



*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

## **Spécifications du Vecteur d'Identification**

**Standard d'interopérabilité entre organismes de la sphère sociale**

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

1  
2  
3

<b>Référence :</b>	Standard Interops2.0_SpécificationsVI
<b>Version :</b>	2.0
<b>Date de dernière mise à jour :</b>	05/04/2012
<b>Niveau de confidentialité :</b>	PUBLIC

4

## Table des mises à jour du document

5  
6

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

7

## SOMMAIRE

<b>SOMMAIRE</b> .....	<b>3</b>
<b>1. INTRODUCTION</b> .....	<b>4</b>
1.1 Objet du document.....	4
1.2 Relation avec d'autres documents .....	4
1.3 Organisation et structure du document.....	4
1.4 Notations.....	4
1.5 Références.....	5
1.5.1 Références internes.....	5
1.5.2 Références externes.....	5
<b>2. ELEMENTS DU VECTEUR D'IDENTIFICATION</b> .....	<b>6</b>
2.1 Présentation.....	6
2.2 Format du vecteur d'identification .....	7
2.2.1 Format d'une assertion SAML 1.1 .....	7
2.2.2 Format d'une assertion SAML 2.0 .....	8
2.2.3 Format d'une réponse SAML 2.0.....	10
2.3 Description des éléments d'un Jeton SAML.....	12
2.3.1 Eléments communs .....	13
2.3.2 Eléments propres à SAML 1.1.....	14
2.3.3 Eléments propres à SAML 2.0.....	15
2.3.4 Description des éléments d'une réponse SAML.....	16
2.4 Utilisation du Vecteur d'Identification pour le mode application à application .....	17
2.5 Utilisation du Vecteur d'Identification pour le mode portail à portail.....	17
<b>3. ANNEXES</b> .....	<b>19</b>
3.1 Exemple d'assertion SAML 1.1 pour le mode application à application.....	19
3.2 Exemple d'assertion SAML 2.0 pour le mode application à application.....	20
3.3 Exemple de réponse SAML 2.0 pour le mode portail à portail .....	22

38

## 1. INTRODUCTION

---

39

### 1.1 Objet du document

40

Ce document présente les spécifications détaillées du Vecteur d'Identification du Standard d'Interopérabilité des Organismes de la Sphère Sociale [R1].

41

42

### 1.2 Relation avec d'autres documents

43

Ce document complète le Standard [R1].

44

### 1.3 Organisation et structure du document

45

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

46

- Le chapitre 2 « **Eléments du Vecteur d'identification** » regroupe une description succincte des éléments du Vecteur d'identification, son format et un exemple

47

48

- Le chapitre 3 « **Annexes** » rassemble les annexes, les références et un exemple de Vecteur d'identification

49

50

### 1.4 Notations

51

Les namespaces suivants seront utilisés :

52

- **ds**

53

Représente le namespace XML-DSig

54

<http://www.w3.org/2000/09/xmlsig#>

55

- **saml**

56

Représente le namespace SAML Assertions V1.1

57

<urn:oasis:names:tc:SAML:1.0:assertion>

58

- **saml2**

59

Représente le namespace SAML Assertions V2.0

60

<urn:oasis:names:tc:SAML:2.0:assertion>

61

- **xs**

62

Représente le namespace spécifiant le schéma XML

63

<http://www.w3.org/2001/XMLSchema>

64

65

## 1.5 Références

66

### 1.5.1 Références internes

Référence	Titre	Auteur	Ver.	Date
[R1]	Standard Interops2.0_Specifications Fonctionnelles	Groupe de travail Interops	2.0	05/04/2012

67

### 1.5.2 Références externes

	Titre	Auteur	Date
[RFC4122]	A Universally Unique Identifier (UUID) URN Namespace	P. Leach, M. Mealling, R. Salz	07/2005
[RGS]	Référentiel Général de Sécurité version 1.0	ANSSI/DGME	06/05/2010
[RGS_A_14]	Référentiel Général de Sécurité version 1.0 Annexe A14 : Profils de Certificats / LCR / OCSP et Algorithmes Cryptographiques	ANSSI/DGME	11/02/2010
[RGS_B_1]	Référentiel Général de Sécurité version 1.0 Annexe B1 : Mécanismes cryptographiques	ANSSI/DGME	26/01/2010
[SAMLCore]	Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1	Eve Maler, Prateek Mishra, Rob Philpott	02/09/2003
[SAML2Core]	Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0	Cantor, Scott, Kemp, John, Philpott, Rob, Maler, Eve	15/03/2005
[SAML2Authn Cxt]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0	J. Kemp et al	15/03/2005

## 2. ELEMENTS DU VECTEUR D'IDENTIFICATION

### 2.1 Présentation

Le Vecteur d'Identification doit contenir *a minima* les éléments du tableau suivant :

