Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre	Ministère du budget, des comptes publics et de la réforme de l'État
Agence nationale de la sécurité des systèmes d'information	Direction générale de la modernisation de l'État

Référentiel Général de Sécurité

version 1.0

Annexe A12

Politique d'Horodatage Type

Version 2.3 du 18 février 2010

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
06/11/2006	2.1	*Document constitutif de la Politique de Référencement Intersectorielle de Sécurité – PRISv2.1.*	DCSSI / SDAE
12/12/2008	2.2	*Document constitutif du Référentiel Général de Sécurité – RGSv0.98, annexe A12.* Modification : • L'extension *extendedKeyUsage* est marquée comme critique conformément au RFC 3161.	DCSSI / DGME
18/02/2010	2.3	*Document constitutif du Référentiel Général de Sécurité – RGSv1.0, annexe A12.* Modifications : • Réécriture des chapitres VI.1.2, VI.2.1 et IX.2 ; • Modifications des obligations pour les AC fournissant des certificats d'horodatage ; • Modification de la durée de validité des certificats d'horodatage ; • Modification des exigences sur le gabarit des certificats d'horodatage.	ANSSI / DGME

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

rgs@ssi.gouv.fr

Direction générale de la modernisation de l'État

Service Projets

64-70 allée de Bercy
75012 Paris

rgs.dgme@finances.gouv.fr

SOMMAIRE

I. Introduction

I.1. Présentation générale

Le présent document fait partie des documents constitutifs du [RGS]. Il concerne la fonction de sécurité « horodatage » et constitue la politique d'horodatage type (PH Type) destinée aux prestataires de services d'horodatage électronique (PSHE) souhaitant fournir des contremarques de temps à des usagers, des agents ou des applications. Il a également pour objet de renseigner les usagers, les agents et promoteurs d'applications utilisant de telles contremarques de temps.

Le service d'horodatage est composé d'un seul niveau de sécurité.

Afin de sécuriser les systèmes d'informations sous la responsabilité d'une autorité administrative (AA), celle-ci peut recourir à la fonction de sécurité « horodatage ». Dès lors, l'autorité administrative doit utiliser des jetons d'horodatage délivrés par des PSHE conformes à la présente PH Type.

Un PSHE peut demander la qualification de son offre de service (délivrance de jetons d'horodatage) selon les modalités précisées dans le [DécretRGS][1]. Ce label permet d'attester de la conformité de l'offre du PSHE au présent référentiel.

Les exigences spécifiées dans la présente PH Type doivent être respectées intégralement par les PSHE, moyennant l'exception suivante. Dans la présente PH Type, un certain nombre de recommandations sont formulées. Les PSHE sont incités à les respecter également dès maintenant car ces recommandations, qui ne sont pas d'application obligatoire dans la présente version de ce document, devraient le devenir dans une version ultérieure.

Cette PH Type n'est pas une PH à part entière : elle ne peut pas être utilisée telle quelle par un PSHE en tant que PH pour être mentionnée dans ses contremarques de temps et sa DPH. Un PSHE souhaitant être qualifié par rapport à la présente PH Type doit en reprendre, dans sa propre PH, l'ensemble des engagements.

La présente PH Type a été élaborée sur la base de la politique d'horodatage de l'ETSI [ETSI_PH]. Les différences entre la PH Type et [ETSI_PH] sont présentées au chapitre XIII.

I.2. Identification du document

La présente PH Type est dénommée "RGS - Politique d'Horodatage Type". Elle peut être identifiée par son numéro d'identifiant d'objet (OID - cf. page de garde et pied de page de chaque page). D'autres éléments, plus explicites, (nom, numéro de version, date de mise à jour) permettent également de l'identifier.

Le numéro d'OID de cette PH Type est indiqué à titre de gestion documentaire. Il ne doit pas être utilisé dans les contremarques de temps. L'AH doit attribuer à sa propre PH, reprenant les exigences de la présente PH Type, un OID qui sera porté dans ses contremarques de temps correspondantes.

Le numéro d'OID du présent document est : 1.2.250.1.137.2.2.1.2.2.4

I.3. Qu'est-ce que l'horodatage ?

