValue> <!-- identifiant cabinet RPPS imaginaire -->
      </Attribute>
      <Attribute Name="LPS_Nom">
        <AttributeValue>SUPER_LPS</AttributeValue> <!-- valeur imaginaire -->
      </Attribute>
      <Attribute Name="LPS_ID">
        <AttributeValue>1243864367554</AttributeValue> <!-- valeur imaginaire -->
      </Attribute>
     <Attribute Name="LPS_Version">
        <AttributeValue>1.1</AttributeValue>
      </Attribute>
      <Attribute Name="Authentification_Mode">
        <AttributeValue>
          <Authentification_Mode xmlns="urn:hl7-org:v3" xsi:type="CE"
            code="DIRECTE" codeSystem="1.2.250.1.213.1.1.4.323" displayName="Authentification directe"/>
        </AttributeValue>
      </Attribute>
      <Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:npi">
        <AttributeValue>801234567890</AttributeValue>
      </Attribute>
      <Attribute Name=" urn:oasis:names:tc:xspa:1.0:organization-id">
        <AttributeValue>401234567890005</AttributeValue>
      </Attribute>
      <Attribute Name="VIHF_Profil">
        <AttributeValue>
          <VIHF_Profil xmlns="urn:hl7-org:v3" xsi:type="CE"
            code="profil_dossier_medical" codeSystem="1.2.250.1.213.1.1.4.312" displayName="Accès à un dossier médical"/>
        </AttributeValue>
      </Attribute>
      <Attribute Name="PSI_Locale">
        <AttributeValue>1.2.250.1.213.1.5.3.456363</AttributeValue> <!-- valeur imaginaire -->
      </Attribute>
      <Attribute Name="Palier_Authentification">
        <AttributeValue>
          <Palier_Authnetification xmlns="urn:hl7-org:v3" xsi:type="CE"
            code="APPPRIP1" codeSystem="1.2.250.1.213.1.5.1.1.1" displayName="Palier 1 de l'authentification privée des
            acteurs sanitaires, médico-sociaux et sociaux personnes physiques"/>
        </AttributeValue>
      </Attribute>
      <Attribute Name="urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code">
        <AttributeValue> INVISIBLE_REPRESENTANTS_LEGAUX^1.2.250.1.213.1.1.4.13</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
```

4.3.1.7. Codes erreur liés au processus d'authentification et d'habilitation

Si le processus d'authentification et d'habilitation se déroule normalement alors le service s'exécute comme prévu.

Si une erreur se produit dans ce processus alors une erreur « Soap Fault » est retournée avec les codes d'erreur suivants, conformes aux recommandations WSS SAML token profile 1.1.

Code erreur	Description dans le profil	Description dans le cadre d'un SIS
`wsse:SecurityTokenUnavailable`	A referenced SAML assertion could not be retrieved.	La requête n'est pas correctement formée : jeton VIHF absent.
`wsse:UnsupportedSecurityToken`	An assertion contains a <saml:Condition> element that the receiver does not understand. The receiver does not understand the extension schema used in an assertion. The receiver does not support the SAML version of a referenced or included assertion.	La requête n'est pas correctement formée : contenu du jeton VIHF incorrect.
`wsse:FailedCheck`	A signature within an assertion or referencing an assertion is invalid.	Erreur dans le processus d'authentification.
`wsse:InvalidSecurityToken`	The issuer of an assertion is not acceptable to the receiver.	Erreur dans le processus d'habilitation : accès refusé

4.3.1.8. Configurations possibles en architecture d'authentification centralisée via un portail d'authentification

Rédaction ultérieure.

4.3.1.9. Fonctionnement général des échanges intégrant le VIHF en architecture d'authentification centralisée

Rédaction ultérieure.

4.3.1.10. Contenu du jeton VIHF en architecture d'authentification centralisée

Rédaction ultérieure.

4.3.1.11. Exemple de jeton VIHF en architecture d'authentification centralisée

Rédaction ultérieure.

