

# Politique de Validation de certificats achatpublic.com

Version 1.0

<b>1</b>	<b><i>Préambule</i></b>	<b>2</b>
1.1	Glossaire et bibliographie	2
1.2	Objet du présent document	2
1.3	Les services d'achatpublic.com	2
1.4	Les marchés publics et la signature électronique	2
<b>2</b>	<b><i>Les signatures électroniques</i></b>	<b>2</b>
2.1	Format des signatures électroniques	2
2.2	La co-signature	3
2.3	Nécessité de vérification a posteriori	3
<b>3</b>	<b><i>Les certificats objets du service de validation</i></b>	<b>3</b>
3.1	Le référencement des Certificats	3
3.2	Cas des Certificats non référencés	3
<b>4</b>	<b><i>Méthode de validation de certificats</i></b>	<b>4</b>
4.1	Le module de récupération des LCR	4
4.2	Le serveur de compléments de signature	4
4.3	Clefs et certificats de validation de certificat	5
4.3.1	Certificat racine d'achatpublic.com	5
4.3.2	Certificat d'horodatage de signature électronique	5
4.3.3	Certificat de signature de preuve de validité	6
4.4	Exploitation de l'information	6
<b>5</b>	<b><i>Engagements d'achatpublic.com</i></b>	<b>7</b>
5.1	Validité des certificats	7
5.2	Autres engagements relatifs aux certificats	8
5.3	Disponibilité du service de validation de certificat	9
5.4	Gestion des clefs privées	9

# 1 Préambule

## 1.1 Glossaire et bibliographie

Un glossaire et une bibliographie recensant les termes employés dans le présent document ainsi que les ouvrages de référence cités seront trouvés dans le document *Achatpublic.com-Politiques de Sécurité-Annexes.pdf*.

## 1.2 Objet du présent document

Le présent document constitue la Politique de validation de certificats d'achatpublic.com.

Il expose le contexte dans lequel achatpublic.com est amenée à se positionner comme Autorité de Validation de certificats, puis explicite le format de preuves de validité de certificats émises, le mode de fabrication de ces preuves, la sémantique de ces preuves et les engagements pris par achatpublic.com sur la validité de ces preuves.

## 1.3 Les services d'achatpublic.com

La société achatpublic.com commercialise un service de dématérialisation des procédures de passation des marchés publics. A ce titre, elle met à disposition de ses clients et usagers une plate-forme accessible sur Internet via l'adresse <http://www.achatpublic.com>, comprenant :

- une Salle des Marchés, dans laquelle se réalisent les échanges sécurisés de données dans le cadre des procédures de passation de marchés publics décrites par le Code des marchés publics ;
- une Salle d'Enchères électroniques inversées, dans laquelle se déroule la mise en concurrence simultanée de plusieurs candidats à un marché public.

## 1.4 Les marchés publics et la signature électronique

Les notions d'engagement d'une part, et d'intégrité des documents d'autre part, étant indissociables du Code des Marchés Publics, achatpublic.com a développé et intégré dans ses services des outils permettant à ses clients et usagers de réaliser et vérifier des signatures électroniques au sens des articles 1316 à 1316-4 du Code Civil [Code civil].

Certains documents devront être signés par plusieurs signataires, par exemple l'acte d'engagement signé par la personne habilitée à engager l'entreprise soumissionnaire, et la personne responsable du marché.

Les signatures électroniques réalisées dans les procédures de passation des marchés publics seront potentiellement vérifiées longtemps après avoir été réalisées, par exemple dans le cadre du contrôle de légalité ou en cas de contentieux. Il importe donc de faire en sorte d'assurer la faisabilité de cette vérification a posteriori.

Les outils de réalisation et de vérification de signature électronique sont disponibles à toutes les étapes de la procédure de dématérialisation où une signature électronique peut être nécessaire : constitution du Dossier de Consultation des Entreprises, constitution de la candidature et de l'offre, tenue de la Commission d'Appel d'Offres, etc. En outre, deux outils sont fournis indépendamment de la procédure, afin de permettre la réalisation et la vérification de signatures électroniques en temps différé par rapport à la procédure.

