



**Ministère du budget, des comptes publics et de la fonction publique**

# **Format de signature XAdES de l'administration électronique**

**V1.0**

**AVEC VOUS** l'administration  
**SE MODERNISE**

Format de signature XAdES de l'administration électronique

Référence		Date	
Format de signature Xades V1.0.doc		17/12/2007	
Identification d'objet (OID)		Racine OID et gestionnaire	
1.2.250.1.137.2.1.1.1.1.1		1.2.250.1.137 SDAE	
Responsable		Version	
DGME/SDAE		1.0	
Critère de diffusion		Nombre de pages	
PUBLIC		17	

HISTORIQUE DES VERSIONS

DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
17/12/2007	1.0	Version initiale du document	DGME-SDAE

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	2/18

Références documentaires

Références documentaires normatives

Nota : les URL mentionnés dans ce chapitre ont été collectées à la date de publication du document.

Référence	Document
<b>[XML-1.0]</b>	Nom : XML URL : <a href="http://www.w3.org/XML/Core/">http://www.w3.org/XML/Core/</a> Référence : Extensible Markup Language (XML) 1.0 (Fourth Edition) Date : 16 août 2006 Editeur : W3C
<b>[XML-1.1]</b>	Nom : XML URL : <a href="http://www.w3.org/XML/Core/">http://www.w3.org/XML/Core/</a> Référence : Extensible Markup Language (XML) 1.1 (Second Edition) Date : 16 août 2006 Editeur : W3C
<b>[XML/Dsig]</b>	Nom : XML Signature (Syntax and Processing) URL : <a href="http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/">http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/</a> Référence : xmlsig-core-20020212 Date : 12 février 2002 Editeur : W3C
<b>[XAdES 1.3.2]</b>	Nom : XML Advanced Electronic Signatures URL: <a href="http://webapp.etsi.org/action%5CPU/20060307/ts_101903v010302p.pdf">http://webapp.etsi.org/action%5CPU/20060307/ts_101903v010302p.pdf</a> Référence : ETSI TS 101 903 Version 1.3.2 Date : 6 mars 2006 Editeur : ETSI-ESI
<b>[PRIS V2.1]</b>	Nom : PRISv2.1 URL: <a href="http://synergies-publiquesfr/article.php3?id_article=381">http://synergies-publiquesfr/article.php3?id_article=381</a> Référence : Politique de Référencement Intersectorielle de Sécurité (PRISv2.1) Version : v2.1 Date: 14/11/2006 Editeur: DGME-SDAE
<b>[RFC2119]</b>	Nom : Key words in use for RFC to indicate Requirement Levels URL: <a href="http://www.ietf.org/rfc/rfc2119.txt">http://www.ietf.org/rfc/rfc2119.txt</a> Référence RFC 2119 Date : mars 1997 Editeur: IETF

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	3/18

Références documentaires informatives

<b>[XML/Enc]</b>	<p>Nom: XML Encryption (Syntax and Processing)                  URL: <a href="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/">http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/</a>                  Référence : xmlenc-core-20021210                  Date : 10 décembre 2002                  Éditeur : W3C</p>
<b>[RFC 4051]</b>	<p>Nom: Additional XML Security Uniform Resource Identifiers (URIs)                  URL: <a href="http://www.ietf.org/rfc/rfc4051.txt">http://www.ietf.org/rfc/rfc4051.txt</a>                  Référence: RFC 4051                  Date: avril 2005                  Éditeur : IETF</p>
<b>[RGI]</b>	<p>Nom: Référentiel Général d'Interopérabilité Volet Technique                  URL  <a href="https://www.ateliers.adele.gouv.fr/ministeres/domaines_d_expertise/architecture_fonction/public/rgi/referentiel_general1617/downloadFile/file/Referentiel_General_Interoperabilite_Volet_Technique_V0.90.pdf?nocache=1144939697.22">https://www.ateliers.adele.gouv.fr/ministeres/domaines_d_expertise/architecture_fonction/public/rgi/referentiel_general1617/downloadFile/file/Referentiel_General_Interoperabilite_Volet_Technique_V0.90.pdf?nocache=1144939697.22</a>                  autre URL: <a href="http://synergies-publiques.fr/article.php?id_article=405">http:// synergies-publiques.fr/article.php?id_article=405</a>                  Référence : rgi/referentiel_general1617                  Version : V0.94                  Date: 13 avril 2006                  Éditeur: DGME</p>
<b>[ETSI-ESF]</b>	<p>Nom: Electronic Signature Formats                  URL: <a href="http://www.etsi.org">http://www.etsi.org</a>                  Référence ETSI TS 101 733                  Version : 1.6.3                  Date: septembre 2006                  Éditeur: ETSI-ESI</p>
<b>[ETSI-SIGPOL]</b>	<p>Nom: XML format for signature policies                  URL: <a href="http://www.etsi.org">http://www.etsi.org</a>                  Référence ETSI TS 102 038                  Version : 1.1.1                  Date: avril 2002                  Éditeur: ETSI-ESI</p>

