Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

MINISTÈRE DU TRAVAIL, DE l'EMPLOI ET DE LA SANTÉ

MINISTÈRE DES SOLIDARITÉ ET DE LA COHÉSION SOCIALE

MINISTÈRE DU BUDGET, DES COMPTES PUBLICS ET DE LA RÉFORME DE L'ÉTAT

Format d'échange des traces

Standard d'interopérabilité entre organismes de la sphère sociale

Réf. : Standard Interops2.0_FormatEchangeTraces
Version 2.0 du 05/04/2012

Référence : **Version :** **Date de dernière mise à jour :**	Standard Interops2.0_FormatEchangeTraces 2.0 05/04/2012
Niveau de confidentialité :	PUBLIC

Table des mises à jour du document

N° de version	Date	Auteur	Objet de la mise à jour
2.0	05/04/12	Groupe de travail Interops	Version pour diffusion

SOMMAIRE

1. INTRODUCTION

1.1 Objet du document

L'objet de ce document est de définir les cas d'usage des échanges des traces et le format pivot d'échange des traces entre les organismes

1.2 Organisation et structure du document

La structure du présent document est, en sus de la présente introduction, organisé comme suit :

- Le chapitre 2 « **Principes généraux** » présente les éléments tracés par les organismes et le principe de rapprochement
- Le chapitre 3 « **Modélisation des échanges** » définit les échanges possibles entre organisme concernant les traces
- Le chapitre 4 « **Format des données** » présente le format des données échangées

1.3 Références

1.3.1 Références internes

Référence		Titre	Auteur	Ver.	Date
[VI]	Standard Interops2.0_SpecificationsVI	Spécifications du Vecteur d'Identification	Groupe de travail Interops	2.0	05/04/2012

1.3.2 Références externes

	Titre	Auteur	Date
[Auth2.0]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0	J. Kemp et al	15/03/2005
[Core1.1]	Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1	Eve Maler, Prateek Mishra, Rob Philpott	02/09/2003
[Core2.0]	Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0	Cantor, Scott, Kemp, John, Philpott, Rob, Maler, Eve	15/03/2005

2. PRINCIPES GENERAUX

La convention établie entre les organismes définit le format d'échanges des traces InterOPS. Ces traces ne sont pas à confondre avec les besoins de traces applicatives. Ces dernières ne sont pas abordées dans ce document. Leur format et leur contenu reste ouvert et à étudier au niveau du projet fonctionnel.

2.1 Les éléments tracés

2.1.1 Organisme client

L'organisme client doit tracer dans le cadre de la fourniture de la solution :

- L'authentification de l'application cliente ou de l'utilisateur
- La génération d'un VI pour l'application cliente ou pour l'utilisateur

La trace d'une authentification de l'application cliente ou de l'utilisateur doit comporter les éléments suivants :

- Date de l'événement
- Identifiant local à l'organisme client de l'application cliente ou de l'utilisateur
- Méthode d'authentification
- Statut de l'authentification (succès et échec)

La trace de génération du VI doit comporter les éléments suivants :

- Date de l'événement
- Identifiant local à l'organisme client de l'application cliente ou de l'utilisateur
- Identifiant du service visé
- Identifiant « impersonnifié » de l'application cliente ou de l'utilisateur, contenu dans le sujet de l'assertion
- Identifiant du VI
- VI transmis, contenant la signature

2.1.2 Organisme fournisseur

L'organisme fournisseur doit tracer dans le cadre de la fourniture de la solution :

- La réception et la vérification du VI
- La transaction effectuée par l'application ou par un utilisateur

La trace de réception et vérification du VI doit comporter les éléments suivants :

- Date de l'événement
- Identifiant « impersonnifié » de l'application cliente ou de l'utilisateur, contenu dans le sujet de l'assertion
- Identifiant du service visé
- Identifiant local à l'organisme fournisseur de l'utilisateur
- Identifiant du VI
- VI reçu, contenant la signature
- Statut de la vérification (succès et échec)

La trace d'une transaction doit comporter les éléments suivants :

