

Politique d'Horodatage achatpublic.com

Version 1.0

1	<i>Préambule</i>	2
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 l'horodatage	2
1.5	Cartographie des horodatages réalisés par la plate-forme achatpublic.com	3
2	<i>Format de l'horodatage</i>	6
2.1	Format des jetons d'horodatage	6
2.2	Clefs et certificats d'horodatage	6
2.2.1	Certificat racine d'achatpublic.com	6
2.2.2	Certificat d'horodatage de signature électronique	6
2.2.3	Certificat d'horodatage de preuve	7
2.3	Inclusion de jetons d'horodatage dans les signatures électroniques	8
2.4	Exploitation de l'information d'horodatage dans les signatures électroniques	8
2.5	Format des preuves horodatées	9
2.6	Exploitation des preuves horodatées	9
3	<i>Méthode de génération des jetons d'horodatage</i>	9
3.1	La synchronisation des serveurs	9
3.2	Fonctionnement du serveur d'horodatage	9
3.3	Conservation des preuves et des jetons d'horodatage	10
4	<i>Engagements d'achatpublic.com</i>	10
4.1	Portée de l'engagement	10
4.2	Sémantique de l'horodatage	10
4.3	Précision de l'horodatage	10
4.4	Disponibilité du service d'horodatage	11
4.5	Gestion des clefs privées	11

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.rtf*.

1.2 *Objet du présent document*

Le présent document constitue la Politique d'Horodatage d'achatpublic.com.

Il expose le contexte dans lequel achatpublic.com est amenée à se positionner comme Autorité d'Horodatage, puis explicite les cas dans lesquels des jetons d'horodatage seront délivrés par achatpublic.com, le mode de fabrication de ces jetons d'horodatage et plus largement des preuves dans lesquels ils seront inclus, la sémantique de ces preuves et les engagements pris par achatpublic.com sur la précision et la validité des jetons d'horodatage.

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 l'horodatage*

La notion de « date certaine » étant indissociable du Code des Marchés Publics, achatpublic.com a développé et intégré dans ses services des outils permettant de placer dans le temps, c'est à dire horodater, des événements. En outre, la technique d'horodatage employée permet à achatpublic.com de fournir à ses clients et usagers des éléments fiables pouvant faire office de preuve en cas de contestation.

1.5 Cartographie des horodatages réalisés par la plate-forme achatpublic.com

Étape	Demandeurs	Éléments transmis à achatpublic.com	Usage
	Destinataires		
Signature électronique 	Personne Publique Soumissionnaire <hr/> Personne Publique Soumissionnaire	Hash SHA1 du document à signer	Toute signature électronique visant à être ensuite vérifiée par le signataire lui-même, le destinataire ou un autre organe de contrôle.
Dépôt d'empreinte Extension : .pde	Soumissionnaire <hr/> Personne Publique Soumissionnaire	Document xml comprenant les hash SHA1 des enveloppes chiffrées composant le pli. achatpublic.com horodate ce document xml.	Inclusion dans le registre des dépôts afin de vérifier les hors-délai. Transmission au soumissionnaire comme preuve de son dépôt. Vérification par le soumissionnaire lui-même, la Personne Publique ou un autre organe de contrôle.
Dépôt de pli Extension : .pdp	Soumissionnaire <hr/> Personne Publique Soumissionnaire	Envelopes chiffrées composant le pli. achatpublic.com en effectue le hash par deux algorithmes SHA1 et MD5, inclut ces hash dans un document xml, compare les hash SHA1 réalisés avec ceux transmis dans le dépôt d'empreinte, puis horodate le document xml.	Inclusion dans le registre des dépôts afin de vérifier les hors-délai. Transmission au soumissionnaire comme preuve de son dépôt. Vérification par le soumissionnaire lui-même, la Personne Publique ou un autre organe de contrôle.
Preuve d'ouverture des plis Extension : .pop	Personne Publique <hr/> Personne Publique	Extraction du registre technique des informations relatives aux clefs de déchiffrement téléchargées ou non par la Personne Publique. Composition d'un document xml. Horodatage de ce document xml.	Permettre à la Personne Publique de vérifier ou de prouver à un tiers quelles enveloppes ont été ouvertes et lesquelles ne l'ont pas été.
Envoi d'un avis en publication Extension : .pep	Service de publication <hr/> Personne Publique	Composition par le service de publication d'un fichier xml contenant l'identité de la Personne Publique, le type de publication demandé et le hash des informations de publication. Horodatage de ce document xml par achatpublic.com	Date certaine d'envoi en publication pour le contrôle de légalité.