L'horodatage permet d'attester qu'une donnée existe à un instant donné Pour cela, il convient d'associer une représentation sans équivoque d'une donnée, par exemple une valeur de hachage associée à un identifiant d'algorithme de hachage, à un instant dans le temps. La garantie de cette association est fournie au moyen d'une contremarque de temps qui est une structure signée qui contient en particulier :

[1] En particulier, ce label est délivré par un organisme privé, accrédité par un organisme d'accréditation (le COFRAC en France) et habilité par l'ANSSI.

- l'identifiant de la politique d'horodatage sous laquelle la contremarque de temps a été générée ;
- la valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
- la date et le temps UTC ;
- l'identifiant du certificat de l'Unité d'horodatage (UH) qui a généré la contremarque de temps (qui contient aussi le nom de l'Autorité d'horodatage).

L'horodatage ne nécessite pas le déploiement d'une infrastructure étendue pour que la validité des certificats des unités d'horodatage puisse être vérifiée. En particulier, les utilisateurs finaux ne doivent pas nécessairement avoir des certificats eux-mêmes, mais doivent avoir accès aux informations de validité des certificats d'horodatage (chaîne de certification, LRC, …) pour vérifier les contremarques de temps.

La clé privée ou les clés utilisées pour générer les contremarques de temps sont gérées par l'Autorité d'horodatage qui conserve la pleine et entière responsabilité pour satisfaire aux exigences définies dans le document actuel. Une Autorité d'horodatage peut faire fonctionner plusieurs unités d'horodatage (UH). Chaque unité d'horodatage dispose de sa propre bi-clé.

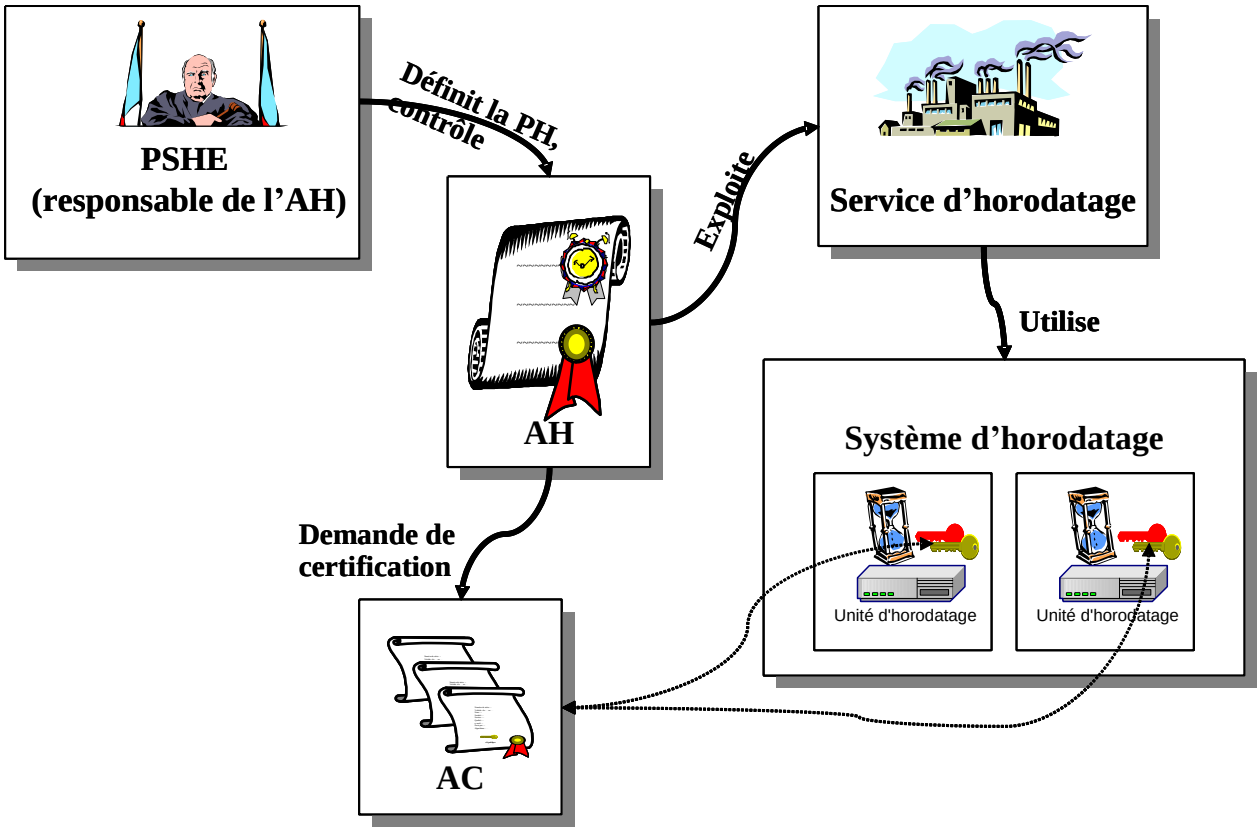
I.4. Comment établir la confiance en l'horodatage