- Date de l'événement
- Identifiant local à l'organisme fournisseur de l'application cliente ou de l'utilisateur
- URL visé (Interops-A), URL de la page (Interops-P) ou du service (Interops-S)
- Action réalisée
- Statut de l'action (succès et échec)

Côté organisme fournisseur, l'identifiant local est un identifiant « pivot » entre les traces de vérification et les traces de transaction. Il doit permettre d'identifier les transactions effectuées sur le temps d'une session ouverte par la transmission d'un VI. Afin d'assurer la correspondance entre les traces de vérification et de transaction, cet identifiant local peut être égal à l'identifiant du VI (cf. 3.3.1) ou tout autre identifiant aléatoire généré par le système de l'organisme client.

Dans le cas où l'on voudra centrer les traces côté organisme fournisseur sur les actions d'un utilisateur donné, l'identifiant local à l'organisme fournisseur peut être la représentation de l'application cliente ou de l'utilisateur dans l'espace de confiance de l'organisme fournisseur. L'Identifiant local à l'organisme fournisseur serait alors égal à l'identifiant de l'application cliente ou de l'utilisateur transmis dans le VI.

2.2 Les principes de rapprochement

Un processus de rapprochement s'effectue en transmettant l'**identifiant de l'organisme** et l'**identifiant du VI**.

Il doit permettre exceptionnellement :

- A un organisme client de récupérer les traces applicatives et les traces de vérification de ses utilisateurs
- A un organisme fournisseur de déclarer le comportement suspect d'un ou des utilisateurs d'un organisme donné accédant à son SI

Il est également envisageable qu'un tiers demande des traces aux organismes clients et/ou fournisseurs.

3. MODELISATION DES ECHANGES

3.1 Identification des acteurs

On identifiera uniquement 3 acteurs :

- L'organisme client ou toute personne appartenant à cet organisme ayant les droits suffisants
- L'organisme fournisseur ou toute personne appartenant à cet organisme ayant les droits suffisants
- Un tiers

3.2 Identification des cas d'usage

Les interactions entre les acteurs identifiés peuvent être modélisées selon les cas d'utilisation suivant :

- Demande de traces de vérification et de traces applicatives
- Déclaration de comportement suspect

3.3 Modèle de données

Deux types d'information peuvent être échangés :

- Une demande par un organisme client ou fournisseur
- La réponse de l'organisme fournisseur contenant les traces

Les méthodes d'échange ne sont pas précisées dans ce document. Ainsi, les données peuvent échangées par mail, par web service, etc.

3.3.1 Demande d'un organisme

Une demande d'un organisme, qu'il soit l'organisme client, l'organisme fournisseur ou un Tiers, comme rappelé ci-dessus (cf. §2.2 « Les principes de rapprochement ») est constituée pour chaque VI de :

- L'identifiant de l'organisme client émetteur du VI
- L'identifiants du VI qui fait l'objet de la demande

Selon le mode utilisé (Interops-A, Interops-P ou Interops-S), l'identifiant du VI pourra être (cf. [VI]) :

- L'attribut `AssertionID` d'une assertion SAML 1.1
- L'attribut `ID` d'une assertion SAML 2.0
- L'attribut `ID` d'une assertion SAML 2.0 incluse dans un élément SAML 2.0 `Response`

3.3.2 Réponse d'un organisme fournisseur

La réponse de l'organisme fournisseur se décompose en deux parties :

- Les traces de vérification correspondant aux identifiants d'assertion demandés
- Les traces applicatives des actions réalisées par le ou les utilisateurs s'étant authentifiés sur le SI en utilisant les assertions identifiées dans la demande le temps de la session

Comme rappelé au §0, une trace de vérification pour être exploitable par l'organisme client doit comporter les éléments suivants :

- Date de l'événement si le VI a été trouvé
- Statut de la vérification
- Identifiant du VI
- Identifiant de l'organisme client
- VI s'il a été trouvé

De même, les traces applicatives doivent comporter les éléments suivants :