4.3.1.12. Codes erreur liés au processus d'authentification et d'habilitation en architecture centralisée

Rédaction ultérieure.

4.3.2. Exigences techniques pour les systèmes initiateurs

4.3.2.1. Configuration « authentification indirecte »

Le système doit intégrer au moins deux certificats émis par une IGC autorisée par les référentiels d'authentification de la PGSSI-S :

- un certificat d'authentification utilisé pour l'établissement des connexions (type SSL) ;
- un certificat de signature utilisé pour les signatures électroniques des jetons et des services (type signature).

Il doit aussi implémenter la reconnaissance des certificats racine et intermédiaires des IGC autorités de certification des services accédés sur les systèmes cibles (nécessaire pour l'établissement des connexions). Les autorités de certification des services sont choisies par les systèmes cibles parmi les IGC autorisées pour les référentiels d'authentification de la PGSSI-S pour l'authentification des téléservices.

Cela implique donc l'implémentation des fonctionnalités suivantes :

- la possibilité de mise à jour des certificats racine et intermédiaires des IGC concernées (à expiration des certificats) **;**
- l'accès aux listes de révocation de certificats des IGC concernées.

Pour des raisons de traçabilité, le système doit être capable, pour chaque requête envoyée au système cible, de retrouver l'identité de l'utilisateur final. Il faut donc établir le lien entre l'identifiant envoyé dans les jetons VIHF et une personne physique.

4.3.2.2. Configuration « authentification directe »

Lorsque l'authentification directe est réalisée à partir d'un certificat confiné dans une carte CPx, le LPS doit pouvoir accéder aux fonctionnalités des cartes CPS pour la mise en œuvre des mécanismes d'authentification.

L'accès aux cartes CPS doit se faire via le middleware fourni par l'ANS (Cryptolibs CPS), la CPS étant introduite soit dans un lecteur homologué par le GIE SESAM-VITALE, soit dans un lecteur PC/SC.

L'accès à ces composants doit se faire selon les bonnes pratiques afin de ne pas mettre en péril le fonctionnement des autres logiciels utilisant ces mêmes composants.

Le LPS doit aussi implémenter la reconnaissance des certificats racine et intermédiaires des IGC, autorités de certification des services accédés sur les systèmes cibles (nécessaire pour l'établissement des connexions). Les autorités de certification des services sont choisies par les systèmes cibles parmi les IGC autorisées pour les référentiels d'authentification de la PGSSI-S pour l'authentification des téléservices.

Cela implique donc l'implémentation des fonctionnalités suivantes :

- la possibilité de mise à jour des certificats racine et intermédiaires des IGC concernées (à expiration des certificats) **;**
- l'accès aux listes de révocation de certificats publiées par l'autorité de certification des IGC concernées.

4.3.2.3. Configuration « authentification déléguée »

Le système doit intégrer au moins deux certificats serveur émis par une IGC autorisée par les référentiels d'authentification de la PGSSI-S :

- un certificat d'authentification utilisé pour l'établissement des connexions (type SSL) ;
- un certificat de signature utilisé pour les éventuelles signatures électroniques des jetons et des services (type signature).

Il doit aussi implémenter la reconnaissance des certificats racine et intermédiaires des IGC, autorités de certification des services accédés sur les systèmes cibles (nécessaire pour l'établissement des connexions). Les autorités de certification des services sont choisies par les systèmes cibles parmi les IGC autorisées pour les référentiels d'authentification de la PGSSI-S pour l'authentification des téléservices.

Cela implique donc l'implémentation des fonctionnalités suivantes :

- la possibilité de mise à jour des certificats racine et intermédiaires des IGC concernées (à expiration des certificats) **;**
- l'accès aux listes de révocation de certificats des IGC concernées.

Pour des raisons de traçabilité, le système doit être capable, pour chaque requête envoyée au système cible, de retrouver l'identité de l'utilisateur final. Il faut donc établir le lien entre l'identifiant envoyé dans les jetons VIHF et une personne physique.