# 2 Les signatures électroniques

## 2.1 Format des signatures électroniques

Les signatures électroniques réalisées par les outils de signature électronique fournis par achatpublic.com sur sa plate-forme sont au format suivant :

- La signature d'un document se matérialise sous la forme d'un fichier informatique créé au même emplacement que le fichier signé. Si le fichier signé s'appelle « nom.ext », le fichier de signature s'appellera « nom.ext.sig ».
- La signature est au format CMS en mode détaché, conformément à [RFC 2630].

- L'algorithme de signature employé est RSA avec condensation SHA1.
- Le fichier de signature est encodé en Base 64.

## ***2.2 La co-signature***

La possibilité est offerte de réaliser des co-signatures, c'est-à-dire que plusieurs personnes peuvent signer un même document.

Dans le cas des co-signatures, le même fichier contiendra séquentiellement les signatures de tous les signataires.

## ***2.3 Nécessité de vérification a posteriori***

Afin de permettre la vérification a posteriori d'une signature électronique, il est nécessaire de pouvoir vérifier qu'à la date de la signature, le certificat du signataire était bien un certificat valide émis par une Autorité de Certification digne de confiance.

Pour cela, les signatures électroniques réalisées par les outils d'achatpublic.com peuvent comporter deux éléments fournis par la plate-forme achatpublic.com :

- une preuve de validité du certificat, dont le format est décrit plus bas dans le présent document ;
- un jeton d'horodatage au format TSP conformément à la [RFC 3161], dont le format est décrit dans la Politique d'Horodatage d'achatpublic.com - voir ce document.

Lorsqu'il est présent, le jeton d'horodatage indique une date et une heure auxquelles achatpublic.com atteste que le document existait, conformément à la Politique d'Horodatage d'achatpublic.com - voir ce document.

Lorsqu'elle est présente, la preuve de validité du certificat atteste qu'aux date et heure indiquées dans le jeton d'horodatage, le certificat du signataire était valide au sens décrit dans le présent document. achatpublic.com, par l'émission de ces preuves de validité de certificats, se positionne en tant qu'Autorité de Validation. Le présent document décrit les méthodes et les engagements que prend achatpublic.com dans l'exercice de cette fonction.

# **3 Les certificats objets du service de validation**

## ***3.1 Le référencement des Certificats***

achatpublic.com procède, sur la base du référencement réalisé par le MINEFI dans le cadre de TéléTVA, à un référencement des Certificats en lesquels on peut raisonnablement avoir confiance au vu de leur niveau de sécurité et des engagements des Autorités de Certification qui les émettent.

L'activité d'Autorité de Validation d'achatpublic.com s'exerce uniquement sur les certificats référencés par achatpublic.com. achatpublic.com n'effectuera aucune vérification de validité sur des certificats qui ne seraient pas référencés par elle-même.

La liste des Certificats référencés par achatpublic.com est disponible sur le site <http://www.achatpublic.com>.

## ***3.2 Cas des Certificats non référencés***

Les clients ou usagers de la plate-forme de services d'achatpublic.com qui disposeraient d'un certificat non référencé auprès d'achatpublic.com ne sont pas bloqués dans l'usage des outils de signature électronique de ladite plate-forme. Ils pourront ainsi réaliser des signatures électroniques au même format que les porteurs de certificats référencés.

Toutefois, achatpublic.com ne s'engagera en aucune façon sur la validité ou la non-validité du certificat du signataire, et donc sur la validité technique de sa signature. La charge de la vérification de la validité du certificat incombera donc entièrement au destinataire de la signature électronique.

## 4 Méthode de validation de certificats

### 4.1 Le module de récupération des LCR

La vérification de la validité d'un certificat se fonde sur l'analyse de la Liste de Certificats Révoqués émises par l'Autorité de Certification qui a émis le certificat, comme décrit dans [RFC 3280].

Un service automatique de la plate-forme achatpublic.com dispose, pour chaque Certificat référencé par achatpublic.com, d'une URL à laquelle l'Autorité de Certification qui les émet s'engage à mettre à disposition sa Liste de Certificats Révoqués.

Périodiquement, toutes les 24 heures, ce service se connecte à cette URL et en télécharge la dernière Liste de Certificats Révoqués. Le service vérifie alors la signature de la Liste de Certificats Révoqués émise par l'Autorité de Certification en question ainsi que ses dates de validité.

En cas d'indisponibilité d'une Liste de Certificats Révoqués, le service effectue de nouvelles tentatives de téléchargement à intervalles d'une heure.