- Date de l'événement
- Statut de la transaction
- Identifiant du VI
- Identifiant de l'organisme client
- URL de la page
- Action réalisée le cas échéant

NB : comme il est précisé dans la spécification du VI (cf. [VI]), le VI désigne l'élément signé, soit :

- **L'assertion SAML 1.1 ou 2.0 dans Interops-A**
- **La réponse SAML 2.0 dans Interops-P ou Interops-S**

3.4 Demande de traces de vérification et de traces applicatives

3.4.1 Description du cas d'usage

Ce cas d'utilisation doit permettre à un **demandeur** de récupérer des traces de vérification et des traces applicatives auprès d'un **organisme fournisseur**. Ce demandeur peut être un organisme client, avec lequel l'organisme fournisseur a contractualisé ou un tiers ayant les habilitations nécessaires.

Le demandeur dans une **demande** indique le ou les identifiants de VI et l'identifiant de l'organisme client pour lesquels il désire obtenir des informations.

L'organisme fournisseur doit vérifier que la demande est valide, c'est-à-dire que l'identifiant de l'organisme correspond bien à l'organisme client ou, dans le cas d'un tiers, qu'il a les habilitations requises.

L'organisme fournisseur transmet une **réponse** au demandeur

L'organisme fournisseur indique pour chaque VI si :

- La vérification a réussie
- La vérification a échouée
- Le VI n'existe pas

L'organisme fournisseur indique également dans sa réponse les traces applicatives correspondant à la session ouverte pour l'assertion donnée si la vérification a réussie.

3.4.2 Diagramme de séquence

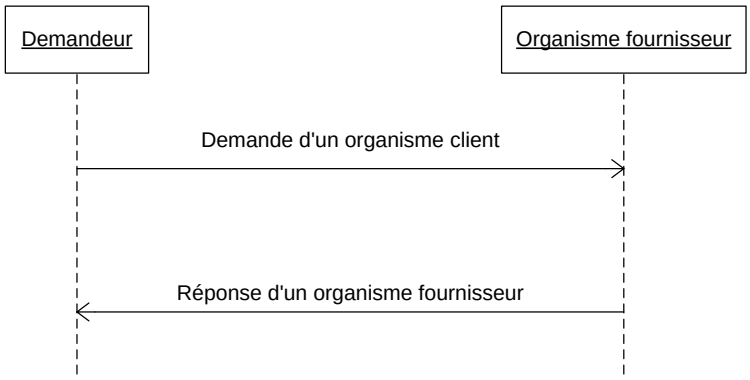

Figure 1 : diagramme de séquence d'une demande de traces de vérification et de traces applicatives

3.5 Déclaration de comportement suspect

3.5.1 Description du cas d'usage

L'organisme client ne peut transmettre l'identité réelle de l'utilisateur qui s'est connecté à partir de son SI à une application hébergée par un organisme fournisseur.

Dans le cas où l'organisme fournisseur détecte un comportement suspect, il contact l'organisme client en lui transmettant la liste des VI relative au comportement suspect. La liste des VI est transmise dans une **demande**. Les VI sont identifiés par l'identifiant de l'assertion et l'identifiant de l'organisme client.

L'organisme client doit alors :

- Vérifier qu'il a effectivement émis ces assertions
- Investiguer pour connaître l'origine du problème (utilisateur frauduleux, usurpation d'identité, etc.)

L'organisme client préviendra l'organisme fournisseur des mesures qui auront été prises.