Si l'authentification de l'utilisateur final est réalisée à partir d'un certificat confiné dans une carte CPx, le système initiateur auquel le système cibla à délégué l'authentification doit pouvoir accéder aux fonctionnalités des cartes CPS pour la mise en œuvre des mécanismes d'authentification.

L'accès aux cartes CPS doit se faire via le middleware fourni par l'ANS (Cryptolibs CPS), la CPS étant introduite soit dans un lecteur homologué par le GIE SESAM-VITALE, soit dans un lecteur PC/SC.

L'accès à ces composants doit se faire selon les bonnes pratiques afin de ne pas mettre en péril le fonctionnement des autres logiciels utilisant ces mêmes composants.

Le système initiateur doit aussi implémenter la reconnaissance des certificats racine et intermédiaires des IGC, autorités de certification des services accédés sur les systèmes cibles (nécessaire pour l'établissement des connexions). Les autorités de certification des services sont choisies par les systèmes cibles parmi les IGC autorisées pour les référentiels d'authentification de la PGSSI-S pour l'authentification des téléservices.

Cela implique donc l'implémentation des fonctionnalités suivantes :

- la possibilité de mise à jour des certificats racine et intermédiaires des IGC concernées (à expiration des certificats) **;**
- l'accès aux listes de révocation de certificats publiées par l'autorité de certification des IGC concernées.

4.4. Contrôle d'accès

Le contrôle d'accès est géré par le système cible, service par service. Pour plus de détails, se référer au volet de la couche service correspondant.

4.5. Eléments du VIHF spécifiques au système cible

Le VIHF définit un cadre général qui doit être instancié par service cible.

En fonction de ses objectifs fonctionnels de sécurité, d'une analyse de risque et de certaines contraintes opérationnelles (telles qu'un compromis performance/sécurité ou les capacités techniques des composants utilisables et disponibles), le système cible doit préciser plusieurs points, en distinguant éventuellement chaque configuration d'authentification (directe, indirecte).

Les principaux points à préciser sont :

- les versions de TLS supportées, et les configurations qui y sont liées, la version de TLS minimale admise étant la 1.0 ;
- l'autorité de certification retenue pour l'authentification pour le système cible, dont l'IGC doit être prise en compte dans la configuration du système initiateur pour l'établissement des sessions TLS ;
- l'usage de la signature dans l'assertion SAML, qui peut être imposée au système initiateur ; dans ce cas, la signature doit être conforme au format XMLDsig tel que défini par SAML 2.0 ;
- la durée de vie maximum de l'assertion SAML acceptée par le système cible, le système initiateur pouvant la définir d'une durée plus courte ;
- les attributs du VIHF à transmettre obligatoirement parmi ceux qui sont définis dans le VIHF comme optionnels et qui peuvent être requis par le système cible pour faire le contrôle d'accès.

Le système cible peut imposer d'autres mesures de sécurité en fonction de ses besoins.

Annexe 1 : Evolutions futures

Il est prévu à terme la mise en place du Portail National des Systèmes de Santé (PNSS), qui répond à deux besoins essentiels :

- une centralisation des droits des utilisateurs, basée sur le partage de règles entre systèmes de santé, qui permet notamment une gestion unifiée du consentement des patients ;
- une standardisation des moyens techniques pour accéder aux données, tout en prenant en compte la diversité des politiques de sécurité applicables et des environnements techniques des utilisateurs.

Ce PNSS pourra faire l'objet d'un volet spécifique de la couche service dans le cadre de l'élaboration du jeton VIHF utilisé par les volets de la couche transport. Le VIHF utilisé entre les systèmes initiateurs et le portail d'authentification sera décrit dans les sections 4.3.1.8 à 4.3.1.12.