La garantie apportée par l'autorité d'horodatage s'appuie sur des éléments techniques (décrits précédemment) et des règles de gestion qui sont présentées dans la politique d'horodatage. La politique d'horodatage présente aux utilisateurs les engagements que prend l'autorité d'horodatage, notamment ceux pris en matière de sécurité, et décrit de façon macroscopique les moyens mis en œuvre pour tenir ces engagements. Elle revêt une grande importance car elle incarne le niveau de confiance atteint par le service d'horodatage. Elle traduit la reconnaissance formelle de l'importance accordée par l'autorité d'horodatage à la sécurité du service.

Les exigences pour les services d'horodatage décrits dans le document incluent des exigences portant, à la fois sur la gestion de l'horodatage et sur le fonctionnement des unités d'horodatage qui publient les contremarques de temps. L'Autorité d'horodatage, telle qu'identifiée dans la contremarque de temps, a la responsabilité d'assurer que ces exigences sont remplies (par exemple par des obligations contractuelles). Elle peut sous-traiter à d'autres parties un sous-ensemble des services d'horodatage.

Par exemple, des organisations accueillant des unités d'horodatage peuvent exiger de contrôler l'utilisation du service et, au minimum, de savoir si le service est opérationnel ou être capable de mesurer le fonctionnement du service, par exemple le nombre de contremarques de temps produites pendant une période de temps. Un tel contrôle peut être considéré comme étant extérieur au service d'horodatage. La description des opérations de gestion décrites dans le corps principal du document n'est donc pas limitative. La surveillance des opérations, si elle est exécutée directement sur l'unité d'horodatage, peut être autorisée par le fournisseur du service d'horodatage.

I.5. Présentation des rôles et relations



La notion d'Autorité d'Horodatage (AH) telle qu'utilisée dans la présente PH Type est définie au chapitre II.1 ci-dessous.

L'AH exploite l'ensemble des services d'horodatage qui regroupe les diverses prestations organisationnelles et techniques nécessaires à la génération et à la gestion des contremarques de temps. Chaque UH signe ses contremarques de temps à l'aide d'une clé privée dont la clé publique correspondante a été certifiée au préalable par une autorité de certification (AC). Les clés privées sont conservées et mises en œuvre dans des modules d'horodatage.

I.6. Autres aspects

D'un point de vue technique, cette politique s'appuie sur un module d'horodatage pour la protection des clés de signature et de l'horloge.

II. Généralités

II.1. Définitions

Abonné - Entité ayant besoin de faire horodater des données par une Autorité d'horodatage et qui a accepté les conditions d'utilisation de ses services.

Autorité de Certification (AC) - Cf. les Politiques de Certification Types du [RGS].

Autorité d'horodatage (AH) - Au sein d'un PSHE, une Autorité d'Horodatage a en charge, au nom et sous la responsabilité de ce PSHE, l'application d'au moins une politique d'horodatage en s'appuyant sur une ou plusieurs Unités d'Horodatage. Dans le cadre de la présente PH Type, le terme de PSHE n'est pas utilisé en dehors du présent chapitre et du chapitre I.1 et le terme d'AH est le seul utilisé. Il désigne l'AH chargée de l'application de la politique d'horodatage, répondant aux exigences de la présente PH Type, au sein du PSHE souhaitant faire qualifier la famille de contremarques de temps correspondante.