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	4/18

<b>[ISIS-MTT]</b>	<p>Nom: XML Signature and Encryption Message Formats</p> <p>URL:<a href="http://www.isis-mtt.org/uploads/media/ISIS-MTT_Core_Specification_v1.1_03.pdf">http://www.isis-mtt.org/uploads/media/ISIS-MTT_Core_Specification_v1.1_03.pdf</a></p> <p>Référence ISIS-MTT</p> <p>Version : V1.1 Part 8</p> <p>Date: mars 2004</p> <p>Éditeur: ISIS-MTT</p>
<b>[ECOM-XADES]</b>	<p>Nom: XAdES Long Term Signature Format Profile</p> <p>URL <a href="http://www.ecom.jp/LongTermStrage/en/XAdES01_e.pdf">http://www.ecom.jp/LongTermStrage/en/XAdES01_e.pdf</a></p> <p>Référence : XAdES01_e</p> <p>Version V1.0</p> <p>Date: mars 2006</p> <p>Éditeur: Next Generation Electronic Commerce Promotion Council of Japan (ECOM),</p>
<b>[ETSI-ALG]</b>	<p>Nom : Spécification de l'ETSI concernant les algorithmes utilisables dans le contexte des signatures électroniques avancées</p> <p>URL : <a href="http://www.etsi.org/services_products/freestandard/home.htm">http://www.etsi.org/services_products/freestandard/home.htm</a></p> <p>Référence : ETSI TS 102 176-1.</p> <p>Version : V 1.2.1.</p> <p>Date : juillet 2005</p> <p>Éditeur : ETSI</p>
<b>[DCSSI-MC]</b>	<p>Nom : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard</p> <p>URL: <a href="http://www.ssi.gouv.fr/fr/documentation/index.html#politique">http://www.ssi.gouv.fr/fr/documentation/index.html#politique</a></p> <p>Référence : 2791/SGDN/DCSSI/SDS/LCR</p> <p>Version : 1.12</p> <p>Date : 19/12/2006</p> <p>Éditeur : DCSSI</p>
<b>[DCSSI-ALG]</b>	<p>Nom : Algorithmes cryptographiques pour l'interopérabilité du Format v1 de signature électronique XAdES de l'Administration.</p> <p>URL: : <a href="http://www.ssi.gouv.fr/fr/documentation/index.html#xades">http://www.ssi.gouv.fr/fr/documentation/index.html#xades</a></p> <p>Référence : 193/SGDN/DCSSI/SDS</p> <p>Version : 0.4</p> <p>Date : 31/01/2007</p> <p>Éditeur : DCSSI</p>