N°	Elément du vecteur d'identification
1	Numéro de version pour le format du vecteur d'identification
2	Identifiant de vecteur unique pour tous les organismes
3	Identifiant de l'Organisme Client
4	Identifiant de l'utilisateur ou de l'application cliente, éventuellement dépersonnalisé. Il est fortement recommandé d'utiliser un identifiant persistant (cf. paragraphe 2.3 « Description des éléments d'un Jeton SAML »).
5	Date de création
6	Durée de vie de l'habilitation
7	Identifiant de l'Organisme Fournisseur de service
8	Service visé (sous forme d'URI sans partie locale)
9	Liste des PAGM valides pour l'utilisateur ou l'application cliente
10	Attributs Optionnels facultatifs concernant l'identification de l'utilisateur ou de l'application cliente (indication géographique, localisation, niveau de sécurité,...). Ces attributs ne doivent pas contenir de données applicatives.
11	Niveau d'authentification initiale (moyen ou niveau de moyen avec lequel l'authentification initiale de l'utilisateur ou de l'application cliente est réalisée)
12	Signature numérique délivrée par l'organisme de départ

SAML 1.1 ou 2.0 est utilisé pour transmettre les informations du vecteur d'identification.

La signature par l'organisme client permet à tout instant de vérifier l'origine du vecteur d'identification et d'en assurer l'intégrité des informations contenues, telles que les PAGM, la durée de validité, etc. Le vecteur d'identification peut être conservé tel quel pour archivage

Certains des éléments du vecteur d'identification sont conventionnels :

- Le numéro de version pour le format du vecteur d'identification
- L'identifiant de l'Organisme Client
- L'identifiant de l'Organisme Fournisseur de service
- Le service visé (sous forme d'URI sans partie locale)
- La durée de vie de l'habilitation
- Les certificats de signature
- Les PAGM possibles pour le service visé

***☞ Dans le cas où les échanges devront être sécurisés en utilisant des mécanismes conformes au Référentiel Général de Sécurité, les moyens cryptographiques utilisés devront suivre les préconisations contenues dans le [RGS]. En particulier, les tailles de clés et algorithmes utilisés devront***

89 **respecter [RGS\_B\_1] et les profils de certificats devront s'appuyer sur**  
90 **[RGS\_A\_14].**

91 **☞ C'est particulièrement effectif dans le cas de la signature du VI puisqu'on**  
92 **utilise ici la fonction de sécurité « cachet serveur »**

93  
94 D'autres éléments sont définis à la génération du vecteur d'identification à partir du contexte de  
95 sécurité de l'organisme client :

- 96 • L'identifiant de vecteur unique pour tous les organismes
- 97 • L'identifiant de l'utilisateur ou de l'application cliente, éventuellement dépersonnalisé
- 98 • La Date de création
- 99 • Les Attributs Optionnels
- 100 • La liste des PAGM valides pour l'utilisateur ou l'application cliente
- 101 • Le niveau d'authentification initiale

102 **NB : Par convention et sauf précision contraire, dans ce document et dans les autres**  
103 **documents spécifiant le standard Interops, le terme VI désignera l'élément signé. C'est-à-**  
104 **dire :**

- 105 • **L'assertion SAML 1.1 ou 2.0 dans Interops-A**
- 106 • **La réponse SAML 2.0 dans Interops-P**

## 107 2.2 Format du vecteur d'identification

108 Le vecteur d'identification peut être formaté à l'aide du standard SAML 1.1 ou 2.0.

109 La correspondance entre les informations du vecteur d'identification et d'une assertion SAML,  
110 en fonction de la version de SAML utilisée, est définie dans les paragraphes 2.2.1 et 2.2.2.

### 111 2.2.1 Format d'une assertion SAML 1.1

112 Le format d'une assertion SAML 1.1 est décrit ci-dessous.

113 Chaque mot écrit entre crochets en gras rouge (ex : **[ID]**) est une variable paramétrée dont la  
114 valeur est définie dans le §2.3 p12.

```
115  
116 <?xml version="1.0" encoding="UTF-8"?>  
117 <Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion"  
118 xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Issuer="[Issuer]"  
119 AssertionID="[ID]" MajorVersion="1" MinorVersion="1" IssueInstant="  
120 [IssueInstant]">  
121   <Conditions NotBefore="[NotOnBefore]" NotOnOrAfter="[NotOnOrAfter]">  
122     <AudienceRestrictionCondition>  
123       <Audience>[Audience]</Audience>  
124     </AudienceRestrictionCondition>  
125   </Conditions>  
126   <AuthenticationStatement AuthenticationInstant="[AuthnInstant]"  
127   AuthenticationMethod="[MethodAuthn]">  
128     <Subject>  
129       <NameIdentifier Format="[SubjectFormat]">  
130 uid=[SubjectId]
```

```
131         </NameIdentifier>
132         <SubjectConfirmation>
133             <ConfirmationMethod>
134 urn:oasis:names:tc:SAML:1.0:cm:bearer
135             </ConfirmationMethod>
136         </SubjectConfirmation>
137     </Subject>
138 </AuthenticationStatement>
139 <AttributeStatement>
140     <Subject>
141         <NameIdentifier Format=" [SubjectFormat] ">
142 uid= [SubjectId]
143         </NameIdentifier>
144     </Subject>
145     <Attribute AttributeNamespace="urn:iops:attributs:pagm"
146 AttributeName="PAGM">
147         <AttributeValue> [PAGM] </AttributeValue>
148     </Attribute>
149 </AttributeStatement>
150 <ds:Signature>
151     <ds:SignedInfo>
152         <ds:CanonicalizationMethod
153 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
154         <ds:SignatureMethod
155 Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
156         <ds:Reference URI="# [ID] ">
157             <ds:DigestMethod
158 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
159             <ds:DigestValue>...</ds:DigestValue>
160         </ds:Reference>
161     </ds:SignedInfo>
162     <ds:SignatureValue>...</ds:SignatureValue>
163 </ds:Signature>
164 </Assertion>
```