En cas d'indisponibilité prolongée pendant plus de 24 heures, un plan de secours est activé afin qu'achatpublic.com soit en mesure de disposer de la Liste de Certificats Révoqués par un autre moyen.

### 4.2 Le serveur de compléments de signature

A chaque fois qu'un utilisateur de la plate-forme achatpublic.com réalise une signature électronique, l'outil de signature électronique se connecte automatiquement à la plate-forme pour demander les deux compléments à inclure dans la signature électronique afin d'assurer qu'elle soit vérifiable a posteriori : le jeton d'horodatage et la preuve de validité du certificat.

Les éléments fournis à ce service de compléments de signature sont les suivants :

- le condensat SHA1 du document signé ;
- le nom de l'Autorité de Certification ayant émis le certificat du signataire ;
- le numéro de série du certificat du signataire ;
- les dates de validité du certificat du signataire.

Toutes les informations relatives au certificat sont lues par l'outil de signature directement dans le certificat. Aucune autre information que celles décrites ci-dessus n'est transmise à achatpublic.com, en particulier ni l'identité du porteur du certificat, ni le contenu du document signé.

En retour, le signataire obtient :

- une preuve de validité du certificat, sous la forme d'un « Basic OCSP Response » généré conformément au protocole OCSP conformément à [RFC 2560] ;
- un jeton d'horodatage au format TSP conformément à [RFC 3161], dont le format est décrit dans la Politique d'Horodatage d'achatpublic.com - voir ce document.

Le jeton d'horodatage est inscrit dans la signature électronique sous l'« attrType » : « id-smime-aa-timeStampToken », OID : 1.2.840.113549.1.9.16.2.14.

La preuve de validité de certificat est inscrite dans la signature électronique sous l'« attrType » : « Basic OCSP Response », OID : 1.3.6.1.5.5.7.48.1.1.

La sémantique de la preuve de validité du certificat doit être analysée comme suit. La réponse peut prendre trois valeurs :

- « **good** » : l'Autorité de Certification émettrice du certificat est référencée par achatpublic.com, le certificat référencé n'est pas révoqué, la date courante se trouve entre ses dates de début et de fin de validité ;

- « **revoked** » : l'Autorité de Certification émettrice du certificat est référencée par achatpublic.com, le certificat référencé est révoqué ;
- « **unknown** » : ce statut recouvre tous les autres cas. Il est explicité par le champ « **unknownInfo** » qui peut prendre les valeurs suivantes :
  - **0** : certificat non encore valide ;
  - **1** : certificat expiré ;
  - **2** : l'Autorité de Certification émettrice du certificat n'est pas référencée par achatpublic.com ;
  - **3** : l'Autorité de Certification émettrice du certificat est référencée par achatpublic.com mais la liste de certificats révoqués de l'Autorité de Certification émettrice du certificat n'est pas disponible.

### 4.3 Clefs et certificats de validation de certificat

Deux clefs et certificats de signature sont exploités sur la plate-forme achatpublic.com pour le service de validation de certificat : l'une pour les jetons d'horodatage servant de compléments de signatures électroniques, l'autre pour les preuves de validité.

#### 4.3.1 Certificat racine d'achatpublic.com

Les certificats d'horodatage et de validation de certificat d'achatpublic.com sont émis par le certificat racine d'achatpublic.com.

Ce certificat racine est décrit par les éléments suivants :