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	5/18

- 1 - Présentation générale ..... 8**
- 1.1 - **Contexte..... 8**
- 1.2 - **Définitions ..... 8**
- 1.3 - **Périmètre..... 9**
- 1.4 - **Principes retenus pour les signatures ..... 9**
  - 1.4.1 - Documents visés ..... 9
  - 1.4.2 - Nombre de signatures sur le (les) document(s)..... 9
  - 1.4.3 - Politique de signature..... 10
  - 1.4.4 - Politique de document signé ..... 10
  - 1.4.5 - Principes de vérification d'une signature ..... 10
  - 1.4.6 - Choix d'algorithmes de hachage et de signature ..... 10
- 1.5 - **Les standards de signatures électroniques en format XML ..... 10**
- 1.6 - **Synthèse des choix techniques ..... 11**
  - 1.6.1 - Types et nombres de signatures ..... 11
  - 1.6.2 - Politique de signature et Politique de document signé ..... 11
- 1.7 - **Terminologie ..... 11**
- 2 - Détails techniques du format..... 13**
- 2.1 - **Eléments XML ..... 13**
- 2.2 - **Eléments XML-DSIG ..... 13**
  - 2.2.1 - Signature ..... 13
  - 2.2.2 - CanonicalizationMethod ..... 13
  - 2.2.3 - SignatureMethod ..... 14
  - 2.2.4 - Reference URI ..... 14
  - 2.2.5 - DigestMethod..... 14
  - 2.2.6 - KeyInfo..... 14
- 2.3 - **Eléments XAdES..... 15**
  - 2.3.1 - Eléments du schéma XAdES ..... 15
    - 2.3.1.1. Version de la signature XAdES..... 15
    - 2.3.1.2. Qualifying Properties ..... 15
    - 2.3.1.3. SignedProperties..... 16
    - 2.3.1.4. SignedSignatureProperties..... 16
    - 2.3.1.5. CounterSignature ..... 16
  - 2.3.2 - Format XAdES-BES..... 16
    - 2.3.2.1. SigningCertificate ..... 16
    - 2.3.2.2. SigningTime ..... 16
    - 2.3.2.3. ClaimedRoles ..... 17

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	6/18

2.3.2.4.	SignatureProductionPlace .....	17
2.3.2.5.	CommitmentTypeIndication .....	17
2.3.3 -	Format XAdES-EPES .....	17
2.3.3.1.	SignaturePolicyIdentifier .....	18
2.3.3.2.	DataObjectFormat .....	18

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	7/18

# 1 - Présentation générale

---

Ce document spécifie le format de signature XAdES de l'administration électronique à utiliser dans le cadre des échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Son utilisation dans le cadre des échanges ci-dessus est rendue obligatoire par une des règles du Référentiel Général d'Interopérabilité [RGI].

Ce format s'appuie sur les spécifications XAdES de l'ETSI [XAdES-1.3.2].

Il est organisé comme suit :

- le chapitre de présentation générale précise le périmètre et les grands principes de la spécification,
- le chapitre suivant contient les spécifications techniques du format, ainsi que quelques éléments techniques ayant un but didactique sur l'implémentation du standard dans les outils de signature électronique (exemple de [XML-DSIG]).

## 1.1 - Contexte

La présente spécification définit un ensemble de principes, modèles et formats de création et vérification des signatures XAdES utilisées dans le cadre des échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives entre elles.

Le respect de cette spécification par les autorités administratives permet, outre les échanges internes à l'administration, des échanges de documents signés avec des organismes, des entreprises ou des particuliers.

La spécification distingue les opérations réalisées en termes de création et de vérification de signature.

Des documents complémentaires de type "guide de mise en œuvre" pourront être établis par les acteurs de l'administration souhaitant utiliser ce standard dans un contexte d'usage particulier, et par exemple définir des formats de documents, des politiques de signature ou des politiques de documents signés.

Ce document est le résultat de différentes réunions organisées par le DGME/SDAE avec les acteurs concernés des sphères publique et privée.

## 1.2 - Définitions

Ce paragraphe liste les définitions propres à cette spécification. Ces définitions n'ont pas vocation à être utilisées dans d'autres contextes.

**Document signé:** ensemble de données, disponible sous forme d'un ou plusieurs fichiers, comprenant un contenu et une ou plusieurs signatures électroniques.

**Composant d'un document:** partie d'un document qui peut être disponible de manière indépendante, par exemple le contenu du document ou un sous-ensemble du document, ou encore une signature.

**Contenu du document:** ensemble de données initiales du document, disponible sous forme d'un ou plusieurs fichiers, pouvant faire l'objet d'une ou plusieurs signatures.

**Signatures du document:** ensemble de plusieurs signatures d'un document (signé).

**Signature:** données garantissant l'intégrité et l'authenticité d'un composant du document. La partie du document concernée comprend un sous-ensemble ou la totalité du contenu du document, contenant éventuellement des informations supplémentaires (date, rôle, politique, ...) et d'autres signatures (dans le contexte d'une ou plusieurs contre signatures).

**Signature XML-DSIG:** signature créée selon les règles du standard [XML-DSIG].

**Politique de signature:** ensemble de règles qui gouverne la création et la vérification d'une signature (de documents).

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	8/18

**Politique de documents signés:** ensemble de règles qui gouverne la structure d'un document et ses besoins de signature.