## 2.2.2 Format d'une assertion SAML 2.0

Le format d'une assertion SAML 2.0 est décrit ci-dessous.

Chaque mot écrit entre crochets en gras rouge (ex : **[ID]**) est une variable paramétrée dont la valeur est définie dans le §2.3 p12.

```
<?xml version="1.0" encoding="UTF-8"?>
```



```
171 <saml2:Assertion Version="2.0" IssueInstant="[IssueInstant]" ID="[ID]"
172 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
173 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
174 xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:assertion
175 http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-
176 2.0.xsd">
177   <saml2:Issuer>[Issuer]</saml2:Issuer>
178   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
179     <ds:SignedInfo>
180       <ds:CanonicalizationMethod
181 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
182       <ds:SignatureMethod
183 Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
184       <ds:Reference URI="#[ID]">
185         <ds:Transforms>
186           <ds:Transform
187 Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
188           <ds:Transform
189 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
190         </ds:Transforms>
191         <ds:DigestMethod
192 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
193         <ds:DigestValue>...</ds:DigestValue>
194       </ds:Reference>
195     </ds:SignedInfo>
196     <ds:SignatureValue>...</ds:SignatureValue>
197   </ds:Signature>
198   <saml2:Subject>
199     <saml2:NameID Format="[SubjectFormat2]"
200 [SubjectId2]</saml2:NameID>
201     <saml2:SubjectConfirmation
202 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
203       <saml2:SubjectConfirmationData
204 NotOnOrAfter="[NotOnOrAfter]" Recipient="[Recipient]" />
205     </saml2:SubjectConfirmation>
206   </saml2:Subject>
207   <saml2:Conditions NotOnOrAfter="[NotOnOrAfter]"
208 NotBefore="[NotOnBefore]">
209     <saml2:AudienceRestriction>
210       <saml2:Audience>[Audience]</saml2:Audience>
211     </saml2:AudienceRestriction>
212   </saml2:Conditions>
213   <saml2:AuthnStatement AuthnInstant="[AuthnInstant]"
214 SessionIndex="[ID]">
215     <saml2:AuthnContext>
```

```
216         <saml2:AuthnContextClassRef>
217 [MethodAuthn2]
218         </saml2:AuthnContextClassRef>
219     </saml2:AuthnContext>
220 </saml2:AuthnStatement>
221 <saml2:AttributeStatement>
222     <saml2:Attribute Name="PAGM">
223         <saml2:AttributeValue> [PAGM] </saml2:AttributeValue>
224     </saml2:Attribute>
225 </saml2:AttributeStatement>
226 </saml2:Assertion>
```

### 227 **2.2.3 Format d'une réponse SAML 2.0**

228 Le format d'une réponse SAML 2.0 est décrit ci-dessous.

229 Chaque mot écrit entre crochets en gras rouge (ex : **[ID]**) est une variable paramétrée dont la  
230 valeur est définie dans le §2.3 p12.