Annexe 2 : Tableau récapitulatif des attributs SAML pour le VIHF version 1.0

Champ	Requis /Optionnel
VIHF_Version	R
urn:oasis:names:tc:xacml:2.0:subject:role	R
Secteur_Activite	R
urn:oasis:names:tc:xacml:2.0:resource:resource-id	R si nécessaire[12]
Ressource_URN	R
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	R
Mode_Acces_Raison	R si bris de glace
urn:oasis:names:tc:xspa:1.0:subject:subject-id	O
Identifiant_Structure	R
LPS_Nom	O
LPS_Version	O
LPS_ID	O

La version 1.0 du VIHF est uniquement utilisable pour le contexte d'utilisation « accès à un dossier médical » et pour les configurations en authentification directe via certificat électronique et en authentification indirecte.

[12] L'élément urn:oasis:names:tc:xacml:2.0:resource:resource-id est nécessaire pour tout flux concernant un patient. Pour les flux génériques ne concernant pas un patient particulier l'élément urn:oasis:names:tc:xacml:2.0:resource:resource-id n'est pas inclus dans le VIHF .

Annexe 3 : Mapping avec le profil XUA

Le profil IHE XUA dans sa version complète incluant l'extension d'attribut XUA++ (Cross-Enterprise User Assertion - Attribute Extension) a été publié en version « final text » en septembre 2013. Il est intégré aux tomes 1 et 2b du technical framework du domaine ITI d'IHE :

- http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf section 13
- http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf section 3.40

Afin d'aider les développeurs de produits mettant en œuvre ce volet à atteindre la conformité à XUA, les prérequis et les options XUA tels que présentés dans les sections 3.40.4.1.2, 3.40.4.1.2.1, 3.40.4.1.2.2.1 et 3.40.4.1.2.3 sont repris dans le tableau suivant. Les conditions de conformité du VIHF au profil XUA sont présentées dans la colonne « impact VIHF ».

Spécifications XUA	Requis/Optionnel	Impact VIHF
L'assertion doit contenir un champ *Subject* qui contient l'identifiant de l'utilisateur demandant l'accès au service	R	**Pas d'impact** L'élément *Subject/NameID* contient l'identifiant de l'utilisateur final
Le champ *Subject* doit contenir un élément *SubjectConfirmation* et la méthode « bearer confirmation » doit être supportée	R	**Complément à intégrer dans le VIHF** La méthode « bearer confirmation » est la méthode utilisée par défaut dans le VIHF. Mais l'élément *Subject/SubjectConfirmation* n'est pas utilisé dans le VIHF. Pour être conforme au profil XUA, il convient d'ajouter l'élément *Subject/SubjectConfirmation* suivant : <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"\>
Le champ *NotBefore* doit être renseigné avec la date et l'heure de l'élaboration de l'assertion	R	**Pas d'impact** Le champ *NotBefore* correspond à la date de constitution du VIHF
Le champ *AudienceRestriction* doit contenir l'identification du système cible	R	**Contraintes supplémentaires sur le VIHF** Le champ *AudienceRestriction* est optionnel dans le VIHF, il doit être renseigné pour permettre une conformité avec le profil XUA
L'assertion doit contenir un champ *AuthnStatement* avec soit un élément *AuthnContextClassRef*, soit un élément *AuthnContextDeclRef*	R	**Pas d'impact** L'élément *AuthnStatement/AuthnContextClassRef* est un élément obligatoire dans le VIHF *AuthnStatement/AuthnContextClassIRef* peut si nécessaire identifier le PSSI appliqué par le système initiateur