Contremarque de temps - Donnée signée qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là

Coordinated Universal Time (UTC) - Echelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 [TF.460-5].

Nota - Pour la plupart des usages, le temps UTC est équivalent au temps solaire au méridien principal (0°). De manière plus précise, le temps UTC est un compromis entre le temps atomique particulièrement stable (Temps Atomique International -TAI) et le temps solaire dérivé de la rotation irrégulière de la terre lié au temps moyen sidéral de Greenwich (GMST) par une relation de convention.

Déclaration des pratiques d'horodatage (DPH) - Une DPH identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AH applique dans le cadre de la fourniture de ses services d'horodatage et en conformité avec la ou les politiques d'horodatage qu'elle s'est engagée à respecter.

Jeton d'horodatage - Voir contremarque de temps.

Module d'horodatage - Produit de sécurité comportant une ressource cryptographique et qui est dédié à la mise en œuvre des fonctions d'horodatage de l'UH, notamment la génération, la conservation et la mise en œuvre de la clé privée de signature de l'UH ainsi que la génération des contremarques de temps.

Politique d'horodatage (PH) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les abonnés et les utilisateurs de contremarques de temps.

Prestataire de services d'horodatage (PSHE) - L'[ORDONNANCE] introduit et définit les prestataires de service de confiance (PSCO). Un PSHE est un type de PSCO particulier. Un PSHE se définit comme toute personne ou entité qui est responsable de la génération et de la gestion de contremarques de temps, vis-à-vis de ses abonnés et des utilisateurs de ces contremarques de temps. Un PSHE peut fournir différentes familles de contremarques de temps correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSHE comporte au moins une AH mais peut en comporter plusieurs en fonction de son organisation. Un PSHE est identifié dans les certificats de clés publiques des UH dont il a la responsabilité au travers de ses AH.

Produit de sécurité - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Qualification d'un produit de sécurité - Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS]. La procédure de qualification des produits de sécurité est décrite dans le [DécretRGS]. Le [RGS] précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

Qualification d'un prestataire de services d'horodatage - Le [DécretRGS] décrit la procédure de qualification des PSCO. Un PSHE étant un PSCO particulier, la qualification d'un PSHE est un acte par lequel un organisme de qualification atteste de la conformité de tout ou partie de l'offre d'horodatage d'un PSHE à la présente PH Type.

Service d'horodatage - Ensemble des prestations nécessaires à la génération et à la gestion de contremarques de temps.

Système d'horodatage - Ensemble des unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir des services d'horodatage.

Unité d'Horodatage (UH) - Ensemble de matériel et de logiciel en charge de la création de contremarques de temps caractérisé par un identifiant de l'unité d'horodatage accordé par une AC, et une clé unique de signature de contremarques de temps.

UTC(k) - Temps de référence réalisé par le laboratoire "k" et synchronisé avec précision avec le temps UTC, dans le but d'atteindre une précision de ±100 ns, selon la recommandation S5 (1993) du Comité Consultatif pour la définition de la Seconde . (Rec. ITU-R TF.536-1 [TF.536-1]).

Nota - Une liste des laboratoires UTC(k) est indiquée dans la section 1 de la Circulaire T publiée par le BIPM et est disponible sur le site web du BIPM (www.bipm.org).

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives.

Nota - Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager..

Utilisateur de contremarque de temps – Entité (personne ou système) qui fait confiance à une contremarque de temps émise sous une politique d'horodatage donnée par une autorité d'horodatage donnée.

Utilisateur final - Abonné ou utilisateur de contremarques de temps.