231

```
232 <?xml version="1.0" encoding="UTF-8"?>
233 <samlp:Response Destination="[Destination]"
234 IssueInstant="[IssueInstant]" ID="[ID]" Version="2.0"
235 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
236     <saml:Issuer
237 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"> [Issuer] </saml:Issuer>
238
239     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
240         <ds:SignedInfo>
241             <ds:CanonicalizationMethod
242 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
243             <ds:SignatureMethod
244 Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
245             <ds:Reference URI="#[ID]">
246                 <ds:Transforms>
247                     <ds:Transform
248 Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
249                     <ds:Transform
250 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
251                 </ds:Transforms>
252                 <ds:DigestMethod
253 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
254                 <ds:DigestValue>...</ds:DigestValue>
255             </ds:Reference>
256         </ds:SignedInfo>
257         <ds:SignatureValue>
258         ...
```

```
259         </ds:SignatureValue>
260     </ds:Signature>
261     <samlp:Status>
262         <samlp:StatusCode
263 Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
264     </samlp:Status>
265     <saml:Assertion Version="2.0" IssueInstant="[IssueInstant]"
266 ID="[ID]" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
267 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
268 xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:assertion
269 http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-
270 2.0.xsd">
271         <saml:Issuer>[Issuer]</saml:Issuer>
272         <saml:Subject>
273             <saml:NameID Format="[SubjectFormat2]"
274 [SubjectId2]</saml:NameID>
275             <saml:SubjectConfirmation
276 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
277                 <saml:SubjectConfirmationData
278 NotOnOrAfter="[NotOnOrAfter]" Recipient="[Recipient]" />
279             </saml:SubjectConfirmation>
280         </saml:Subject>
281         <saml:Conditions NotOnOrAfter="[NotOnOrAfter]"
282 NotBefore="[NotOnBefore]">
283             <saml:AudienceRestriction>
284                 <saml:Audience>[Audience]</saml:Audience>
285             </saml:AudienceRestriction>
286         </saml:Conditions>
287         <saml:AuthnStatement AuthnInstant="[AuthnInstant]"
288 SessionIndex="[ID]">
289             <saml:AuthnContext>
290                 <saml:AuthnContextClassRef>[MethodAuthn2]
291             </saml:AuthnContextClassRef>
292             </saml:AuthnContext>
293         </saml:AuthnStatement>
294         <saml:AttributeStatement>
295             <saml:Attribute Name="PAGM">
296                 <saml:AttributeValue>
297 [PAGM]</saml:AttributeValue>
298             </saml:Attribute>
299         </saml:AttributeStatement>
300     </saml:Assertion>
301 </samlp:Response>
```

302

## 2.3 Description des éléments d'un Jeton SAML

303

Les variables sont décrites dans les sections ci-après.

304

Les variables peuvent être :

305

- Communes aux formats SAML 1.1 et 2.0

306

- Propres au format SAML 1.1

307

- Propres au format SAML 2.0

308

- Propre au protocole SAML 2.0

309

### 2.3.1 Éléments communs

310

Les variables communes aux formats SAML 1.1 et 2.0 sont décrites dans le tableau ci-dessous.

311

Nom	Description	Format	Exemple	Élément du VI
<b>ID</b>	Identifiant unique de l'assertion	Le format de l'identifiant doit suivre les recommandations de la RFC 4122 [RFC4122] afin d'assurer l'unicité de l'identifiant	uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6	<b>2</b>
<b>IssueInstant</b>	Instant de génération de l'assertion	Valeur de type <code>xs:dateTime</code> (type de donnée de schéma XML) et doit être exprimée en UTC, sans fuseau horaire	2003-04-17T00:46:02Z	<b>5</b>
<b>Issuer</b>	Identification de l'émetteur de l'assertion, et donc de l'organisme client	Le format de l'identification est une URI. L'organisme client doit être identifié par une URI contenant le numéro de version de l'accord d'interopérabilité	urn:interopers:{SIREN SIRET}:idp:{libre}:version	<b>1, 3</b>
<b>NotOnOrAfter</b>	Date d'expiration de l'assertion La date d'expiration est dépendante de la durée de validité de l'assertion et doit prendre en compte une dérive des horloges des systèmes	Valeur de type <code>xs:dateTime</code> (type de donnée de schéma XML) et doit être exprimée en UTC, sans fuseau horaire	2003-04-17T00:46:02Z	<b>6</b>
<b>NotOnBefore</b>	Date de début de validité de l'assertion La date de début de validité de l'assertion doit prendre en compte une dérive des horloges des systèmes. La date de début de validité doit donc être légèrement avancée par rapport à la date d'émission	Valeur de type <code>xs:dateTime</code> (type de donnée de schéma XML) et doit être exprimée en UTC, sans fuseau horaire	2003-04-17T00:46:02Z	<b>6</b>
<b>Audience</b>	Identifiant du service visé	URI décrivant le service visé. Il est recommandé de décrire le service à l'aide d'une URL, comprenant le nom de domaine de l'organisme fournisseur et le nom du service publics précisés dans l'accord	http://rniam.cnnav.fr	<b>7, 8</b>

<b>AuthnInstant</b>	Instant d'authentification de l'utilisateur sur le SI. A moins de disposer de cette information, l'instant d'authentification peut être égal à l'instant de création de l'assertion	Valeur de type type <code>xs:dateTime</code> (type de donnée de schéma XML) et doit être exprimée en UTC, sans fuseau horaire	2003-04-17T00:46:02Z	
<b>PAGM</b>	Liste des PAGM	L'attribut listant les PAGM doit s'appeler <code>PAGM</code> . Une liste de PAGM peut être donnée en multipliant les éléments <AttributeValue> dans l'élément <Attribute> L'AttributeNamespace doit être <code>urn:iops:attributs:pagm</code> .	<Attribute AttributeNamespace="urn:iops:attributs:pagm" AttributeName="PAGM"> <AttributeValue> PAGM1 </AttributeValue> <AttributeValue> PAGM2 </AttributeValue> </Attribute>	<b>9</b>

312

313

### ➤ Format des identifiants d'organismes

314

La recommandation pour les identifiants d'organisme est la suivante :

315

```
urn:interops:{SIREN|SIRET}:{idp|sp}:{libre}
```

316

L'utilisation du SIREN ou du SIRET pour identifier l'organisme répond à deux besoins :

317

- Unicité sur l'ensemble des organismes
- Indépendance de la nomenclature par rapport aux OPS

318

319

Dans le cas de l'organisme client, la version de la convention **doit** être concaténée à l'identifiant pour donner :

320

```
urn:interops:{SIREN|SIRET}:idp:{libre}:version
```

321

### ➤ Attributs complémentaires

322

D'autres attributs peuvent être ajoutés au VI (élément 10). Dans ce cas, ils doivent être déclarés dans l'unique élément `<saml:AttributeStatement>`.