Etape	Demandeurs Destinataires	Éléments transmis à achatpublic.com	Usage
Accusé de réception de document Extension : .pcr	Soumissionnaire Personne Publique Soumissionnaire	<p>Dans l'espace d'échanges, un mail est envoyé au soumissionnaire indiquant une URL et un mot de passe. Lorsqu'il se connecte à cette URL et indique son mot de passe, il accède au téléchargement du document. La plate-forme achatpublic.com génère alors un fichier xml attestant de cet accès et l'horodate. Ce fichier horodaté est fourni au soumissionnaire et à la Personne Publique pour tenir lieu d'Accusé de Réception.</p> <p>Si après un délai paramétrable le retrait n'a pas eu lieu, la Personne Publique en est informée et réitère son envoi par voie papier en recommandé avec accusé de réception.</p>	<p>Date de réception par le soumissionnaire d'un document envoyé par la Personne Publique à travers le sas d'échange vérifiable par la Personne Publique, le soumissionnaire ou un autre organe de contrôle. Utilisé pour :</p> <ul style="list-style-type: none"> • Les rectificatifs et compléments d'information • Les réponses aux fournisseurs • Les demandes de précision, discussions, mises au point • Les courriers de rejet de candidatures et d'offres • Les demandes de certificats sociaux et fiscaux • L'envoi du marché • Les déclarations de marchés sans suite ou infructueux • L'information des candidats rejetés • La mise à disposition du DCE pour les procédures restreintes
Preuve d'envoi de document par le soumissionnaire Extension : .pdr	Soumissionnaire Personne Publique Soumissionnaire	<p>Dans l'espace d'échange, le soumissionnaire vient déposer un document relatif à une consultation. La plate-forme achatpublic.com génère alors un fichier xml attestant de ce dépôt et l'horodate. Ce fichier horodaté est fourni au soumissionnaire et à la Personne Publique pour tenir lieu d'Accusé de Réception.</p>	<p>Date de dépôt par le soumissionnaire de documents dans l'espace d'échanges de la Salle des Marchés vérifiable par la Personne Publique, le soumissionnaire ou un autre organe de contrôle. Utilisé pour :</p> <ul style="list-style-type: none"> • Les questions des fournisseurs • Les réponses aux demandes de précision, discussions, mises au point • Les envois de certificats sociaux et fiscaux

Etape	Demandeurs Destinataires	Éléments transmis à achatpublic.com	Usage
<p>Preuve d'envoi de document par la Personne Publique</p> <p>Extension : .per</p>	<p>Personne Publique</p> <hr/> <p>Personne Publique</p>	<p>Dans l'espace d'échange, la Personne Publique réalise un envoi à l'attention d'un ou plusieurs soumissionnaires. La plate-forme achatpublic.com génère alors un fichier xml attestant de cet envoi et l'horodate. Ce fichier horodaté est fourni à la Personne Publique pour tenir lieu d'Accusé de Réception.</p>	<p>Date d'envoi par la Personne Publique de documents dans l'espace d'échanges de la Salle des Marchés, vérifiable par la Personne Publique, le soumissionnaire ou un autre organe de contrôle. Utilisé pour :</p> <ul style="list-style-type: none"> • Les rectificatifs et compléments d'information • Les réponses aux fournisseurs • Les demandes de précision, discussions, mises au point • Les courriers de rejet de candidatures et d'offres • Les demandes de certificats sociaux et fiscaux • L'envoi du marché • Les déclarations de marchés sans suite ou infructueux • L'information des candidats rejetés • La mise à disposition du DCE pour les procédures restreintes