II.2. Abréviations

Pour le présent document, les abréviations suivantes s'appliquent :

AC	Autorité de Certification
AH	Autorité d'horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CG	Conditions Générales d'utilisation du service d'horodatage
Delta-LRC	Liste de Révocation des Certificats partielle
DGME	Direction Générale de la Modernisation de l'Etat
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunications Standards Institute
LCR	Liste des Certificats Révoqués

IGC	Infrastructure de Gestion de Clés
OID	Object Identifier
PH	Politique d'Horodatage
PP	Profil de Protection
PSHE	Prestataire de Services d'Horodatage
UH	Unité d'Horodatage
UTC	Coordinated Universal Time

III. Politique d'horodatage

Pour cette politique, la date et le temps de chaque contremarque de temps doivent être synchronisés avec le temps UTC avec une exactitude précisée dans la déclaration des pratiques d'horodatage[2].

La présente PH Type impose un format de contremarque de temps spécifique, qui doit répondre aux exigences du chapitre VIII ci-dessous.

Cette politique n'impose pas l'usage d'un protocole d'horodatage spécifique pour demander et obtenir une contremarque de temps auprès d'une AH. Cependant, un protocole a été défini dans le [RFC3161] et profilé dans le document [ETSI_TSP] et son usage est recommandé.

Paramètres utilisés pour la politique d'horodatage

Les caractéristiques principales de cette politique sont comme suit :

- la protection des clés et de l'horloge doit respecter les exigences spécifiées au chapitre IX ci-dessous ;
- la sauvegarde et l'import des clés privées sont interdits ;
- l'AC générant les certificats de clé publique pour les unités d'horodatage doit gérer le service de révocation pour chaque certificat publié.

[2] Il est recommandé que celle-ci soit d'une seconde. Elle ne doit en tout cas pas excéder la minute.

IV. Déclaration des Pratiques d'Horodatage

La déclaration des pratiques d'horodatage expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la politique d'horodatage, en particulier les processus qu'une Autorité d'horodatage emploiera pour la création des contremarques de temps et le maintien de l'exactitude de ses horloges.

La déclaration des pratiques d'horodatage doit être une description détaillée des pratiques opérationnelles d'une Autorité d'horodatage mise en œuvre pour la délivrance des contremarques de temps et la gestion des services d'horodatage.

Une déclaration des pratiques d'horodatage doit définir comment l'Autorité d'horodatage se conforme aux exigences physiques, environnementales, procédurales, organisationnelles et techniques identifiées dans une politique d'horodatage. Une politique d'horodatage est ainsi un document moins spécifique qu'une déclaration des pratiques d'horodatage. Une politique d'horodatage est définie indépendamment des détails particuliers de l'environnement spécifique d'exploitation d'une Autorité d'horodatage, tandis qu'une déclaration des pratiques d'horodatage est façonnée à la structure organisationnelle, aux procédures d'exploitation, aux équipements et à l'environnement de travail d'une Autorité d'horodatage.

La déclaration des pratiques d'horodatage est toujours approuvée par le PSHE.

Contrairement à la politique d'horodatage, la DPH n'a pas pour objet d'être intégralement publiée. Cependant, l'Autorité d'horodatage est tenue de publier les parties publiques des déclarations des pratiques d'horodatage et en particulier :

- le cadre d'application de la DPH ;
- les coordonnées de l'AH ;
- la PH appliquée ;
- les algorithmes de hachage autorisés pour constituer l'objet horodaté ;
- la durée minimum pendant laquelle il est possible de vérifier les contremarques de temps, à compter de leur date de génération ;
- la précision de la date des contremarques de temps par rapport à l'échelle de temps UTC ;
- les obligations des abonnés ;
- les obligations des utilisateurs de contremarque de temps ;
- les informations permettant de vérifier la contremarque de temps ;
- les limitations de responsabilité.

Ces informations publiques peuvent être présentées sous la forme d'un document indépendant (extrait de la DPH) ou bien intégrées aux conditions générales d'utilisation (cf. chapitre suivant).

V. Conditions générales d'utilisation

Compte tenu de la complexité de lecture d'une PH et d'une DPH pour des utilisateurs non-spécialistes du domaine, l'AH doit définir également des conditions générales d'utilisation correspondant aux "TSA Disclosure Statement" (TDS) définis par [ETSI_PH].