**Numéro de série :** 0

**Emetteur :**

- CN = ACHATPUBLIC.COM
- O = ACHATPUBLIC.COM
- C = FR

**Validité :** du jeudi 3 juin 2004 17:51:58 au jeudi 24 mai 2007 17:51:58

**Objet :**

- CN = ACHATPUBLIC.COM
- O = ACHATPUBLIC.COM
- C = FR

**Clef publique RSA 2048 bits :**

```
30 82 01 0a 02 82 01 01 00 98 5d 31 ae bc 83 07 ee 29 c3 e7 e3 48 6f 2b 26 60 47 f2 7e
d0 1d 21 6b 5d 58 e9 67 ae fe ec c9 8f 0b d9 23 0e a3 34 90 5d ae 74 f6 26 a9 d5 bc 5d
d3 a5 e7 dc d3 ec a2 2c 61 6d 0d f4 fa 54 16 94 86 de a1 ed d5 60 5e 89 13 f8 05 ca 6d
78 e0 31 5a 2a 8f 82 cb 33 c0 43 bd 8d 3d c5 6f 74 b9 9a e7 ac 3a e0 a4 64 16 ad 94 8f
c4 b4 a7 aa 0b 00 23 53 a3 0c 70 d9 ce 77 01 a4 f9 8c 22 86 19 38 80 5d 40 d7 c8 a1 63
9c 85 4d 56 55 8d 4b 17 05 fd cb d7 92 fc 3f 07 6b 47 d7 bd cf 63 10 ad ea 6e a3 f5 35
55 15 83 70 32 2f 36 7c e7 d1 ab 25 f7 11 cc d3 35 b7 44 34 96 e5 2a 4a 90 7e fd 92 2c
8b 6f 96 81 61 5f ae a9 bb 92 fc 77 eb 1d d2 fa 08 b4 39 7c 27 f3 36 47 fa 85 56 36 92
3e 19 93 44 28 1c e6 47 8b a0 cc 60 66 69 82 d2 0c 5e 8d 8d cb 7b 17 00 fa fa e3 d3 3f
e9 3f 3e 71 02 03 01 00 01
```

**Identificateur de la clef du sujet :**

```
ac 44 ed 42 9c 63 77 1f 0f a9 ba c0 f2 2a 60 4b db 14 55 81
```

**Algorithme d'empreinte numérique :** SHA1

**Empreinte numérique :**

```
12 9b 9f 71 67 31 93 ac 8c f0 29 96 c9 a6 21 63 42 f6 19 f9
```

#### 4.3.2 Certificat d'horodatage de signature électronique

A compter du 8 décembre 2004, les jetons d'horodatage de signature électronique sont signés par le certificat décrit ci-dessous. Ce certificat est lui-même émis par le certificat racine d'achatpublic.com.

**Numéro de série :** 56

**Emetteur :**

- CN = ACHATPUBLIC.COM

- O = ACHATPUBLIC.COM
- C = FR

**Validité :** du vendredi 26 novembre 2004 10:22:40 au lundi 26 novembre 2007 10:22:40

**Objet :**

- CN = HORODATAGE DE SIGNATURE
- O = ACHATPUBLIC.COM
- C = FR

**Clef publique RSA 2048 bits :**

```
30 82 01 0a 02 82 01 01 00 d3 35 9e 06 c0 db 94 3b ed 60 cf b9 ec 51 43 ee 47 e6 db 73
ad d3 b2 0d 72 96 26 ab bc df 8f 2f 3d 5f fa da b4 bd 05 ac a7 48 b2 41 90 b7 ad ec fb
fe 77 3c c7 97 f4 7f ae 86 5e 4a 87 23 6e 60 18 e1 65 80 c7 5e 4e de 62 b1 31 85 da ad
35 05 ca db a2 76 5b d1 cf 8d ae e6 00 47 40 24 a2 e4 a3 c3 70 12 d1 1f a1 b9 70 3d 50
91 c1 ab ba fa c2 24 dc 9c 23 e8 a4 db 7a 71 1b 19 e8 06 a2 8f f0 29 ef 87 e2 f6 b5 db
18 1d fa 96 d6 c0 2a 35 25 0c 60 7e 69 c9 6e 54 67 48 2f 3a bb 13 c7 18 df ea d0 4d 87
cd 61 24 68 16 df de f1 c3 ca bd bb b2 eb 90 90 6f a3 07 f3 e8 ac 04 55 95 f6 37 ad 27
f1 a1 57 61 a2 0e 35 bb 95 86 f2 bc 02 b2 50 37 3e 48 83 6d 17 40 c4 8b 5e 91 0c fa 11
08 78 85 29 95 1f 0b 24 5f 86 68 6d e4 dc 2d ac ea 1a 1e 66 2f 05 c6 9e 43 1a 9a 51 07
66 39 56 57 02 03 01 00 01
```

**Identificateur de la clef du sujet :**

```
12 cf 27 58 cb 42 09 51 10 eb 5e 83 16 fd a4 6b 3c a8 ed 49
```

**Algorithme d'empreinte numérique : SHA1**

**Empreinte numérique :**

```
b1 ff fa fc 9a e1 e7 57 ec 2c 7d 01 d8 f7 f8 83 71 69 f7 76
```

### 4.3.3 Certificat de signature de preuve de validité

A compter du 8 décembre 2004, les preuves de validité de certificats sont signées par le certificat décrit ci-dessous. Ce certificat est lui-même émis par le certificat racine d'achatpublic.com.