Si l'assertion contient le nom du professionnel de santé, celui-ci doit être	R si le nom du PS est	**Pas d'impact**

Spécifications XUA	Requis/Optionnel	Impact VIHF
renseigné dans le champ complémentaire *urn:oasis:names:tc:xspa:1.0:subject:subject-id*	présent dans l'assertion	*urn:oasis:names:tc:xspa:1.0:subject:subject-id* est un champ complémentaire du VIHF
Si l'assertion contient l'identifiant de la structure pour le compte de laquelle intervient l'utilisateur final, celui-ci doit être renseigné dans le champ complémentaire *urn:oasis:names:tc:xspa:1.0:subject:organization-id*	R si l'identifiant de la structure est présent dans l'assertion	**Contrainte supplémentaire sur le VIHF** Si l'identifiant de la structure est présent dans l'assertion, le champ optionnel *urn:oasis:names:tc:xspa:1.0:subject:organization-id* doit être présent et renseigné avec la même valeur que le champ *Identifiant_Structure*
Si l'assertion contient l'identifiant du professionnel de santé utilisateur, celui-ci doit être renseigné dans le champ complémentaire *urn:oasis:names:tc:xspa:2.0:subject:npi*	R si l'identifiant du professionnel utilisateur est present dans l'assertion	**Contrainte supplémentaire sur le VIHF** Si l'utilisateur final est un professionnel de santé, le champ optionnel *urn:oasis:names:tc:xspa:2.0:subject:npi* doit être présent et renseigné avec la même valeur que le champ *Subject/NameID*
L'assertion doit être signée par le système initiateur	R	**Contrainte supplémentaire sur le VIHF** La signature du VIHF n'est pas obligatoire pour des raisons de performance, pour être conforme au profil XUA, le système initiateur doit systématiquement signer le VIHF
Le rôle fonctionnel de l'utilisateur peut être renseigné dans le champ *urn:oasis:names:tc:xacml:2.0:subject:role*	O	**Pas d'impact** Si le champ *urn:oasis:names:tc:xacml:2.0:subject:role* est utilisé, le VIHF met en œuvre l'option XUA « Subject-Role Option ».
L'identifiant du patient cible de la requête peut être renseigné dans le champ *urn:oasis:names:tc:xacml:2.0:resource:resource-id*	O	**Pas d'impact** Si le champ *urn:oasis:names:tc:xacml:2.0:resource:resource-id* est utilisé, le VIHF met en œuvre l'option XUA « Patient Identifier Attribute ».
Le mode d'accès demandé peut être renseigné dans le champ *urn:oasis:names:tc:xspa:1.0:subject:purposeofuse*	O	**Pas d'impact** Si le champ *urn:oasis:names:tc:xspa:1.0:subject:purposeofuse* est utilisé, le VIHF met en œuvre l'option XUA « PurposeOfUse Option ».

Annexe 4 : Documents de référence

Documents de référence	
[1]	IHE International : Cadre Technique IT Infrastructure
[2]	IHE International : Profil Cross-Enterprise User Assertion – Attribute Extension (XUA++)
[3]	IHE France : Contraintes sur les types de données HL7 v2.5 applicables aux profils d'intégration du cadre technique IT Infrastructure dans le périmètre d'IHE France v1.2 du 8 octobre 2009
[4]	ANS : Cadre Interop SIS – Annexe transversale Sources des données métier pour les personnes et les structures
[5]	ANS : Programme identifiant national de santé : Liste des OID des autorités d'affectation des INS
[6]	ANS : Référentiel d'authentification de la PGSSI-S

Annexe 5 : Historique du document

Version	Rédigé par		Vérifié par		Validé par	
0.0.1	ASIP SANTÉ	Le 25/06/2009	ASIP SANTÉ	Le 25/06/2009	ASIP SANTÉ	Le 25/06/2009