3.5.2 Diagramme de séquence

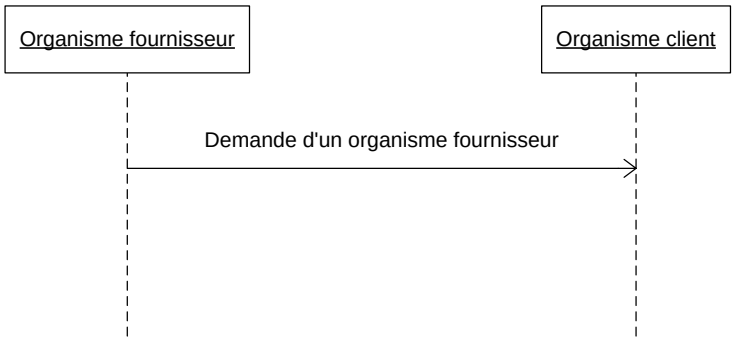

Figure 2 : diagramme de séquence de déclaration de comportement suspect

4. FORMAT DES DONNEES

4.1 Principes

Les données (demande ou réponse) seront des éléments de schéma XML.

La description de ces éléments est faite dans la suite du chapitre. Le schéma XML est disponible en annexe au §5.1 p4.

Le namespace défini par le schéma est :

`urn:interops:fr:SchemaTracesPivot:1.0`

La méthode de transfert de ces données XML ne fait pas partie de ce document. Ils peuvent être échangés par mail, FTP, etc.

4.2 Demande

L'élément `Demande` représente une demande générique qui peut être :

- Une demande de traces de vérification et de traces applicatives
- Une déclaration de comportement suspect

Elle permet de lister les VI en précisant l'identifiant du VI et de l'organisme client.

La figure ci-dessous illustre le type `Demande` :

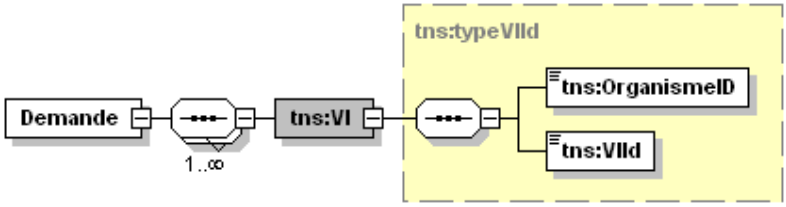

Figure 3 : type `Demande`

Le tableau suivant donne le format des éléments contenu dans l'élément `Demande` :

Nom	Description	Type	Obligatoire	Min	Max
`VI`	Conteneur des paramètres de rapprochement pour un VI	Complexe	Oui	1	1
`OrganismeID`	Identifiant de l'organisme	URI[1]	Oui	1	1
`VIId`	Identifiant du VI	NCName[2]	Oui	1	1

4.3 Réponse

L'élément `Reponse` représente une réponse d'un organisme fournisseur à une demande.

La figure ci-dessous illustre le type `Reponse` :

[1] Cf. http://www.w3.org/TR/xmlschema-2/#anyURI
[2] Cf. http://www.w3.org/TR/xmlschema-2/#NCName