**Numéro de série :** 57

**Emetteur :**

- CN = ACHATPUBLIC.COM
- O = ACHATPUBLIC.COM
- C = FR

**Validité :** du vendredi 26 novembre 2004 12:08:19 au lundi 26 novembre 2007 12:08:19

**Objet :**

- CN = VALIDATION DE CERTIFICAT
- O = ACHATPUBLIC.COM
- C = FR

**Clef publique RSA 2048 bits :**

```
30 82 01 0a 02 82 01 01 00 c5 24 d0 7d 34 29 1d 23 df c4 2e 83 ad 41 b9 c5 25 75 ad 39
87 23 1a 2e 35 03 24 59 2e 89 37 e8 d7 2c 27 01 95 07 64 b3 e4 f0 72 df 31 86 15 95 9e
44 a1 81 fe 96 0f 36 83 39 fc c5 af 9d b9 1a 4c 92 a4 ff 0e 5b d5 25 a9 b0 63 c8 dd 75
75 91 6d 30 51 97 0c 73 cd 6c 23 91 e6 97 53 85 64 f5 77 3b c3 05 e8 d5 7b c1 e9 98 e3
18 f5 52 aa fe 1b 93 cb 11 54 e3 f5 26 c2 ec 27 01 6c e1 00 af 4a ce 79 5a 4d bf 69 f8
8e 7e 79 9a f2 4c db a7 34 00 8e e3 39 42 b2 0f ed 89 95 3b 72 af 37 ff 0a 1d 4a 8a
1f 48 03 1d 90 22 94 3b 9e b9 ea d7 70 7d 3f 37 90 8b 44 65 18 a4 d8 3b 5e 45 bf 9f da
48 29 93 2d 25 cb 70 03 f4 01 0f 45 46 54 f5 ae bc f7 63 4f a1 b9 55 85 98 21 f7 96 f3
6d 6f 20 7a a0 4f 33 4a 8c cb 0b 04 e4 8b 17 6d 26 47 bd 5c 69 5b 86 df 48 f5 d9 2b 7a
e1 97 c6 57 02 03 01 00 01
```

**Identificateur de la clef du sujet :**

```
18 f6 7c 38 51 a9 93 c9 b0 f3 9b e6 ad 2f fa 88 e0 0c 04 6b
```

**Algorithme d'empreinte numérique : SHA1**

**Empreinte numérique :**

```
fd 2f da b6 a0 62 bf ae 81 42 a0 8e a8 ef d3 8a 2f e3 9f d0
```

## 4.4 Exploitation de l'information

Lors de la vérification technique des signatures électroniques à l'aide des outils fournis par achatpublic.com, la signature est vérifiée techniquement, puis les éléments suivants sont vérifiés :

- conformité du jeton d'horodatage avec le document signé ;
- validité du jeton d'horodatage ;
- validité de la preuve de validité de certificat ;
- statut de la preuve de validité de certificat.

Les éléments suivants sont alors indiqués dans l'interface de visualisation :

- validité au sens technique de la signature ;
- identité du signataire ;
- autorité de certification ayant émis le certificat ;
- date de la signature ;
- en cas de non-validité, raison de la non-validité.

Les fichiers de signature et tous les éléments qu'ils contiennent étant à des formats standard définis par les RFC de l'IETF citées dans le présent document, il est possible de réaliser la vérification technique des signatures électroniques réalisées grâce aux outils d'achatpublic.com avec un autre outil de vérification que celui que fournit achatpublic.com. La sémantique des divers champs devra être interprétée en conformité avec le contenu du présent document et, à défaut de description spécifique, conformément aux RFC de l'IETF.