**Mécanisme de hachage ou de condensation:** opérations cryptographiques qui permettent à partir de données de taille quelconque d'en déduire une empreinte de taille fixe caractéristique de l'intégrité des données initiales. Ces opérations sont conçues afin qu'il soit impossible de trouver deux jeux de données ayant même résultat.

**Données hachées:** résultat obtenu par application d'un mécanisme de hachage sur des données.

**Partie signée:** ensemble de données qui ont été utilisées en entrée d'une opération de condensation (application d'un mécanisme de hachage) dont le résultat final (hash ou condensat) est utilisé en entrée d'un mécanisme de signature. Une partie signée peut inclure des parties signées implicitement.

**Partie signée implicitement:** une partie signée peut inclure des données hachées. Les données à l'origine font alors implicitement partie des données signées du fait des propriétés des mécanismes de hachage. Il est ainsi possible de signer implicitement des arborescences de données.

## 1.3 - Périmètre

Cette spécification traite uniquement des signatures selon un sous-ensemble de [XAdES 1.3.2], dont elle décrit les règles et les éventuelles restrictions de format.

Les éléments décrits dans cette spécification concernent uniquement les opérations à respecter pour la création et la vérification "immédiate" d'une signature.

## 1.4 - Principes retenus pour les signatures

### 1.4.1 - Documents visés

Le contenu des documents échangés et leur structure sont libres. Par exemple, il peut s'agir de contenus en format XML représentant un formulaire, ou d'un fichier en format PDF/A cf [RG].

Les signatures peuvent porter sur des contenus simples ou composés. Chaque composant d'un document doit être identifiable. L'identification d'un composant peut être explicite (exemple d'une URI ou d'un nom de fichier) ou encore implicite parce que définie par le contexte d'utilisation.

### 1.4.2 - Nombre de signatures sur le (les) document(s)

Les documents peuvent comprendre une ou plusieurs signatures.

**Exemple 1 :** document émis par une administration vers une autre administration

Le document comprend :

- la signature de 3 agents d'un ministère,
- la signature du chef de service validant les 3 premières,
- la signature représentant la "Marianne" du Ministère concerné.

**Exemple 2 :** document émis par une société vers l'Administration

Le document comprend :

- la signature du représentant légal de l'entreprise,
- une signature représentant le cachet de l'entreprise.

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	9/18

### 1.4.3 - Politique de signature

La partie EPES de XAdES permet de référencer une politique de signature. Décrite dans le texte [ETSI-SIGPOL], une politique de signature est un document qui comprend une partie textuelle compréhensible par un lecteur et une partie autre destinée à être utilisée par des outils de création et de vérification de signature.

### 1.4.4 - Politique de document signé

Cette spécification ne traite pas des politiques de documents signés, même si elles sont nécessaires pour l'interopérabilité (exemple de la limitation du nombre de signatures, des règles d'identification des signatures, des structures ou des types de documents).

### 1.4.5 - Principes de vérification d'une signature

La vérification d'une signature d'un document impose :

- d'identifier la ou les signature(s) à vérifier (cas de présence de plusieurs signatures),
- de mettre à disposition les composants de la partie signée du document (par exemple en cas de signature détachée),
- de vérifier l'adéquation de tous les éléments d'identification (dont la politique de signature et l'identification des signataires) avec les politiques de documents signés,
- de vérifier le respect de la politique de signature.

Ceci afin que l'outil utilisé puisse vérifier la signature dans le respect des sous-ensembles XML-DSIG et XAdES définis dans ce document.

### 1.4.6 - Choix d'algorithmes de hachage et de signature

Le choix des algorithmes de hachage et de signature n'est pas imposé par cette spécification, étant traité dans d'autres documents (listes avec identifiants d'algorithmes [RFC-4051], autres références documentaires informatives [ETSI-ALG] et [DCSSI-MC]).

## 1.5 - Les standards de signatures électroniques en format XML

Pour des documents en format XML, le consortium W3C a défini le format de signature XML-DSIG. En termes de fonctionnalités, ce texte diffère des standards de l'IETF S/MIME relatifs aux formats des documents signés.

Afin de répondre aux besoins de la directive européenne sur la signature électronique, ETSI a produit des spécifications supplémentaires pour S/MIME (en particulier CMS) et pour XML-DSIG.

