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

Référence : **Version :** **Date de dernière mise à jour :**	Standard Interops2.0_SpécificationsVI 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

SOMMAIRE 3

1. INTRODUCTION 4
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

2. ELEMENTS DU VECTEUR D'IDENTIFICATION 6
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

3. ANNEXES 19
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

1. INTRODUCTION

1.1 Objet du document

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

1.2 Relation avec d'autres documents

Ce document complète le Standard [R1].

1.3 Organisation et structure du document

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

- Le chapitre 2 « **Eléments du Vecteur d'identification** » regroupe une description succincte des éléments du Vecteur d'identification, son format et un exemple
- Le chapitre 3 « **Annexes** » rassemble les annexes, les références et un exemple de Vecteur d'identification

1.4 Notations

Les namespaces suivants seront utilisés :

- **`ds`**
  Représente le namespace XML-DSig
  `http://www.w3.org/2000/09/xmldsig#`
- **`saml`**
  Représente le namespace SAML Assertions V1.1
  `urn:oasis:names:tc:SAML:1.0:assertion`
- **`saml2`**
  Représente le namespace SAML Assertions V2.0
  `urn:oasis:names:tc:SAML:2.0:assertion`
- **`xs`**
  Représente le namespace spécifiant le schéma XML
  `http://www.w3.org/2001/XMLSchema`

65 ## 1.5 Références

66 ### 1.5.1 Références internes

Référence		Titre	Auteur	Ver.	Date
[R1]	Standard Interops2.0_SpecificationsFonctionnelles	Spécifications 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
[SAML2AuthnCxt]	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 persistent (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***

respecter [RGS_B_1] et les profils de certificats devront s'appuyer sur [RGS_A_14].

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

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

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

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

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

2.2 Format du vecteur d'identification

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

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

2.2.1 Format d'une assertion SAML 1.1

Le format d'une assertion SAML 1.1 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"?>
<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Issuer="[Issuer]"
AssertionID="[ID]" MajorVersion="1" MinorVersion="1" IssueInstant="
[IssueInstant]">
   <Conditions NotBefore="[NotOnBefore]" NotOnOrAfter="[NotOnOrAfter]">
          <AudienceRestrictionCondition>
                 <Audience>[Audience]</Audience>
          </AudienceRestrictionCondition>
   </Conditions>
   <AuthenticationStatement AuthenticationInstant="[AuthnInstant]"
AuthenticationMethod="[MethodAuthn]">
          <Subject>
                 <NameIdentifier Format="[SubjectFormat]">
uid=[SubjectId]
```

```
                </NameIdentifier>
                <SubjectConfirmation>
                        <ConfirmationMethod>
urn:oasis:names:tc:SAML:1.0:cm:bearer
                        </ConfirmationMethod>
                </SubjectConfirmation>
        </Subject>
  </AuthenticationStatement>
  <AttributeStatement>
        <Subject>
                <NameIdentifier Format="[SubjectFormat]">
uid=[SubjectId]
                </NameIdentifier>
        </Subject>
        <Attribute AttributeNamespace="urn:iops:attributs:pagm"
AttributeName="PAGM">
                <AttributeValue>[PAGM]</AttributeValue>
        </Attribute>
  </AttributeStatement>
  <ds:Signature>
        <ds:SignedInfo>
                <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                <ds:Reference URI="#[ID]">
                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>...</ds:DigestValue>
                </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
  </ds:Signature>
</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"?>
```

```
<saml2:Assertion Version="2.0" IssueInstant="[IssueInstant]" ID="[ID]"
xmlns:saml2="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">
   <saml2:Issuer>[Issuer]</saml2:Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
                 <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                 <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                 <ds:Reference URI="#[ID]">
                        <ds:Transforms>
                               <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                               <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        </ds:Transforms>
                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>...</ds:DigestValue>
                 </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>...</ds:SignatureValue>
   </ds:Signature>
   <saml2:Subject>
          <saml2:NameID Format="[SubjectFormat2]">
[SubjectId2]</saml2:NameID>
          <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                 <saml2:SubjectConfirmationData
NotOnOrAfter="[NotOnOrAfter]" Recipient="[Recipient]"/>
          </saml2:SubjectConfirmation>
   </saml2:Subject>
   <saml2:Conditions NotOnOrAfter="[NotOnOrAfter]"
NotBefore="[NotOnBefore]">
          <saml2:AudienceRestriction>
                 <saml2:Audience>[Audience]</saml2:Audience>
          </saml2:AudienceRestriction>
   </saml2:Conditions>
   <saml2:AuthnStatement AuthnInstant="[AuthnInstant]"
SessionIndex="[ID]">
          <saml2:AuthnContext>
```