Ces conditions générales d'utilisation ne sont pas destinées à remplacer la politique d'horodatage ou la déclaration des pratiques d'horodatage mais sont destinées à des abonnés et à des utilisateurs de contremarques de temps non-techniciens afin qu'ils puissent facilement comprendre l'information essentielle dont ils doivent avoir connaissance.

Des conditions générales d'utilisation peuvent aider une Autorité d'horodatage à démontrer comment elle répond aux exigences réglementaires, en particulier celles liées à la protection du consommateur.

Une Autorité d'horodatage spécifiera dans ses conditions générales d'utilisation les identifiants des politiques d'horodatage supportées.

Les Autorités d'horodatage sont tenues de définir leurs propres conditions générales d'utilisation et de les rendre disponibles aux abonnés et aux utilisateurs de contremarques de temps sous une ou des forme(s) lisible(s), compréhensible(s) et pérenne(s).

Il est recommandé que ces conditions générales aient une structure conforme à celle décrite en annexe B de [ETSI_PH] et reprennent ainsi, à destination des abonnés et des utilisateurs, les informations pertinentes de la PH et la DPH de l'AH (conditions d'usages des contremarques de temps, obligations et responsabilités des différentes parties, garanties et limites de garanties de l'AH, etc. : cf. chapitre VI.1.6).

Ces conditions générales d'utilisation peuvent être présentées :

- sous la forme de documents indépendants, et/soit ;
- dans le contrat avec l'abonné et/ou les utilisateurs, et/soit ;
- dans la déclaration des pratiques d'horodatage à condition qu'elles soient compréhensibles au lecteur, dans ce cas cette partie de la DPH devra être publiée.

VI. Contenu de la politique d'horodatage

Ce chapitre décrit les dispositions générales ainsi que les exigences opérationnelles, physiques et environnementales, procédurales et organisationnelles et enfin de sécurité technique, auxquelles l'AH doit se conformer. Cet ensemble de règle précise le contenu d'une politique d'horodatage.

VI.1. Dispositions générales

VI.1.1. Obligations de l'Autorité d'horodatage

L'Autorité d'horodatage doit garantir la conformité des exigences et des procédures prescrites dans cette politique, même quand les fonctionnalités d'horodatage sont remplies par des sous-traitants.

L'Autorité d'horodatage doit garantir l'adhésion aux obligations complémentaires indiquées dans la contremarque de temps ou bien directement ou bien incorporée par référence.

L'Autorité d'horodatage doit fournir des services d'horodatage conformément à sa déclaration des pratiques d'horodatage.

L'Autorité d'horodatage doit remplir tous ses engagements tels que stipulés dans ses conditions générales d'utilisation.

VI.1.2. Obligations de l'abonné

Au-delà des exigences spécifiques incluses dans les conditions générales d'utilisation du service d'horodatage, et que doit respecter l'abonné, il est recommandé que ce dernier, au moment de l'obtention d'une contremarque de temps, vérifie que le certificat de l'unité d'horodatage n'est pas révoqué, mais cela dépend de l'environnement d'utilisation. En effet, si le certificat est émis par le système d'information, il peut être superflu de vérifier celui-ci systématiquement, l'organisme utilisateur doit apprécier l'impact d'une erreur découverte par échantillonnage et le risque de certificats erronés entre deux contrôles au regard des performances. Inversement, si les certificats d'UH proviennent d'AH différentes, une vérification systématique est fortement recommandée.

VI.1.3. Obligations de l'utilisateur de contremarques de temps

Les conditions générales d'utilisation disponibles pour les utilisateurs de contremarques de temps doivent inclure une obligation qui spécifie que, pour faire confiance à une contremarque de temps, il devra :

a) Vérifier que la contremarque de temps a été correctement signée, et que le certificat de l'unité d'horodatage est valide à l'instant de la vérification.

Nota - Pendant la validité du certificat d'une unité d'horodatage, la validité de la clé de signature peut être vérifiée en utilisant l'état de révocation courant du certificat de l'unité d'horodatage. Si le temps de vérification excède la fin de la période de validité du certificat correspondant, voir le chapitre X ci-dessous.

b) tenir compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la politique d'horodatage, la déclaration des pratiques d'horodatage et les conditions générales d'utilisation.