Les formats des Services Web Sécurisés (WSS) du W3C et d'OASIS définissent des extensions de signatures pour des échanges SOAP. Ces standards relatifs à WSS imposent certaines restrictions sur les formats XML-DSIG et ajoutent des extensions qui ne sont pas nécessaires dans un contexte de signature de documents.

Ces contraintes et extensions ne sont pas retenues dans cette spécification. En d'autres termes, les applications en mode SOAP sécurisé (WSS) ne sont pas concernées par le présent document.

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	10/18

## 1.6 - Synthèse des choix techniques

Cette spécification repose sur un empilement de trois socles techniques : XML, XML-DSIG et XAdES. Pour XAdES, seules les parties BES et EPES sont utilisées et aucune recommandation n'est formulée pour ce qui concerne les autres fonctionnalités de XAdES.

L'objectif principal de cette spécification est donc celui de définir les éléments utilisés de ces trois socles.

*Précision : en ce qui concerne le socle XAdES, il ne s'agit pas d'un profil complet.*

### 1.6.1 - Types et nombres de signatures

Le présent document ne définit aucune restriction sur les possibilités de [XML-DSIG] qui peuvent en conséquence toutes être utilisées.

Sont ainsi possibles :

- les signatures enveloppant le contenu du document,
- les signatures enveloppées dans le document,
- les signatures détachées du contenu du document,

ou toutes combinaisons de ces types. Ce document n'impose aucune des règles pour la création ou la vérification de plusieurs signatures.

Les signatures peuvent contenir des attributs qui les qualifient (tels que date, lieu de signature, rôle des signataires, type d'engagement) définis par [XAdES 1.3.2].

### 1.6.2 - Politique de signature et Politique de document signé

Ce document utilise le concept de politique de signature de XAdES-EPES [XAdES 1.3.2].

Aucun traitement automatique des politiques de signature n'est imposé aux outils de création ou vérification de signature. Néanmoins, du fait des possibilités de création ou de vérification par un utilisateur « humain », les outils doivent proposer une fonction d'affichage des règles de la politique de signature.

XAdES-EPES précise que la politique de signature est référencée par une URI (universal resource identifier) ou un URN (universal resource name) représentant un OID (object identifier) et un hash du contenu (ces deux éléments font parties des données signées).

Le fait que le contenu soit une partie signée ne signifie pas que la Politique de signature et la Politique de document signé soient valables dans ce contexte. D'autres moyens de vérification indépendants de chaque document signé s'imposent pour cet objet, non traités dans la présente spécification.

## 1.7 - Terminologie

La présente spécification distingue les « exigences » d'implémentation qui portent sur la création (CRE) de celles qui portent sur la vérification (VER) de la signature.

Ces définitions ont pour objectifs de permettre :

- que chaque document signé respectant les exigences notées CRE puisse être vérifié par un outil conforme aux exigences notées VER,
- que le maximum de documents créés par d'autres acteurs que ceux concernés par ce document (par exemple par une administration étrangère) soit vérifiable si l'on respecte les exigences VER,
- que le maximum de documents créés selon les exigences CRE puisse être relativement facilement vérifié par d'autres acteurs ou partenaires de l'administration.

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	11/18

Le niveau de recommandation est indiqué par des catégories en suivant la terminologie du [RFC2119] qui définit les mots anglais MUST, SHALL, SHOULD, RECOMMENDED, MAY, OPTIONAL et les inverses MUST NOT, SHALL NOT, SHOULD NOT. La spécification [XAdES 1.3.2] utilise le terme MAY NOT qui doit être interprété comme MUST NOT.

Les termes utilisés dans cette spécification correspondent aux définitions du RGI qui n'utilise un sous-ensemble de ces définitions.

Termes utilisés	Equivalences avec des termes du RFC 2119 et XML-DSIG
OBLIGATOIRE	SHALL, MUST, REQUIRED.
RECOMMANDE	SHOULD, RECOMMENDED
DECONSEILLE	SHOULD NOT, NOT RECOMMENDED
INTERDIT	MUST NOT, SHALL NOT

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	12/18

## 2 - Détails techniques du format

---

### 2.1 - Éléments XML

Il existe actuellement deux versions [XML-1.0] et [XML-1.1].

- **CRE:**
  - Il est **OBLIGATOIRE** de permettre la création de documents en version 1.1.
  - Il est **RECOMMANDE** d'indiquer la valeur 1.0, si le contenu du document ne nécessite pas la version 1.1.
- **VER:** Il est **OBLIGATOIRE** de pouvoir traiter les documents (vérifier les signatures) en version 1.0 et 1.1.