2 Format de l'horodatage

2.1 Format des jetons d'horodatage

Les jetons d'horodatage réalisés par achatpublic.com sur sa plate-forme sont au format défini par le protocole TSP, conformément à [RFC 3161].

Le jeton d'horodatage contient le hash SHA1 du document horodaté.

Le jeton d'horodatage est signé par achatpublic.com conformément à la norme, à l'aide d'une clef RSA de 2048 bits.

2.2 Clefs et certificats d'horodatage

Deux clefs et certificats de signature de jetons d'horodatage différents sont exploités sur la plate-forme achatpublic.com : l'une pour les jetons d'horodatage servant de compléments de signatures électroniques, l'autre pour les jetons d'horodatage servant à constituer des preuves horodatées.

2.2.1 Certificat racine d'achatpublic.com

Les certificats d'horodatage 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
```

2.2.2 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
```

2.2.3 Certificat d'horodatage de preuve

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

Numéro de série : 55

Emetteur :

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

Validité : du vendredi 26 novembre 2004 10:21:33 au lundi 26 novembre 2007 10:21:33

Objet :

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

Clef publique RSA 2048 bits :

```
30 82 01 0a 02 82 01 01 00 df 06 f9 ff 56 85 7f 6a ee a9 09 a0 a9 89 18 27 18 91 80 b5
8b 39 bb 14 eb d3 51 b2 a0 ce 32 51 62 cb 11 0c 8c 5c ec 0c db b4 bf e9 79 f6 f7 3b f2
88 ca 83 d8 c0 cc 54 bf 7a e9 f1 2f 14 26 ac 65 bc fe 8b 8f b9 01 2e 21 03 6e 3d 72 b5
b4 b0 01 86 ee 79 c4 ac 76 15 46 31 60 4b 07 6f a3 f9 9e 4e 1b b8 1a e1 86 9c c8 02 04
85 12 40 00 f4 d3 52 e9 59 27 87 b4 c7 0e 4a e0 fc ba c3 8d 50 c2 5e 58 63 87 8c ab c4
be da dc 68 10 70 b2 5d 16 27 3f 36 17 4a 06 1f 7c 12 37 e8 09 93 34 30 8e f7 e1 97 65
20 bd b3 ed 5f 68 5a 3e c3 cd 5c 95 14 36 2a 02 ad eb 7b 45 e0 65 70 08 06 5d 1e af 4b
76 ff ee 52 45 fe 3f 45 b7 10 d5 79 96 0e 64 be 9f c6 5e 5e 01 0d 3d c5 e3 c2 15 2b aa
0e 2d 50 63 73 34 71 60 a8 ad 16 04 61 e0 cf f6 e6 c7 09 67 13 2f f7 fc 78 6e fe 9f cd
4a 2b de 2b 02 03 01 00 01
```

Identificateur de la clef du sujet :

```
fb fd 27 95 4d c1 86 f2 4c 21 de e0 c8 a4 49 f3 9d e8 94 06
```

Algorithme d'empreinte numérique : SHA1

Empreinte numérique :

```
d8 44 61 f0 4f ef 94 0c 38 d9 c4 2a a2 55 8e 59 98 b0 23 ad
```

2.3 Inclusion de jetons d'horodatage dans les signatures électroniques

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 dans la Politique de Validation de certificats d'achatpublic.com - voir ce document ;
- un jeton d'horodatage au format décrit par le présent document.