VI.1.4. Obligations pour les AC fournissant les certificats des unités d'horodatage

Les certificats des clés publiques délivrés aux unités d'horodatage doivent être délivrés par des prestataires de service de certification électronique (PSCE) conformes au RGS, c'est à dire respectant au minimum les exigences du niveau de sécurité une étoile (*) de la Politique de Certification Type "cachet serveur". Un prestataire de service d'horodatage (PSH) souhaitant faire qualifier son service d'horodatage conformément à la procédure décrite dans le décret RGS devra recourir à un service de certification électronique d'un PSCE lui même qualifié

Nota - Les certificats des unités d'horodatage peuvent être générés par une Autorité de Certification opérée par la même organisation que l'Autorité d'horodatage, ou par une organisation différente.

VI.1.5. Déclarations des pratiques d'horodatage

L'Autorité d'horodatage doit garantir qu'elle possède la fiabilité nécessaire pour fournir des services d'horodatage. En particulier :

a) L'Autorité d'horodatage doit faire effectuer une évaluation de risques pour évaluer les actifs et les menaces pour ces actifs afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles.

b) L'Autorité d'horodatage doit avoir une déclaration des pratiques et des procédures utilisées pour adresser toutes les exigences identifiées dans chaque politique d'horodatage supportée.

Nota - Cette politique n'impose aucune exigence quant à la structure de la déclaration des pratiques d'horodatage.

c) La déclaration des pratiques d'horodatage doit identifier les obligations de toutes les organisations externes participant à la fourniture des services d'horodatage, y compris la politique applicable et les pratiques. Cela inclut l'AC fournissant les certificats aux unités d'horodatage.

d) L'Autorité d'horodatage doit mettre à la disposition des abonnés et des utilisateurs de contremarques de temps les éléments publics de sa déclaration des pratiques d'horodatage, s'il y a lieu, et toute autre documentation appropriée, tel que nécessaire pour évaluer la conformité à la politique d'horodatage.

Nota - Il n'est pas exigé que l'Autorité d'horodatage rende publics tous les détails de ses pratiques.

e) L'Autorité d'horodatage devra disposer d'une organisation adéquate pour l'approbation de la déclaration des pratiques d'horodatage et la vérification de la concordance entre cette déclaration et les politiques d'horodatage choisies.

f) Le responsable opérationnel de l'Autorité d'horodatage doit garantir que les pratiques sont correctement mises en œuvre.

g) L'Autorité d'horodatage doit définir une procédure de contrôle périodique de la conformité des pratiques, y compris les responsabilités, à la déclaration des pratiques d'horodatage.

h) L'Autorité d'horodatage doit informer au préalable les abonnés pour tout changement qu'elle a l'intention de faire dans la partie publique de sa déclaration des pratiques d'horodatage et, après l'approbation comme dans (e) ci-dessus, immédiatement mettre à la disposition des abonnés et des utilisateurs de contremarques de temps la partie publique révisée de la déclaration des pratiques d'horodatage comme exigé sous (d) ci-dessus.

i) Si l'Autorité d'horodatage a été évaluée pour être en conformité avec la Politique d'horodatage identifiée et si une modification envisagée à l'initiative de l'Autorité d'horodatage pouvait entraîner une non-conformité avec la politique d'horodatage ou avec la déclaration des pratiques d'horodatage, alors l'Autorité d'horodatage doit indiquer qu'elle soumettra cette modification à l'organisme évaluateur indépendant pour avis.

Si elles ne font partie pas des conditions générales d'utilisation du service d'horodatage, les déclarations des pratiques d'horodatage doivent comporter, au moins pour chaque politique d'horodatage, supportée par l'Autorité d'horodatage :

a) Les obligations de l'abonné.

b) Les obligations des utilisateurs de contremarques de temps.