```
                <saml2:AuthnContextClassRef>
[MethodAuthn2]
                </saml2:AuthnContextClassRef>
        </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
        <saml2:Attribute Name="PAGM">
                <saml2:AttributeValue>[PAGM]</saml2:AttributeValue>
        </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```

2.2.3 Format d'une réponse SAML 2.0

Le format d'une réponse 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"?>
<samlp:Response Destination="[Destination]"
IssueInstant="[IssueInstant]" ID="[ID]" Version="2.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">[Issuer]</saml:Issu
er>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
                <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                <ds:Reference URI="#[ID]">
                        <ds:Transforms>
                                <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        </ds:Transforms>
                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>...</ds:DigestValue>
                </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
        ...
```

```
          </ds:SignatureValue>
   </ds:Signature>
   <samlp:Status>
          <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
   </samlp:Status>
   <saml:Assertion Version="2.0" IssueInstant="[IssueInstant]"
ID="[ID]" xmlns:saml="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">
          <saml:Issuer>[Issuer]</saml:Issuer>
          <saml:Subject>
                 <saml:NameID Format="[SubjectFormat2]">
[SubjectId2]</saml:NameID>
                 <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                        <saml:SubjectConfirmationData
NotOnOrAfter="[NotOnOrAfter]" Recipient="[Recipient]"/>
                 </saml:SubjectConfirmation>
          </saml:Subject>
          <saml:Conditions NotOnOrAfter="[NotOnOrAfter]"
NotBefore="[NotOnBefore]">
                 <saml:AudienceRestriction>
                        <saml:Audience>[Audience]</saml:Audience>
                 </saml:AudienceRestriction>
          </saml:Conditions>
          <saml:AuthnStatement AuthnInstant="[AuthnInstant]"
SessionIndex="[ID]">
                 <saml:AuthnContext>
                        <saml:AuthnContextClassRef>[MethodAuthn2]
                        </saml:AuthnContextClassRef>
                 </saml:AuthnContext>
          </saml:AuthnStatement>
          <saml:AttributeStatement>
                 <saml:Attribute Name="PAGM">
                        <saml:AttributeValue>
[PAGM]</saml:AttributeValue>
                 </saml:Attribute>
          </saml:AttributeStatement>
   </saml:Assertion>
</samlp:Response>
```

2.3 Description des éléments d'un Jeton SAML

Les variables sont décrites dans les sections ci-après.

Les variables peuvent être :

- Communes aux formats SAML 1.1 et 2.0
- Propres au format SAML 1.1
- Propres au format SAML 2.0
- Propre au protocole SAML 2.0

2.3.1 Eléments communs

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

Nom	Description	Format	Exemple	Elément du VI
ID	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`	**2**
IssueInstant	Instant de génération de l'assertion	Valeur de type type `xs:dateTime` (type de donnée de schéma XML) et doit être exprimée en UTC, sans fuseau horaire	`2003-04-17T00:46:02Z`	**5**
Issuer	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:interops:{SIREN|SIRET}:idp:{libre}:version`	**1, 3**
NotOnOrAfter	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 type `xs:dateTime` (type de donnée de schéma XML) et doit être exprimée en UTC, sans fuseau horaire	`2003-04-17T00:46:02Z`	**6**
NotOnBefore	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 `xs:dateTime` (type de donnée de schéma XML) et doit être exprimée en UTC, sans fuseau horaire	`2003-04-17T00:46:02Z`	**6**
Audience	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.cnav.fr`	**7, 8**

AuthnInstant	Instant d'authentification de l'usager 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 `xs:dateTime` (type de donnée de schéma XML) et doit être exprimée en UTC, sans fuseau horaire	`2003-04-17T00:46:02Z`	

PAGM	Liste des PAGM	L'attribut listant les PAGM doit s'appeler `PAGM`.
		Une liste de PAGM peut être donnée en multipliant les éléments `<AttributeValue>` dans l'élément `<Attribute>`
		L'AttributeNamespace doit être `urn:iops:attributs:pagm`.
			`<Attribute AttributeNamespace="urn:iops:attributs:pagm" AttributeName="PAGM">`
			`<AttributeValue>`
			`PAGM1`
			`</AttributeValue>`
			`<AttributeValue>`
			`PAGM2`
			`</AttributeValue>`
			`</Attribute>`
				9

➢ **Format des identifiants d'organismes**

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

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

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

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

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

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