	Motif et nature de la modification : **Publication pour première phase de concertation**					
0.0.2	ASIP SANTÉ	Le 08/09/2009	ASIP SANTÉ	Le 08/09/2009	ASIP SANTÉ	Le 08/09/2009
	Motif et nature de la modification : **Prise en compte des commentaires reçus au 31/08. Publication en entrée de la session de validation des 14 & 15 sept.**					
0.0.3	ASIP SANTÉ	Le 17/09/2009	ASIP SANTÉ	Le 17/09/2009	ASIP SANTÉ	Le 17/09/2009
	Motif et nature de la modification : **Post session d'experts des 14 & 15 sept.** **Ajout du jeton VIHF exemple, et compléments sur les champs SAML**					
0.1.0	ASIP SANTÉ	Le 02/10/2009	ASIP SANTÉ	Le 02/10/2009	ASIP SANTÉ	Le 02/10/2009
	Motif et nature de la modification : **Publication post approbation par représentants des industriels**					
0.1.1	ASIP SANTÉ	Le 24/02/2010	ASIP SANTÉ	Le 24/02/2010	ASIP SANTÉ	Le 24/02/2010
	Motif et nature de la modification : **Publication sans changement dans la version 0.1.1 du CI-SIS**					
0.2.0	ASIP SANTÉ	Le 14/09/2010	ASIP SANTÉ	Le 14/09/2010	ASIP SANTÉ	Le 14/09/2010
	Motif et nature de la modification : **Evolution du contenu « Identification et authentification » pour prendre en compte les évolutions décidées dans le cadre du projet DMP. Prise en compte de IHE XUA ++ version juillet 2010.**					
0.2.0.1	ASIP SANTÉ	Le 23/09/2010	ASIP SANTÉ	Le 23/09/2010	ASIP SANTÉ	Le 23/09/2010
	Motif et nature de la modification : ► Précision du mode d'authentification ► Ajout du champ « AuthnInstant »					
1.0.0	ASIP SANTÉ	Le 05/11/2010	ASIP SANTÉ	Le 05/11/2010	ASIP SANTÉ	Le 05/11/2010
	Motif et nature de la modification : ► Expression de la date et heure en temps universel coordonné (UTC) ► Ajout des références à l'annexe transversale spécifiant les sources des données métier pour les personnes et les structures					
1.0.1	ASIP SANTÉ	Le 15/11/2010	ASIP SANTÉ	Le 15/11/2010	ASIP SANTÉ	Le 15/11/2010
	Motif et nature de la modification : **Publication sans changement dans la version 1.0.1 du CI-SIS**					
1.1.0	ASIP SANTÉ	Le 21/02/2012	ASIP SANTÉ	Le 21/02/2012	ASIP SANTÉ	Le 21/02/2012
	Motif et nature de la modification : ► Erratum 1–23/11/10 : § 4.3.1.5.1.1 – Mise en conformité de l'ordre des RDN des exemples avec les règles de la RFC 2253 ► Erratum 2–14/12/10 : Correction de l'OID de la nomenclature G15 dans deux exemples § 4.3.1.5.3.2 page 31 et § 4.3.1.6 page 38 ► § 4.3.1.5.1.4 page 26 Correction du nom de l'attribut dans le titre : @AuthentInstant devient @AuthnInstant					

Version	Rédigé par		Vérifié par		Validé par	
	► Correction de la chaîne de caractères &amp ; en & constituant les exemples d'INS lorsqu'ils ne figurent pas dans un exemple montrant une partie d'un message XML ► Correction de l'exemple de l'identifiant de cabinet RPPS sur 15 caractères par. 4.3.1.6 ► Mise en revue interne					
1.2.0	ASIP SANTÉ	Le 19/04/2012	ASIP SANTÉ	Le 19/04/2012	ASIP SANTÉ	Le 19/04/2012
	Motif et nature de la modification : **Prise en compte des commentaires à la suite de la revue interne** ► Référence à la liste des OID des autorités d'affectation des INS au lieu de lister les OID associés aux types d'INS					
1.3.0	ASIP SANTÉ	Le 15/10/2012	ASIP SANTÉ	Le 15/10/2012	ASIP SANTÉ	Le 15/10/2012
	Motif et nature de la modification : **Publication version 1.3.0, sans changement**					
1.3.1 (version non publiée)	ASIP SANTÉ	Le 28/01/2013	ASIP SANTÉ	Le 28/01/2013	ASIP SANTÉ	Le 28/01/2013