323

Comme pour les PAGM, un nom et des valeurs et un namespace sont donnés. Ces attributs sont spécifiques à chaque accord d'interopérabilité.

324

## 2.3.2 Éléments propres à SAML 1.1

325

Les variables propres au format SAML 1.1 sont décrites dans le tableau ci-dessous.

326

Nom	Description	Format	Exemple	Élément du VI
<b>SubjectFormat</b>	Identifiant du format de l'identifiant de l'utilisateur ou de l'application cliente pour SAML 1.1	Le format de l'identifiant dépend de l'accord d'interopérabilité. <b>Il est fortement recommandé d'« impersonnifier » les usagers tout en garantissant l'unicité.</b> D'autres formats sont cependant disponible [SAMLCore]	urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName	
<b>SubjectId</b>	Identifiant de l'utilisateur ou de l'application cliente	Dans le cas où le format urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName est pris, l'identifiant, à la charge de l'organisme client, peut être représenté par une chaîne X509	uid=abjj1992	<b>4</b>
<b>MethodAuthn</b>	Méthode d'authentification de l'utilisateur ou de l'application cliente sur le SI de l'organisme client	La méthode d'authentification est une URI. Pour l'ensemble des valeurs normalisées, se reporter à [SAMLCore]	urn:oasis:names:tc:SAML:1.0:am:password	<b>11</b>

327

### 2.3.3 Éléments propres à SAML 2.0

328

Les variables propres au format SAML 2.0 sont décrites dans le tableau ci-dessous.

329

Nom	Description	Format	Exemple	Élément du VI
<b>SubjectFormat2</b>	Identifiant du format de l'identifiant de l'utilisateur ou de l'application cliente pour SAML 2.0	Le format de l'identifiant dépend de l'accord d'interopérabilité. <b>Il est fortement recommandé d'« impersonnifier » les usagers et donc d'utiliser le format urn:oasis:names:tc:SAML:2.0:nameid-format:persistent. Ce format indique qu'un identifiant opaque persistant est utilisé pour identifier les utilisateurs ou les applications clientes. La persistance s'entend comme un identifiant unique pour un utilisateur ou une application cliente dans le cadre d'une relation organisme client – organisme fournisseur donnée, et ce pour une période cohérente avec la durée opérationnelle (durée de</b>	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	

		<b>vie des traces d'audit, de la convention, etc.).</b> D'autres formats sont cependant disponible [SAML2Core]. On peut imaginer que pour « impersonnier » l'utilisateur ou l'application cliente, on régénère l'identifiant aléatoire (transient)		
<b>SubjectId2</b>	Identifiant de l'utilisateur ou de l'application cliente	Dans le cas où le format <code>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</code> est pris, tout identifiant pseudo-aléatoire ne permettant pas d'identifier un utilisateur est utilisable		<b>4</b>
<b>MethodAuthn2</b>	Méthode d'authentification de l'utilisateur sur le SI de l'organisme client	La méthode d'authentification est une URI. Pour l'ensemble des valeurs normalisées, se reporter à [SAML2AuthnCxt]	<code>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</code>	<b>11</b>
<b>Recipient</b>	Identifiant de l'organisme fournisseur	URI identifiant l'organisme client pouvant recevoir l'assertion	<code>urn:interop:sp:{SIREN SIRET}:{libre}</code>	

330

### 2.3.4 Description des éléments d'une réponse SAML

Nom	Description	Format	Exemple
<b>ID</b>	Identifiant unique de la réponse	Le format de l'identifiant doit suivre les recommandations de la RFC 4122 [RFC4122] afin d'assurer l'unicité de l'identifiant	<code>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</code>
<b>IssueInstant</b>	Instant de génération de la réponse	Valeur de type <code>type xs:dateTime</code> (type de donnée de schéma XML) et doit être exprimée en UTC, sans fuseau horaire	<code>2003-04-17T00:46:02Z</code>
<b>Issuer</b>	Identification de l'émetteur de la réponse, et donc de l'organisme client	Le format de l'identification est une URI. L'organisme client doit être identifié par une URI, pouvant contenir le numéro de version de l'accord d'interopérabilité Cet identifiant est identique à l'élément <code>Issuer</code> de l'assertion	<code>urn:interop:idp:{SIREN SIRET}:{libre}:version</code>
<b>Destination</b>	URI identifiant l'adresse du service de réception des assertions	Cette URL correspond à la valeur du paramètre « action » du formulaire utilisé pour soumettre la réponse SAML. L'organisme fournisseur doit vérifier que la valeur de ce champ correspond bien à l'adresse à laquelle elle a été reçue.	<code>https://www.exemple.com:9031/sp/ACS.saml2</code>



331  
332  
333  
334  
335  
336  
337

## 2.4 Utilisation du Vecteur d'Identification pour le mode application à application

Dans le mode application à application, le Vecteur d'Identification est signé. Une signature (enveloppée) XML, correspondant à l'élément 12 du Vecteur d'Identification, est incluse dans l'assertion SAML.