➢ **Attributs complémentaires**

D'autres attributs peuvent être ajoutés au VI (élément 10). Dans ce cas, ils doivent être déclarés dans l'unique élément `<saml:AttributeStatement>`. Comme pour les PAGM, un nom et des valeurs et un namespace sont donnés. Ces attributs sont spécifiques à chaque accord d'interopérabilité.

2.3.2 Eléments propres à SAML 1.1

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

Nom	Description	Format	Exemple	Elément du VI
SubjectFormat	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. **Il est fortement recommandé d'« impersonnifier » les usagers tout en garantissant l'unicité.** D'autres formats sont cependant disponible [SAMLCore]	`urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName`	
SubjectId	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`	**4**
MethodAuthn	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`	**11**

2.3.3 Eléments propres à SAML 2.0

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

Nom	Description	Format	Exemple	Elément du VI
SubjectFormat2	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. **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**	`urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`	

		vie des traces d'audit, de la convention, etc.). D'autres formats sont cependant disponible [SAML2Core]. On peut imaginer que pour « impersonnfier » l'utilisateur ou l'application cliente, on régénère l'identifiant aléatoire (`transient`)		
SubjectId2	Identifiant de l'utilisateur ou de l'application cliente	Dans le cas où le format `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` est pris, tout identifiant pseudo-aléatoire ne permettant pas d'identifier un utilisateur est utilisable		**4**
MethodAuthn2	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]	`urn:oasis:names:tc:SAML:2.0:ac:classes:Password`	**11**
Recipient	Identifiant de l'organisme fournisseur	URI identifiant l'organisme client pouvant recevoir l'assertion	`urn:interops:sp:{SIREN|SIRET}:{libre}`	

330

2.3.4 Description des éléments d'une réponse SAML

Nom	Description	Format	Exemple
ID	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	`f81d4fae-7dec-11d0-a765-00a0c91e6bf6`
IssueInstant	Instant de génération de la réponse	Valeur de type type `xs:dateTime` (type de donnée de schéma XML) et doit être exprimée en UTC, sans fuseau horaire	`2003-04-17T00:46:02Z`
Issuer	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 `Issuer` de l'assertion	`urn:interops:idp:{SIREN|SIRET}:{libre}:version`
Destination	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.	`https://www.exemple.com:9031/sp/ACS.saml2`

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
Algorithme de hachage	SHA1	http://www.w3.org/2000/09/xmldsig#sha1
Canonicalisation XML	Canonicalisation XML Exclusive	http://www.w3.org/2001/10/xml-exc-c14n#
Transformation	Signature enveloppée	http://www.w3.org/2000/09/xmldsig#enveloped-signature
Signature	RSAwithSHA1	http://www.w3.org/2000/09/xmldsig#rsa-sha1

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.

> ***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.***

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

- Pour SAML 1.1 :
  - Elle est précisée dans l'élément `/saml:AuthenticationStatement/saml:Subject/saml:SubjectConfirmation/ saml:ConfirmationMethod`
  - Elle prend la valeur :

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

    `urn:oasis:names:tc:SAML:2.0:cm:sender-vouches`

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

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

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.

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

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

	Description	URN
Algorithme de hachage	SHA1	http://www.w3.org/2000/09/xmldsig#sha1
Canonicalisation XML	Canonicalisation XML Exclusive	http://www.w3.org/2001/10/xml-exc-c14n#
Transformation	Signature enveloppée	http://www.w3.org/2000/09/xmldsig#enveloped-signature
Signature	RSAwithSHA1	http://www.w3.org/2000/09/xmldsig#rsa-sha1

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.

> ***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.***

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

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

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

3. ANNEXES

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

Un exemple d'assertion est donné ci-dessous :

```
<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">
  <saml:Conditions NotBefore="2007-09-03T19:02:15Z"
NotOnOrAfter="2007-09-03T20: 02:35Z">
    <saml:AudienceRestrictionCondition>
      <saml:Audience>http://adresse-fournisseur/</saml:Audience>
    </saml:AudienceRestrictionCondition>
  </saml:Conditions>
  <saml:AuthenticationStatement AuthenticationInstant="2007-09-
03T17:37:27Z"
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
    <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>
```