Lorsqu'il est présent, le jeton d'horodatage indique une date et une heure auxquelles achatpublic.com atteste que le document existait, sur la foi de l'existence du hash SHA1 du document, transmis à la plate-forme achatpublic.com par l'outil de signature électronique.

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 hash 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.

Seul le hash SHA1 du document est utilisé pour générer le jeton d'horodatage.

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.

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.

2.4 Exploitation de l'information d'horodatage dans les signatures électroniques

Lors de la vérification des signatures électronique 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 de la signature ;
- identité du signataire ;
- autorité de certification ayant émis le certificat ;
- date de la signature ;
- en cas d'invalidité, raison de l'invalidité.

Les fichiers de signature et tous les éléments qu'ils contiennent, y compris les jetons d'horodatage, étant à des formats standard définis par les RFC de l'IETF citées dans le présent document, il est possible de réaliser la

vérification 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.

2.5 Format des preuves horodatées

Une preuve fournie par la plate-forme achatpublic.com a systématiquement le format suivant :

- un fichier au format xml « nom.xml » contenant les éléments d'information appelés à faire foi est généré, soit sur le poste de travail du demandeur, soit sur la plate-forme achatpublic.com selon le lieu où ces informations sont disponibles ;
- ce fichier est hashé par l'algorithme SHA1 ;
- le hash SHA1 est envoyé au serveur d'horodatage pour générer le jeton TSP signé par achatpublic.com ;
- le hash SHA1 et le jeton sont stockés dans un fichier au format CMS, conformément à [RFC 2630], encodé en base 64. Ce fichier se nomme « nom.xml.hor » ;
- le fichier « nom.xml » et « nom.xml.hor » sont rassemblés en une archive au format zip ;
- c'est cette archive qui constitue la preuve : elle contient tous les éléments permettant de vérifier l'information qui était disponible pour achatpublic.com à la date indiquée dans le jeton d'horodatage.

2.6 Exploitation des preuves horodatées

L'outil d'affichage et de vérification des preuves fourni par achatpublic.com permet, en fonction de la sémantique de chacune des preuves, d'afficher le contenu pertinent pour l'utilisateur. Les éléments suivants sont systématiquement vérifiés :

- conformité du jeton d'horodatage avec le document horodaté ;
- validité du jeton d'horodatage.

La date et l'heure de constitution de la preuve sont alors systématiquement indiquées dans l'interface de visualisation.

Les fichiers de preuve étant au format xml et les jetons d'horodatage au format TSP standard décrit par le présent document, il est possible de réaliser la vérification des preuves horodatées fournies par achatpublic.com avec un autre outil de vérification que celui que fournit achatpublic.com. La sémantique des divers champs du jeton d'horodatage devra être interprétée en conformité avec le contenu du présent document et, à défaut de description spécifique, conformément aux RFC de l'IETF. La sémantique du contenu des preuves horodatées devra être interprétée conformément à l'usage fait de chacune de ces preuves, décrit plus haut dans le présent document.

3 Méthode de génération des jetons d'horodatage

3.1 La synchronisation des serveurs

achatpublic.com s'engage à ce que les différents serveurs constituant sa plate-forme soient synchronisés et maintenus à l'heure avec une dérive toujours inférieure à une minute par rapport à l'heure juste.

Ce maintien à l'heure est réalisée par le protocole NTP décrit dans [RFC 1305], par synchronisation avec les trois serveurs de temps suivants :

- chronos.cru.fr : Comité Réseau des Universités
- ntp-p1.obspm.fr : Observatoire de paris
- ntp-sop.inria.fr : INRIA

3.2 Fonctionnement du serveur d'horodatage

Chaque service d'horodatage de la plate-forme achatpublic.com dispose d'une clef privée de signature RSA de 2048 bits, et exploite pour réaliser les horodatages l'heure de la machine sur laquelle il s'exécute.

Le serveur d'horodatage reçoit en entrée un hash SHA1.

Il renvoie un jeton d'horodatage TSP signé conformément à [RFC 3161].