Toutes les implémentations devront supporter le format de signature XML-DSig suivant :

	Description	URN
<b>Algorithme de hachage</b>	SHA1	<a href="http://www.w3.org/2000/09/xmldsig#sha1">http://www.w3.org/2000/09/xmldsig#sha1</a>
<b>Canonicalisation XML</b>	Canonicalisation XML Exclusive	<a href="http://www.w3.org/2001/10/xml-exc-c14n#">http://www.w3.org/2001/10/xml-exc-c14n#</a>
<b>Transformation</b>	Signature enveloppée	<a href="http://www.w3.org/2000/09/xmldsig#envelope-d-signature">http://www.w3.org/2000/09/xmldsig#envelope-d-signature</a>
<b>Signature</b>	RSAwithSHA1	<a href="http://www.w3.org/2000/09/xmldsig#rsa-sha1">http://www.w3.org/2000/09/xmldsig#rsa-sha1</a>

338  
339  
340  
341  
342

La signature XML-DSig doit contenir un élément `ds:KeyInfo` indiquant quelle clé a été employée pour la signature. Toutes les implémentations devront supporter l'insertion des éléments `ds:X509Data` et `ds:X509Certificate`.

Les organismes doivent par ailleurs s'échanger les chaînes de certification.

343  
344  
345

**La signature « cachet serveur » est une fonction de sécurité faisant appel à des mécanismes cryptographiques qui peut nécessiter d'être conforme au RGS. Concernant cette conformité, se reporter à la note du paragraphe 2.1.**

346  
347

La « méthode de confirmation » est fonction de la version de SAML utilisée :

348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358

- Pour SAML 1.1 :
  - o Elle est précisée dans l'élément `/saml:AuthenticationStatement/saml:Subject/saml:SubjectConfirmation/ saml:ConfirmationMethod`
  - o Elle prend la valeur : `urn:oasis:names:tc:SAML:1.0:cm:sender-vouches`
- Pour SAML 2.0 :
  - o Elle est précisée dans l'élément `/saml:Subject/saml:SubjectConfirmation`
  - o Elle prend la valeur : `urn:oasis:names:tc:SAML:2.0:cm:sender-vouches`

359  
360

On pourra se reporter aux paragraphes 3.1 et 3.2 pour des exemples de VI conformes à la spécification.

361

## 2.5 Utilisation du Vecteur d'Identification pour le mode portail à portail

362  
363

Dans le mode portail à portail, le profil Web SSO Post de SAML 2.0 est utilisé : l'assertion SAML jouant le rôle de Vecteur d'Identification est incluse dans une réponse SAML.

364 L'assertion SAML peut être signée, mais la réponse SAML doit être obligatoirement signée. La  
 365 signature de la réponse joue alors le rôle de la signature XML, correspondant à l'élément 12 du  
 366 Vecteur d'Identification.

367 Toutes les implémentations devront supporter le format de signature XML-DSig suivant :

368

	Description	URN
<b>Algorithme de hachage</b>	SHA1	<a href="http://www.w3.org/2000/09/xmldsig#sha1">http://www.w3.org/2000/09/xmldsig#sha1</a>
<b>Canonicalisation XML</b>	Canonicalisation XML Exclusive	<a href="http://www.w3.org/2001/10/xml-exc-c14n#">http://www.w3.org/2001/10/xml-exc-c14n#</a>
<b>Transformation</b>	Signature enveloppée	<a href="http://www.w3.org/2000/09/xmldsig#envelope-d-signature">http://www.w3.org/2000/09/xmldsig#envelope-d-signature</a>
<b>Signature</b>	RSAwithSHA1	<a href="http://www.w3.org/2000/09/xmldsig#rsa-sha1">http://www.w3.org/2000/09/xmldsig#rsa-sha1</a>

369

370 La signature XML-DSig doit contenir un élément `ds:KeyInfo` indiquant quelle clé a été  
 371 employée pour la signature. Toutes les implémentations devront supporter l'insertion des  
 372 éléments `ds:X509Data` et `ds:X509Certificate`.