### 2.2 - Éléments XML-DSIG

Ce chapitre se limite à décrire les différences entre [XML-DSIG] et la présente spécification.

**Les éléments XML-DSIG non mentionnés dans ce document sont repris tels quels.**

Les éléments XML-DSIG ne sont pas préfixés dans ce sous-chapitre, les éléments de XAdES sont préfixés par "xad:"

#### 2.2.1 - Signature

Afin de valider une signature [XML-DSIG], il est nécessaire de disposer :

- d'informations concernant la clef publique et/ou l'identité de l'entité qui a signé, et
- d'une chaîne de confiance.

L'élément KeyInfo sert à fournir au vérificateur des informations nécessaires pour permettre la vérification de la signature.

Cette information peut être fournie par l'outil de signature soit en entrée, soit en sortie ou par un autre outil ayant connaissance d'informations partagées (voir aussi l'extension xad:SigningCertificate de XAdES).

- **CRE:** Il est **OBLIGATOIRE** de renseigner au moins une occurrence de l'élément KeyInfo (pour un document devant être échangé),
- **VER:** Il est **OBLIGATOIRE** de disposer d'un élément KeyInfo pour vérifier la signature.

L'attribut ID permet de référencer une signature dans une structure XML.

- **CRE:** Il est **OBLIGATOIRE** de renseigner l'attribut ID,
- **VER:** Il est **OBLIGATOIRE** de s'appuyer sur l'existence d'un attribut ID.

#### 2.2.2 - CanonicalizationMethod

Pour éviter les problèmes avec les multiples signatures imbriquées, le W3C a défini plusieurs algorithmes, dont l'algorithme de forme canonique exclusive (`xml-exc-c14n`) est le plus récent. L'algorithme est identifié par l'URI <http://www.w3.org/2001/10/xml-exc-c14n#>.

Nota : cet algorithme évite des problèmes avec l'algorithme `xml-c14n` (identifié par l'URI <http://www.w3.org/2001/10/xml-c14n#>) dans le cas de plusieurs signatures imbriquées.

Il y a deux algorithmes correspondants qui incluent des commentaires XML. <http://www.w3.org/2001/10/xml-exc-c14n#WithComments> et <http://www.w3.org/2001/10/xml-c14n#WithComments>.

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	13/18

- **CRE:**
  - Il est **OBLIGATOIRE** de supporter les algorithmes `xml-exc-c14n`.
  - Il est **RECOMMANDE** de supporter les algorithmes `xml-c14n` pour assurer la compatibilité avec des implémentations existantes en cas de simple signature.
- **VER:**
  - Il est **OBLIGATOIRE** de traiter l'algorithme `xml-exc-c14n`
  - Il est **RECOMMANDE** de supporter l'algorithme `xml-c14n` pour assurer la compatibilité avec des implémentations existantes en cas de simple signature.

### 2.2.3 - SignatureMethod

Le choix des mécanismes de signature n'est pas imposé par cette spécification, étant traité dans d'autres documents (voir références documentaires informatives sur les algorithmes [ETSI-ALG] et [DCSSI-MC]).

### 2.2.4 - Reference URI

XML-DSIG ne limite pas le choix de type d'URI pour des références externes.

- **CRE:**
  - Il est **OBLIGATOIRE** de supporter des types HTTP ou HTTPS.
  - Il est **RECOMMANDE** de supporter le type LDAP et FTP pour référencer des certificats.
- **VER:**
  - Il est **OBLIGATOIRE** de supporter des URI du type HTTP, HTTPS, LDAP et FTP.
  - Il est **RECOMMANDE** de supporter la résolution d'URI par l'outil de vérification ou d'imposer la fourniture des documents en entrée.

### 2.2.5 - DigestMethod

Pour les choix des mécanismes de condensation, il faut se référer aux documents relatifs aux algorithmes définis dans le référentiel documentaire.

### 2.2.6 - KeyInfo

Ce champ permet d'introduire des informations permettant de déterminer la nature de la clef utilisée et d'identifier l'entité qui a produit la signature. Seuls les certificats au format X.509 conformes aux spécifications [PRIS-V2.1 ou supérieures] doivent être utilisés.

La règle suivante a comme but de simplifier les implémentations et de permettre une vérification de signature directement par la couche XML-DSIG.