Le serveur d'horodatage peut être appelé par les autres services de la plate-forme, dont il est un sous-traitant : le service de compléments de signature électronique, ou un service de génération de preuve.

Ce sont ces services qui réalisent la mise en forme, l'acheminement et le stockage des jetons d'horodatage.

C'est la signature du jeton TSP par la clef privée détenue par le serveur qui fait foi de la validité de l'horodatage, et de l'authenticité de sa provenance.

Les clefs et certificats de signature des jetons d'horodatage ont été différenciés entre les horodatages servant de complément de signature et les horodatages servant de constitution de preuves horodatées, afin qu'un usager de la plate-forme effectuant la signature d'un document à la syntaxe identique à une preuve constituée par la plate-forme ne puisse pas, par ce moyen, forger une preuve lui-même en lieu et place de la plate-forme achatpublic.com.

3.3 Conservation des preuves et des jetons d'horodatage

Les jetons d'horodatage inclus dans les signatures électroniques ne sont jamais conservés par la plate-forme achatpublic.com. Ils sont transmis au signataire pour une inclusion immédiate et automatique dans le fichier de signature électronique, dont ils font partie intégrante.

Les preuves horodatées sont transmises ou mises à la disposition des destinataires, qui ont la charge de leur archivage. Elles sont traitées par achatpublic.com comme toutes les autres pièces de la procédure.

4 Engagements d'achatpublic.com

4.1 Portée de l'engagement

Les engagements d'achatpublic.com ne portent que sur les horodatages réalisés par achatpublic.com sur sa plate-forme, à l'exclusion de tout autre horodatage réalisée par tout autre outil.

Les engagements d'achatpublic.com ne portent que sur les preuves horodatées réalisés par achatpublic.com sur sa plate-forme, à l'exclusion de toute autre preuve réalisée par tout autre outil. La signature par achatpublic.com des jetons d'horodatage permet de reconnaître les jetons d'horodatage et les preuves horodatées émises par achatpublic.com et sur la validité desquelles achatpublic.com s'engage exclusivement.

4.2 Sémantique de l'horodatage

La sémantique de l'horodatage doit s'entendre comme suit : à la date et à l'heure indiquées dans le jeton d'horodatage interprété conformément à [RFC 3161], le document dont le hash est inclus dans le jeton d'horodatage existait.

Lorsqu'il s'agit d'une preuve horodatée, à cette sémantique s'ajoute l'engagement d'achatpublic.com sur la véracité des informations contenues dans le document xml constituant la preuve.

4.3 Précision de l'horodatage

Les jetons d'horodatage fournis par la plate-forme achatpublic.com doivent être interprétés avec une précision n'allant pas au-delà de la minute.

achatpublic.com s'engage sur l'heure incluse dans les jetons d'horodatage qu'elle fournit avec une erreur maximale d'une minute.

Pour la génération des preuves par la plate-forme achatpublic.com, l'heure contenue dans le jeton d'horodatage, et qui fait foi, est l'heure de fin de la constitution de la preuve.

Par exemple, les preuves de dépôt de pli donnent lieu au hash du pli reçu, ce hash faisant partie intégrante du fichier xml à horodater. Or si le pli est volumineux, cette opération de hash peut prendre plusieurs minutes, et la preuve ne sera ainsi constituée que plusieurs minutes après la réception effective du pli. Néanmoins, c'est l'heure du jeton d'horodatage qui fera foi de la bonne réception du pli, et qui est la seule sur laquelle achatpublic.com prend un engagement.

4.4 Disponibilité du service d'horodatage

achatpublic.com s'engage à exploiter le service d'horodatage 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.

4.5 Gestion des clés privées

achatpublic.com s'engage à exploiter les clés privées nécessaires au service d'horodatage selon les pratiques de l'état de l'art relatif à l'exploitation de tels services. En particulier, ces clés 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 clés privées.