373 Les organismes doivent par ailleurs s'échanger les chaînes de certification.

374 ***La signature « cachet serveur » est une fonction de sécurité faisant appel à des***  
 375 ***mécanismes cryptographiques qui peut nécessiter d'être conforme au RGS.***  
 376 ***Concernant cette conformité, se reporter à la note du paragraphe 2.1.***

377

378 La méthode de confirmation précisée dans l'élément  
 379 `/saml:Subject/saml:SubjectConfirmation` prend la valeur :

380 `urn:oasis:names:tc:SAML:2.0:cm:bearer`

381

382 On pourra se reporter au paragraphe 3.3 pour un exemple de VI conforme à la spécification.

383

## 3. ANNEXES

384

### 3.1 Exemple d'assertion SAML 1.1 pour le mode application à application

385

Un exemple d'assertion est donné ci-dessous :

386

387

388

389

390

391

```
<saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"  
xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"  
Issuer="urn:iops:saql:idp:1" AssertionID="_d7b830d0-3f39-0410-a4d0-  
91314a1fb6c8" MajorVersion="1" MinorVersion="1" IssueInstant="2007-09-  
03T19:02:25Z">
```

392

393

```
  <saml:Conditions NotBefore="2007-09-03T19:02:15Z"  
NotOnOrAfter="2007-09-03T20:02:35Z">
```

394

395

396

397

```
  <saml:AudienceRestrictionCondition>  
    <saml:Audience>http://adresse-fournisseur/</saml:Audience>  
  </saml:AudienceRestrictionCondition>  
</saml:Conditions>
```

398

399

400

401

402

403

404

405

406

407

```
  <saml:AuthenticationStatement AuthenticationInstant="2007-09-  
03T17:37:27Z"  
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
```

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

```
  <saml:Subject>  
    <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-  
format:unspecified">id-avé-accent-source</saml:NameIdentifier>  
    <saml:SubjectConfirmation>  
      <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:sender-  
vouches</saml:ConfirmationMethod>  
    </saml:SubjectConfirmation>  
  </saml:Subject>  
</saml:AuthenticationStatement>  
<saml:AttributeStatement>  
  <saml:Subject>  
    <saml:NameIdentifier  
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"  
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">id-avé-  
accent-source</saml:NameIdentifier>  
  </saml:Subject>  
    <saml:Attribute AttributeNamespace="urn:iops:attributs:pagm"  
AttributeName="PAGM">  
      <saml:AttributeValue>pagm1</saml:AttributeValue>  
    </saml:Attribute>  
    <saml:Attribute AttributeNamespace="urn:iops:attributs:optionnal"  
AttributeName="departement">  
      <saml:AttributeValue>22</saml:AttributeValue>
```

```
425     <saml:AttributeValue>44</saml:AttributeValue>
426     </saml:Attribute>
427     <saml:Attribute AttributeNamespace="urn:iops:attributs:optionnal"
428     AttributeName="ville">
429         <saml:AttributeValue>st_brieuc</saml:AttributeValue>
430         <saml:AttributeValue>Nantes</saml:AttributeValue>
431     </saml:Attribute>
432 </saml:AttributeStatement>
433 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
434 <SignedInfo>
435 <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
436 c14n#" />
437 <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
438 sha1" />
439 <Reference URI="#_d7b830d0-3f39-0410-a4d0-91314a1fb6c8">
440 <Transforms>
441 <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
442 signature" />
443 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
444 </Transforms>
445 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
446 <DigestValue>YaJbbcU5f...lJdzCcE=</DigestValue>
447 </Reference>
448 </SignedInfo>
449 <SignatureValue>eD5Rkt6RQC...CwkIZjWLSsE=</SignatureValue>
450 <KeyInfo>
451 <X509Data>
452 <X509Certificate>MIIB2DCCAUGg...lmFkJn7/Ng=</X509Certificate>
453 <X509Certificate>MIIB4jCCAUGg...GFe7QdEO</X509Certificate>
454 <X509Certificate>MIIB3TCCAUAQ...pA==</X509Certificate>
455 </X509Data>
456 </KeyInfo>
457 </Signature></saml:Assertion>
```