- **CRE:**
  - Il est **OBLIGATOIRE** de renseigner cet élément, même en présence d'un élément `xa:SigningCertificate` de XAdES.
  - Il est **DECONSEILLE** d'inclure l'élément dans la partie signée.

Les règles suivantes limitent le choix des valeurs à `X509Data`:

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	14/18

- **CRE:**
  - Il est **OBLIGATOIRE** d'utiliser le choix X509Data ou le choix RetrievalMethod avec un type X509Data.
  - Il est **RECOMMANDE** de remplacer le choix RetrievalMethod pour les documents échangés par X509Data en cas d'une URI non locale.
  
- **VER:**
  - Il est **OBLIGATOIRE** de supporter la vérification d'une signature à base de certificats X.509.
  - Il est **RECOMMANDE** de supporter la récupération de certificat par RetrievalMethod.

## 2.3 - Éléments XAdES

Dans ce chapitre nous précisons le sous-ensemble de XAdES qui a été retenu pour cette spécification, avec pour base [XAdES 1.3.2.]

Cette spécification décrit un sous ensemble de XAdES-EPES avec, en résumé, les propriétés suivantes.

Les éléments suivants doivent obligatoirement apparaître dans les propriétés signées (*signedProperties*) :

- certificat de signature,
- identifiant de la politique de signature.

Les éléments suivants restent facultatifs:

- date de signature,
- heure de signature,
- lieu de la signature,
- rôle du signataire,
- type d'engagement.

Dans ce sous-chapitre les éléments de XML-DSIG sont préfixés par "ds : "

### 2.3.1 - Éléments du schéma XAdES

#### 2.3.1.1. Version de la signature XAdES

La sémantique de tous les éléments de XAdES utilisés dans cette spécification est indépendante de la version de XAdES. En conséquence aucun traitement particulier ne sera demandé pour l'indication de la version XAdES dans les signatures.

#### 2.3.1.2. Qualifying Properties

Cet élément est contenu dans un élément `ds:Object` et sert à contenir plusieurs autres éléments des formats XAdES.

Il y a deux types de sous-éléments : les *SignedProperties*, dont le contenu est inclus dans la signature (par liaison cryptographique avec une fonction de hachage) et les *UnsignedProperties* qui ne sont pas incluses dans la signature. Parmi ces dernières se trouvent les contre-signatures (type *CounterSignature*).

- **CRE:**
  - Il est **OBLIGATOIRE** de supporter la création d'un élément *SignedProperties*.
  - Il est **OBLIGATOIRE** que l'attribut `Target` corresponde à la valeur de l'attribut `ID` d'un élément `ds:Signature`.
  
- **VER:** Il est **OBLIGATOIRE** de supporter les éléments *SignedProperties*.

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	15/18

### 2.3.1.3. SignedProperties

L'élément `SignedProperties` est référencé par un élément `ds:Reference` pour l'inclusion dans la signature [XML-DSIG]. Il contient des éléments faisant partie de la structure signée.

- **CRE:** Il est **OBLIGATOIRE** d'inclure au moins un élément `SignedSignatureProperties`.
- **VER:** Il est **OBLIGATOIRE** de supporter le traitement de `SignedProperties`.

### 2.3.1.4. SignedSignatureProperties

La présence de cet élément dépend de la façon de référencer le certificat de signature et de l'utilisation d'éléments facultatifs, qui sont décrits plus loin en 2.3.2.1 (`SigningCertificate`).

### 2.3.1.5. CounterSignature

Cet élément permet de "contre signer" une signature.

- **VER:** Il est **RECOMMANDE** de supporter le traitement de `CounterSignature` des `UnsignedProperties`.

## 2.3.2 - Format XAdES-BES

Pour le format XAdES-BES, la norme demande le support d'inclusion du certificat du signataire dans la signature soit par l'inclusion d'un élément `ds:KeyInfo`, soit par l'utilisation d'un élément `SigningCertificate` dans les `SignedSignatureProperties`.

Les deux cas nécessitent un traitement spécifique au delà du traitement de base XML-DSIG. Il s'agit de vérifier que l'information sur le certificat dans `ds:KeyInfo` est incluse dans la signature, soit directement par `ds:KeyInfo` soit par l'élément `SigningCertificate`.