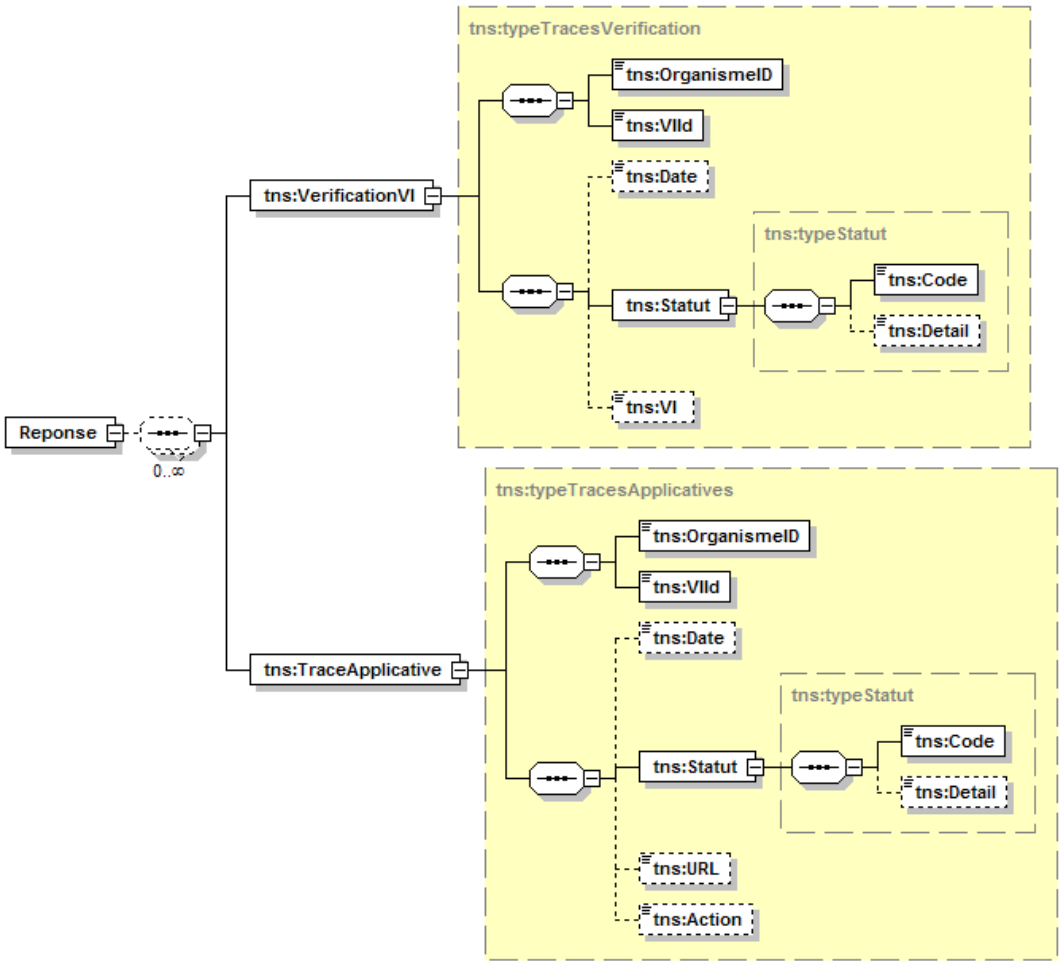

Figure 4 : type `Reponse`

Le tableau suivant donne le format des éléments contenu dans l'élément `Reponse` :

Nom	Description	Type	Obligatoire	Min	Max
`VerificationVI`	Conteneur des éléments de vérification du VI	Complexe	Oui	0	∞
`TraceApplicative`	Conteneur des éléments de traces applicatives	Complexe	Oui	0	∞

4.3.1 Élément VerificationVI

L'élément VerificationVI s'appuie sur le type « typeTracesVerification ». Il permet de représenter les éléments d'une trace de vérification de VI.

Le tableau suivant donne le format des champs du type complexe « typeTracesVerification » :

Nom	Description	Type	Obligatoire	Min	Max
`OrganismeID`	Identifiant de l'organisme client	URI[3]	Oui	1	1
`VIId`	Identifiant du VI	NCName[4]	Oui	1	1

[3] Cf. http://www.w3.org/TR/xmlschema-2/#anyURI
[4] Cf. http://www.w3.org/TR/xmlschema-2/#NCName

Date	Date et heure de l'événement (vérification du VI) d'après le temps universel (UTC)	dateTime[5]	Non	0	1
Statut	Définit le statut de la vérification	Complexe	Oui	1	1
Code	Code de retour	String	Oui	1	1
Detail	Contient des détails, notamment en cas d'échec	String	Non	0	1
VI	Contient le VI vérifié. Il est transmis encodé en Base64	String	Non	0	1

Les valeurs que peut prendre le champ Code de l'élément Statut sont décrites dans le tableau suivant :

Valeur	Description
Success	La vérification a réussi
Failed	La vérification a échoué
NotFound	Le VI n'a pas été trouvé
Undetermined	Autres cas

Les éléments Date et VI sont obligatoires si l'identifiant du VI a effectivement été trouvé (champ « Code » différent de « NotFound »).

4.3.1 Élément TraceApplicative

L'élément TraceApplicative s'appuie sur le type « typeTraceApplicative ». Il permet de représenter les éléments d'une trace applicative (génération d'un contexte de sécurité, trace de l'application visée).