## 458 3.2 Exemple d'assertion SAML 2.0 pour le mode application à application

```
459 <saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
460 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
461 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
462 xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:assertion
463 http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-
464 2.0.xsd" ID="_86bb16eb-3f39-0410-9d53-919a2d5a47b9" Version="2.0"
465 IssueInstant="2007-09-03T19:09:56Z">
```

```
466 <saml:Issuer>urn:iops:saql:idp:2</saml:Issuer><Signature
467 xmlns="http://www.w3.org/2000/09/xmldsig#">
468 <SignedInfo>
469 <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
470 c14n#" />
471 <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
472 sha1" />
473 <Reference URI="#_86bb16eb-3f39-0410-9d53-919a2d5a47b9">
474 <Transforms>
475 <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
476 signature" />
477 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
478 </Transforms>
479 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
480 <DigestValue>59QJ/N...zTtwPZIw0=</DigestValue>
481 </Reference>
482 </SignedInfo>
483 <SignatureValue>QKWB9mK...tQnWRFmL78=</SignatureValue>
484 <KeyInfo>
485 <X509Data>
486 <X509Certificate>MIIB2DCCAUG...61mFkJn7/Ng=</X509Certificate>
487 <X509Certificate>MIIB4jCCAUu...GFe7QdEO</X509Certificate>
488 <X509Certificate>MIIB3TCCAUa...BqxnwnpnpA==</X509Certificate>
489 </X509Data>
490 </KeyInfo>
491 </Signature>
492 <saml:Subject>
493 <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
494 format:entity">identifiant-source</saml:NameID>
495 <saml:SubjectConfirmation
496 Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">
497 <saml:SubjectConfirmationData NotOnOrAfter="2007-09-
498 03T20:10:06Z" Recipient="urn:iops:saql:sp" />
499 </saml:SubjectConfirmation>
500 </saml:Subject>
501 <saml:Conditions NotBefore="2007-09-03T19:09:46Z"
502 NotOnOrAfter="2007-09-03T20:10:06Z">
503 <saml:AudienceRestriction>
504 <saml:Audience>http://adresse-fournisseur/</saml:Audience>
505 </saml:AudienceRestriction>
506 </saml:Conditions>
```

```
507 <saml:AuthnStatement AuthnInstant="2007-09-03T17:44:57Z"  
508 SessionIndex="_86bb16eb-3f39-0410-9d53-919a2d5a47b9">  
509 <saml:AuthnContext>  
510 <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unsp  
511 ecified</saml:AuthnContextClassRef>  
512 </saml:AuthnContext>  
513 </saml:AuthnStatement>  
514 <saml:AttributeStatement>  
515 <saml:Attribute Name="PAGM">  
516 <saml:AttributeValue>pagml</saml:AttributeValue>  
517 </saml:Attribute>  
518 </saml:AttributeStatement>  
519 </saml:Assertion>
```

### 520 3.3 Exemple de réponse SAML 2.0 pour le mode portail à portail

```
521 <samlp:Response xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
522 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"  
523 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_2226f7ff-3f39-  
524 0410-9d53-919a2d5a47b9" Version="2.0" IssueInstant="2007-09-  
525 03T19:15:46Z" Destination="http://destination-adresse/"  
526 xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:assertion  
527 http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-  
528 2.0.xsd">  
529 <saml:Issuer>urn:iops:saql:idp:4</saml:Issuer><Signature  
530 xmlns="http://www.w3.org/2000/09/xmldsig#">  
531 <SignedInfo>  
532 <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-  
533 c14n#" />  
534 <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-  
535 sha1" />  
536 <Reference URI="#_2226f7ff-3f39-0410-9d53-919a2d5a47b9">  
537 <Transforms>  
538 <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-  
539 signature" />  
540 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />  
541 </Transforms>  
542 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />  
543 <DigestValue>CO4voR...Wt4QD4cA=</DigestValue>  
544 </Reference>  
545 </SignedInfo>  
546 <SignatureValue>UCKCy48G...zMc9MZq4k=</SignatureValue>  
547 <KeyInfo>  
548 <X509Data>
```

```
549 <X509Certificate>MIIB2DCCA...61mFkJn7/Ng=</X509Certificate>
550 <X509Certificate>MIIB4jCCA...GF7QdEO</X509Certificate>
551 <X509Certificate>MIIB3TCCA...BqxwnpnpA==</X509Certificate>
552 </X509Data>
553 </KeyInfo>
554 </Signature>
555   <samlp:Status>
556     <samlp:StatusCode
557 Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
558   </samlp:Status>
559   <saml:Assertion ID="_3a26f7ff-3f39-0410-9d53-919a2d5a47b9"
560 Version="2.0" IssueInstant="2007-09-03T19:15:46Z">
561     <saml:Issuer>urn:iops:saql:idp:4</saml:Issuer>
562     <saml:Subject>
563       <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
564 format:entity">identifiant-source</saml:NameID>
565       <saml:SubjectConfirmation
566 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
567         <saml:SubjectConfirmationData NotOnOrAfter="2007-09-
568 03T20:15:56Z" Recipient="urn:iops:saql:sp"/>
569       </saml:SubjectConfirmation>
570     </saml:Subject>
571     <saml:Conditions NotBefore="2007-09-03T19:15:36Z"
572 NotOnOrAfter="2007-09-03T20:15:56Z">
573       <saml:AudienceRestriction>
574         <saml:Audience>http://adresse-fournisseur/</saml:Audience>
575       </saml:AudienceRestriction>
576     </saml:Conditions>
577     <saml:AuthnStatement AuthnInstant="2007-09-03T17:50:48Z"
578 SessionIndex="_3a26f7ff-3f39-0410-9d53-919a2d5a47b9">
579       <saml:AuthnContext>
580 <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unsp
581 ecified</saml:AuthnContextClassRef>
582       </saml:AuthnContext>
583     </saml:AuthnStatement>
584     <saml:AttributeStatement>
585       <saml:Attribute Name="PAGM">
586         <saml:AttributeValue>pagml</saml:AttributeValue>
587       </saml:Attribute>
588     </saml:AttributeStatement>
589   </saml:Assertion>
590 </samlp:Response>
```