	Motif et nature de la modification : Evolution du VIHF pour prendre en compte d'autres contextes d'utilisation et d'autres architectures d'authentification (authentification des patients, authentification déléguée, utilisation pour des services non centrés patient comme l'accès à des annuaires de PS)					
1.3.2	ASIP SANTÉ	Le 06/05/2015	ASIP SANTÉ	Le 06/05/2015	ASIP SANTÉ	Le 06/05/2015
	Motif et nature de la modification : Prise en compte de la version finale de XUA++ intégrée à la version 10 du technical framework du domaine ITI d'IHE. § 4.3.1.5.1.2, 4.3.1.5.5.3.1 et 4.3.1.6 : Suppression des éléments concernant l'INS-A					
1.3.2.1	ASIP SANTÉ	Le 06/11/2017	ASIP SANTÉ	Le 06/11/2017	ASIP SANTÉ	Le 06/11/2017
	Motif et nature de la modification : ► Sections 4.3.1.5.1.2, 4.3.1.5.5.3.1: reformulation pour permettre de véhiculer plusieurs types d'identifiant patient (modification suite au lot 1 d'évolutions mineures du CI-SIS) ► Sections 2, 4.3.2.1, 4.3.2.2, 4.3.2.3 : référence à l'IGC Santé comme une des IGC utilisables (modification suite au lot 1 d'évolutions mineures du CI-SIS) ► Sections 4.3.1.5.2, 4.3.1.5.3.1, 4.3.1.5.3.20, 4.3.1.5.3.21, 4.3.1.5.5.2, 4.3.1.5.6.2, 4.3.1.6 : ajout au VIHF deux nouveaux attributs optionnels pour porter les informations nécessaires à l'identification de la politique de sécurité locale dans le cas d'une authentification indirecte ou déléguée (modification suite au lot 1 d'évolutions mineures du CI-SIS) ► Sections 4.3.1.5.2, 4.3.1.5.3.22, 4.3.1.5.5.2, 4.3.1.6 : associer aux documents et aux traces la restriction d'audience correspondante. Un nouvel attribut optionnel au VIHF est proposé pour porter cette information (modification suite au lot 1 d'évolutions mineures du CI-SIS)					
1.4	ASIP SANTÉ	Le 04/12/2017	ASIP SANTÉ	Le 04/12/2017	ASIP SANTÉ	Le 04/12/2017
	Motif et nature de la modification : Publication sans modification pour alignement du numéro de version avec la règle de gestion des numéros de version dans le CI-SIS					
1.5	ASIP SANTÉ	Le 01/07/2018	ASIP SANTÉ	Le 01/07/2018	ASIP SANTÉ	Le 01/07/2018

Version	Rédigé par		Vérifié par		Validé par	
	Motif et nature de la modification : Prise en compte des évolutions des certificats. Fin de vie de la carte CPS2ter et l'arrivée de la carte CPS3.3. Les sections concernées : 4.3.2.1, 4.3.2.2 et 4.3.2.3					
1.6	ANS	Le 5/11/2020	ANS	Le 5/11/2020	ANS	Le 5/11/2020
	Motif et nature de la modification : ► Suite aux évolutions des spécifications IHE, l'obligation d'avoir un paramètre 'action' contenant la valeur « urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b » dans les requêtes est levée ► Harmonisation des renvois aux nomenclatures des objets de santé et allégement des contraintes d'utilisation des jeux de valeurs ► Modification du document au format ANS ► Modification des termes redondants « juridique et réglementaire » en « juridique » ► Insertion des informations relatives au transport de l'INS et des traits complémentaires					
1.7	ANS	Le 9/02/2021	ANS	Le 9/02/2021	ANS	Le 9/02/2021
	Motif et nature de la modification : ► Le transport de l'INS du patient devient obligatoire et rend, de fait, caduque l'INS-C. Ceci entraine la suppression des références à l'INS-C.					
1.8	ANS	Le 17/08/2021	ANS	Le 17/08/2021	ANS	Le 17/08/2021
	Motif et nature de la modification : ► Mise à jour du nom ASIP					