### 2.3.2.1. SigningCertificate

- **CRE:**
  - Il est **RECOMMANDE** d'inclure un élément `SigningCertificate`.
  - Dans ce cas (inclusion de l'élément `SigningCertificate`), il est **OBLIGATOIRE** que l'élément contienne la référence et le digest du certificat.
- **VER:** Il est **OBLIGATOIRE** d'implémenter le support de l'élément pour toutes les possibilités de création décrites dans ce document.

*Précision : bien que [XAdES 1.3.2] ne précise pas la manière dont le format d'entrée de la fonction de hachage doit être calculé, toutes les implémentations utilisent un codage en DER du certificat.*

### 2.3.2.2. SigningTime

Cet élément permet au signataire d'inclure la date présumée de création de la signature.

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	16/18

Afin d'assurer la compatibilité avec la Politique d'Horodatage de la [PRIS V2.1], la date doit être mentionnée en utilisant l'échelle de temps UTC (Universal Time Coordinated).

- **CRE:** Il est **OBLIGATOIRE** de permettre l'inclusion d'un élément de type `SigningTime`
- **VER:** Il est **OBLIGATOIRE** de supporter l'élément `SigningTime`.

### 2.3.2.3. ClaimedRoles

Cet élément est une des options des `SignerRole` permettant au signataire d'inclure son rôle présumé avec un type XML ouvert (incluant du texte).

- **CRE:** Il est **OBLIGATOIRE** de permettre l'inclusion de cet élément en format texte.
- **VER:** Il est **OBLIGATOIRE** de supporter cet élément.

### 2.3.2.4. SignatureProductionPlace

Cet élément permet d'indiquer le lieu présumé de la signature.

- **CRE:** Il est **OBLIGATOIRE** de permettre l'inclusion de cet élément en format texte.
- **VER:** Il est **OBLIGATOIRE** de supporter cet élément.

*Précision : des restrictions des valeurs de `SignatureProductionPlace` pourront être décrites dans des documents d'application de ce format.*

### 2.3.2.5. CommitmentTypeIndication

XAdES définit quelques types d'engagements.

- **CRE:** Il est **RECOMMANDE** de permettre l'inclusion de cet élément.
- **VER:** Il est **OBLIGATOIRE** de supporter cet élément.

## 2.3.3 - Format XAdES-EPES

Le format XAdES-EPES oblige à référencer les politiques de signatures. Une politique de signature est référencée par une URI ou un "object identifier" encodé en URN.

En plus de cette référence, il permet d'indiquer les éléments supplémentaires (requis par la norme XAdES) concernant le condensé de la politique de signature et la référence de l'algorithme de hachage utilisé pour calculer ce condensé.

La valeur de l'élément `Identifieur` (du nœud `SigPolicyId`) contient l'URI de la politique de signature.

La valeur de l'élément `Description` contient la description de la politique de signature.

L'algorithme de hachage de la politique de signature est indiqué comme attribut de l'élément `ds:DigestMethod` (du nœud `SigPolicyHash`)

La valeur du hash (encodé en base 64) de la politique est insérée dans de l'élément `ds:DigestValue` (dans l'élément `SigPolicyHash`).

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	17/18

### 2.3.3.1. SignaturePolicyIdentfier

- **CRE:**
  - Il est **OBLIGATOIRE** d'inclure un élément `SignaturePolicyIdentfier` parmi les `SignedSignaturePolicies`.
  - Il est **OBLIGATOIRE** de fournir les éléments de politique
    - soit par la fourniture d'une URI/URN contenant le document de politique (ainsi l'URI/URN et son hash seront inclus dans la signature),
    - soit par la fourniture du document lui-même.
- **VER:**
  - Il est **RECOMMANDE** de supporter l'élément `SignaturePolicyIdentfier` de manière automatique ou semi-automatique.
  - Il est **OBLIGATOIRE** de donner l'accès au contenu de la politique en cas de vérification non automatique par l'utilisateur.

### 2.3.3.2. DataObjectFormat

- **CRE:**
  - Il est **OBLIGATOIRE** d'inclure au moins un des 3 sous éléments suivant : `ObjectIdentifier`, `MimeType` ou `Description`.
  - Il est **RECOMMANDE** de renseigner l'élément `MimeType`.
- **VER:**
  - Il est **OBLIGATOIRE** de supporter cet élément.

Format de signature XAdES de l'administration électronique				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.1.1.1.1.1	1.0	17/12/2007	PUBLIC	18/18