## 5 Engagements d'achatpublic.com

### 5.1 Validité des certificats

Au sens de la présente politique de validation, la vérification de la signature électronique permet uniquement d'affirmer qu'à la date de la signature, le certificat du signataire était bien un certificat valide émis par une Autorité de Certification digne de confiance. La date de la signature prise en compte est celle indiquée dans le jeton d'horodatage associé à la preuve de validité du certificat.

achatpublic.com ne prend aucun engagement sur la vérification ou la validité de toute autre signature électronique réalisée par tout autre outil.

achatpublic.com ne prend aucun engagement sur les preuves de validité qu'elle n'aurait pas émises. La signature par achatpublic.com des preuves de validité de certificats permet de reconnaître les preuves émises par achatpublic.com et sur la validité desquelles achatpublic.com s'engage exclusivement.

Lorsqu'un certificat a un statut « good », achatpublic.com s'engage à vérifier les éléments suivants :

- l'Autorité de Certification ayant émis le certificat est référencée par achatpublic.com ;
- la chaîne de certification menant du certificat à cette Autorité est entièrement valide techniquement ;
- le certificat est techniquement bien formé et en particulier la signature du certificat est valide ;
- la date courante se trouve entre les dates de début et de fin de validité du certificat ;
- achatpublic.com dispose d'une Liste de Certificats Révoqués en cours de validité émise par l'Autorité de Certification ayant émis le certificat et dans laquelle le certificat n'est pas présent.

Lorsqu'un certificat a un statut « revoked », achatpublic.com s'engage à vérifier les éléments suivants :

- l'Autorité de Certification ayant émis le certificat est référencée par achatpublic.com ;
- la chaîne de certification menant du certificat à cette Autorité est entièrement valide techniquement ;
- le certificat est techniquement bien formé et en particulier la signature du certificat est valide ;
- achatpublic.com dispose d'une Liste de Certificats Révoqués en cours de validité émise par l'Autorité de Certification ayant émis le certificat et dans laquelle le certificat est présent.

Lorsqu'un certificat a un statut « unknown », achatpublic.com s'engage à vérifier les éléments suivants, en fonction de la valeur du champ « unknownInfo » :

- **unknownInfo = 0** :
  - l'Autorité de Certification ayant émis le certificat est référencée par achatpublic.com ;
  - la chaîne de certification menant du certificat à cette Autorité est entièrement valide techniquement ;

- le certificat est techniquement bien formé et en particulier la signature du certificat est valide ;
- achatpublic.com dispose d'une Liste de Certificats Révoqués en cours de validité émise par l'Autorité de Certification ayant émis le certificat et dans laquelle le certificat n'est pas présent ;
- la date courante est antérieure à la date de début de validité du certificat.
- **unknownInfo = 1 :**
  - l'Autorité de Certification ayant émis le certificat est référencée par achatpublic.com ;
  - la chaîne de certification menant du certificat à cette Autorité est entièrement valide techniquement ;
  - le certificat est techniquement bien formé et en particulier la signature du certificat est valide ;
  - achatpublic.com dispose d'une Liste de Certificats Révoqués en cours de validité émise par l'Autorité de Certification ayant émis le certificat et dans laquelle le certificat n'est pas présent ;
  - la date courante est postérieure à la date de fin de validité du certificat.
- **unknownInfo = 2 :**
  - l'Autorité de Certification ayant émis le certificat n'est pas référencée par achatpublic.com.
- **unknownInfo = 3 :**
  - l'Autorité de Certification ayant émis le certificat est référencée par achatpublic.com ;
  - la chaîne de certification menant du certificat à cette Autorité est entièrement valide techniquement ;
  - le certificat est techniquement bien formé et en particulier la signature du certificat est valide ;
  - la date courante se trouve entre les dates de début et de fin de validité du certificat ;
  - achatpublic.com ne dispose pas d'une Liste de Certificats Révoqués en cours de validité émise par l'Autorité de Certification ayant émis le certificat.

## 5.2 *Autres engagements relatifs aux certificats*

achatpublic.com ne vérifie pas que le certificat de signature soit utilisé conformément à la Politique de Certification de l'Autorité de Certification qui l'a émis, en particulier en ce qui concerne une éventuelle limite sur le montant des engagements financiers permis ou sur les usages autorisés.

achatpublic.com n'effectue aucune vérification sur le rôle du signataire au sein de l'organisation à laquelle il appartient : pouvoir d'engager l'entreprise, délégations de pouvoirs, responsabilité en matière de marchés publics...