```
      <saml:AttributeValue>44</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeNamespace="urn:iops:attributs:optionnal"
AttributeName="ville">
      <saml:AttributeValue>st brieuc</saml:AttributeValue>
      <saml:AttributeValue>Nantes</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
<Reference URI="#_d7b830d0-3f39-0410-a4d0-91314a1fb6c8">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>YaJbbcU5f...lJdzCcE=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>eD5Rkt6RQC...CwkIZjWLWSsE=</SignatureValue>
<KeyInfo>
<X509Data>
<X509Certificate>MIIB2DCCAUGg...1mFkJn7/Ng=</X509Certificate>
<X509Certificate>MIIB4jCCAUug...GFe7QdEO</X509Certificate>
<X509Certificate>MIIB3TCCAUag...pA==</X509Certificate>
</X509Data>
</KeyInfo>
</Signature></saml:Assertion>
```

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

```
<saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
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="_86bb16eb-3f39-0410-9d53-919a2d5a47b9" Version="2.0"
IssueInstant="2007-09-03T19:09:56Z">
```

```
  <saml:Issuer>urn:iops:saql:idp:2</saml:Issuer><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
<Reference URI="#_86bb16eb-3f39-0410-9d53-919a2d5a47b9">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>59QJ/N...zTtwPZIw0=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>QKWB9mK...tQnWRFmL78=</SignatureValue>
<KeyInfo>
<X509Data>
<X509Certificate>MIIB2DCCAUG...61mFkJn7/Ng=</X509Certificate>
<X509Certificate>MIIB4jCCAUu...GFe7QdEO</X509Certificate>
<X509Certificate>MIIB3TCCAUa...BqxwnpnpA==</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
  <saml:Subject>
    <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">identifiant-source</saml:NameID>
    <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">
      <saml:SubjectConfirmationData NotOnOrAfter="2007-09-
03T20:10:06Z" Recipient="urn:iops:saql:sp"/>
    </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotBefore="2007-09-03T19:09:46Z"
NotOnOrAfter="2007-09-03T20:10:06Z">
    <saml:AudienceRestriction>
      <saml:Audience>http://adresse-fournisseur/</saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
```

```
  <saml:AuthnStatement AuthnInstant="2007-09-03T17:44:57Z"
SessionIndex="_86bb16eb-3f39-0410-9d53-919a2d5a47b9">
    <saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unsp
ecified</saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
    <saml:Attribute Name="PAGM">
      <saml:AttributeValue>pagm1</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

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

```
<samlp:Response xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_2226f7ff-3f39-
0410-9d53-919a2d5a47b9" Version="2.0" IssueInstant="2007-09-
03T19:15:46Z" Destination="http://destination-adresse/"
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">
  <saml:Issuer>urn:iops:saql:idp:4</saml:Issuer><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
<Reference URI="#_2226f7ff-3f39-0410-9d53-919a2d5a47b9">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>CO4voR...Wt4QD4cA=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>UCKCy48G...zMc9MZq4k=</SignatureValue>
<KeyInfo>
<X509Data>
```

```
<X509Certificate>MIIB2DCCA...61mFkJn7/Ng=</X509Certificate>
<X509Certificate>MIIB4jCCA...GFe7QdEO</X509Certificate>
<X509Certificate>MIIB3TCCA...BqxwnpnpA==</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
  <samlp:Status>
    <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:Assertion ID="_3a26f7ff-3f39-0410-9d53-919a2d5a47b9"
Version="2.0" IssueInstant="2007-09-03T19:15:46Z">
    <saml:Issuer>urn:iops:saql:idp:4</saml:Issuer>
    <saml:Subject>
      <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">identifiant-source</saml:NameID>
      <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData NotOnOrAfter="2007-09-
03T20:15:56Z" Recipient="urn:iops:saql:sp"/>
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2007-09-03T19:15:36Z"
NotOnOrAfter="2007-09-03T20:15:56Z">
      <saml:AudienceRestriction>
        <saml:Audience>http://adresse-fournisseur/</saml:Audience>
      </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2007-09-03T17:50:48Z"
SessionIndex="_3a26f7ff-3f39-0410-9d53-919a2d5a47b9">
      <saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unsp
ecified</saml:AuthnContextClassRef>
      </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
      <saml:Attribute Name="PAGM">
        <saml:AttributeValue>pagm1</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>
</samlp:Response>
```