Le tableau suivant donne le format des champs du type complexe « typeTraceApplicative » :

Nom	Description	Type	Obligatoire	Min	Max
OrganismeID	Identifiant de l'organisme client	URI	Oui	1	1
VIId	Identifiant du VI	NCName	Oui	1	1
Date	Date et heure de l'événement (trace applicative) d'après le temps universel (UTC)	dateTime	Non	0	1
Statut	Définit le statut de la transaction (accès à une page, action réalisée, etc.)	Complexe	Oui	1	1
Code	Code de retour	String	Oui	1	1
Detail	Contient des détails, notamment en cas d'échec	String	Non	0	1
URL	URL de la page accédée durant la transaction	String	Non	0	1
Action	Description de l'action effectuée par l'utilisateur ou l'application cliente	String	Non	0	1

Les valeurs que peut prendre le champ Code de l'élément Statut sont décrites dans le tableau suivant :

[5] Cf. http://www.w3.org/TR/xmlschema-2/#dateTime

Valeur	Description
`Success`	Le service a été rendu (quel que soit le résultat de du service par ailleurs)
`Failed`	Le service n'a pas pu être rendu
`NotFound`	Le VI n'a pas été trouvé
`Undetermined`	Autres cas

Les éléments `Date`, `URL` et `Action` ne sont présents que si l'identifiant du VI a effectivement été trouvé (champ « Code » différent de « NotFound »).

La convention technique permet d'indiquer la présence ou non du champ action ainsi qu'un descriptif de son contenu (paramètres d'entrée, résultats, etc.).

L'organisme fournisseur doit décrire son contenu de manière à ce qu'il soit interprétable par l'organisme client.

5. ANNEXE

5.1 Schéma

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:tns="urn:interops:fr:SchemaTracesPivot:1.0"
targetNamespace="urn:interops:fr:SchemaTracesPivot:1.0"
elementFormDefault="qualified" attributeFormDefault="unqualified">
     <complexType name="typeVIId">
          <sequence>
               <element name="OrganismeID" type="anyURI"/>
               <element name="VIId" type="NCName"/>
          </sequence>
     </complexType>
     <complexType name="typeTracesVerification">
          <complexContent>
               <extension base="tns:typeVIId">
                    <sequence>
                         <element name="Date" type="dateTime"
minOccurs="0"/>
                         <element name="Statut" type="tns:typeStatut"/>
                         <element name="VI" type="string"
minOccurs="0"/>
                    </sequence>
               </extension>
          </complexContent>
     </complexType>
     <complexType name="typeTracesApplicatives">
          <complexContent>
               <extension base="tns:typeVIId">
                    <sequence>
                         <element name="Date" type="dateTime"/>
                         <element name="Statut" type="tns:typeStatut"/>
                         <element name="URL" type="string"/>
                         <element name="Action" type="string"
nillable="false" minOccurs="0"/>
                    </sequence>
               </extension>
          </complexContent>
     </complexType>
     <complexType name="typeStatut">
          <sequence>
               <element name="Code">
                    <simpleType>
                         <restriction base="string">
                              <enumeration value="Success"/>
                              <enumeration value="Failed"/>
                              <enumeration value="NotFound"/>
                              <enumeration value="Undetermined"/>
                         </restriction>
                    </simpleType>
               </element>
               <element name="Detail" type="string" nillable="false"
minOccurs="0"/>
          </sequence>
          <!--
-->
```

```
     </complexType>
     <element name="Demande">
          <complexType>
               <sequence maxOccurs="unbounded">
                    <element name="VI" type="tns:typeVIId"/>
               </sequence>
          </complexType>
     </element>
     <element name="Reponse">
          <complexType>
               <sequence minOccurs="0" maxOccurs="unbounded">
                    <element name="VerificationVI"
type="tns:typeTracesVerification"/>
                    <element name="TraceApplicative"
type="tns:typeTracesApplicatives"/>
               </sequence>
          </complexType>
     </element>
</schema>
```