Tous les éléments de vérification de la signature allant au-delà des seuls engagements d'achatpublic.com mentionnés dans le présent document sont exclusivement à la charge et sous la responsabilité de la personne vérifiant la signature.

En particulier, lorsqu'une signature est réalisée avec un certificat émanant d'une Autorité de Certification qui n'est pas référencée par achatpublic.com, toutes les vérifications relatives à la validité de ce certificat et à la confiance que l'on peut lui accorder sont exclusivement à la charge et sous la responsabilité de la personne vérifiant la signature.

achatpublic.com est responsable de la vérification de la validité des certificats utilisés par ses clients et ses usagers dans le cadre de la dématérialisation de leurs procédures de passation de marchés publics et ce dans les limites des indications fournies par l'Autorité de Certification dans sa liste de révocation, de la disponibilité de celle-ci et de la date de validité indiquée par celle-ci dans les certificats qu'elle émet et signe, et dans la mesure où l'Autorité de Certification est référencée par achatpublic.com. achatpublic.com ne saurait être tenue pour responsable de l'usage du certificat par un client de l'Autorité de Certification excédant les limitations relatives aux plafonds d'engagement mentionnées dans les documents contractuels de l'Autorité de Certification ou encore pour tout autres usages contraires à ceux autorisés par les documents contractuels liant l'Autorité de Certification et ses clients.

L'Autorité de Certification est responsable de la validité des informations qu'elle fournit dans ses certificats et dans sa liste de certificats révoqués et de la disponibilité de celle-ci.

Ainsi, par exemple, achatpublic.com ne saurait être tenue, en aucune façon, pour responsable des erreurs survenues dans la vérification des certificats ayant pour cause une inexactitude ou un manque de diligence de l'Autorité de Certification dans la mise à jour de sa liste de révocation ou dans la délivrance des certificats.

En outre, achatpublic.com n'assume aucun engagement ni responsabilité quant à l'utilisation des signatures électroniques et des preuves de validité qu'elle émet pour le client ou l'utilisateur qui ne serait pas conforme à la réglementation en vigueur relative à la protection des logiciels, quant à l'usure normale des média informatiques du client ou de l'utilisateur, la détérioration des informations portées sur lesdits médias informatiques due à l'influence des champs magnétiques.

achatpublic.com ne sera en aucun cas tenue pour responsable des éventuels dommages indirects, consécutifs ou connexes, ou d'autres réclamations ou obligations quelconques résultant d'un acte délictueux, d'un contrat ou d'une autre cause à l'égard d'un service en relation avec la présente politique de validation. Cette limite de responsabilité s'entend, et de façon non limitative, de tout préjudice financier ou commercial, perte de bénéfices, perte d'exploitation, trouble commercial, manque à gagner, pertes ou actions intentées par un tiers contre le client ou l'utilisateur, trouvant leur origine ou étant la conséquence du présent contrat ou inhérents à l'utilisation ou la fiabilité d'une preuve de validité ou d'une signature qu'achatpublic.com émet.

### ***5.3 Disponibilité du service de validation de certificat***

achatpublic.com s'engage à exploiter le service de validation de certificats selon les pratiques de l'état de l'art relatif à l'exploitation de tels services. En particulier, achatpublic.com fera de son mieux pour réduire au minimum possible les périodes d'indisponibilité du service.

achatpublic.com s'engage à être auditable de manière à pouvoir fournir une mesure objective de la qualité de service rendue dans le service de validation de certificats.

Il est à noter qu'en cas d'indisponibilité du service lors d'une signature électronique, la signature se réalise tout de même, et que les éléments complémentaires - horodatage, preuve de validité de certificat - sont ajoutés à la signature automatiquement lors de sa première vérification. Ainsi, une éventuelle indisponibilité du service n'empêche pas la continuité du déroulement de la procédure de passation du marché.

### ***5.4 Gestion des clefs privées***

achatpublic.com s'engage à exploiter les clefs privées nécessaires au service de validation de certificats selon les pratiques de l'état de l'art relatif à l'exploitation de tels services. En particulier, ces clefs ont été générées hors-ligne et transmises à l'exploitant sous la protection d'un double chiffrement, levé au démarrage de l'application sur le serveur.

achatpublic.com s'engage à être auditable de manière à pouvoir fournir une mesure objective de la qualité de la gestion de ses clefs privées.