VI.1.6. Conditions générales d'utilisation

L'Autorité d'horodatage doit mettre à disposition de tous ses abonnés et des utilisateurs potentiels de contremarques de temps, au moins pour chaque politique d'horodatage supportée par l'Autorité d'horodatage :

a) Une information sur un point de contact pour l'Autorité d'horodatage.

b) Une description ou une référence de la politique d'horodatage appliquée.

c) Au moins un algorithme de hachage qui peut être utilisé pour représenter la donnée à horodater.

d) La période de temps minimum, hors cas de révocation, durant laquelle les contremarques de temps seront vérifiables.

e) L'exactitude du temps dans les contremarques de temps par rapport au temps UTC.

f) N'importe quelles limitations sur l'utilisation du service d'horodatage.

g) Les obligations de l'abonné, si elles ne font partie ni du contrat avec l'abonné, ni de la déclaration des pratiques d'horodatage.

h) Les obligations des utilisateurs de contremarques de temps, si elles ne font partie ni du contrat avec les utilisateurs de contremarques de temps, ni de la déclaration des pratiques d'horodatage.

i) L'information sur la manière de vérifier les contremarques de temps de telle façon que l'utilisateur de contremarques de temps puisse "raisonnablement avoir confiance" dans les contremarques de temps ainsi que les restrictions possibles sur sa période de validité.

j) La période de temps pendant laquelle les fichiers d'audit de l'Autorité d'horodatage sont conservés.

k) Le système légal applicable.

l) Les limitations de responsabilité.

m) Les procédures pour les plaintes et le règlement des conflits.

n) Le nom de l'organisme de qualification indépendant ayant validé la conformité avec la présente PH Type.

o) Les éléments permettant de valider la chaîne de certificats (du certificat de l'unité d'horodatage au certificat auto-signé). Un certificat racine auto-signé ne permet pas de garantir par lui-même que la clé publique correspondante appartient bien à l'AC considérée. Sa diffusion doit s'accompagner de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat, et éventuellement de la clé publique, ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC.

p) Le nom du pays dans lequel l'Autorité d'horodatage est établie et l'identifiant de l'Autorité d'horodatage (tel que figurant dans le certificat de l'unité d'horodatage).

L'autorité d'horodatage peut également mettre à disposition les conditions de disponibilité du service, par exemple le temps moyen d'indisponibilité du service d'horodatage, le temps moyen de rétablissement du service suite à une indisponibilité et les dispositions prises pour les plans de secours, y compris les services de secours prévus.

VI.1.7. Conformité avec les exigences légales

L'Autorité d'horodatage doit garantir la conformité avec les exigences légales. En particulier :

a) Des mesures techniques appropriées et organisationnelles doivent être prises contre le traitement non autorisé ou illégal des données personnelles (cf. [CNIL]), contre la perte accidentelle, la destruction de données personnelles ou les dégâts commis aux données personnelles.

b) Les informations fournies par les abonnés à l'Autorité d'horodatage ne doivent pas être divulguées, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.

VI.2. Exigences opérationnelles

VI.2.1. Gestion des requêtes de contremarques de temps

La fourniture d'une contremarque de temps en réponse à une demande (par exemple les performances et le prix du service) est à la discrétion de l'Autorité d'horodatage selon les conditions générales d'utilisation avec l'abonné. Il est toutefois recommandé que la réponse de la part du PSHE à une requête de création de contremarque de temps n'excède pas quelques secondes[3], ceci afin de ne pas nuire ni dégrader l'ergonomie de l'application appelante.

VI.2.2. Fichiers d'audit

L'Autorité d'horodatage doit garantir que toutes les informations appropriées concernant le fonctionnement du service d'horodatage sont enregistrées pendant une période de temps suffisante et précisée dans la déclaration des pratiques d'horodatage), en particulier dans le but de fournir une preuve en cas d'enquêtes légales.

En particulier :

Général

a) Les événements spécifiques et les données enregistrées doivent être documentés par l'Autorité d'horodatage.

b) La confidentialité et l'intégrité des enregistrements d'audit courants et archivés relatifs au fonctionnement des services d'horodatage doivent être assurée.

c) Les enregistrements relatifs à l'administration des services d'horodatage doivent être intégralement archivés et de manière adaptée à la sensibilité des informations.

d) Les enregistrements relatifs au fonctionnement des services d'horodatage doivent être disponibles si exigé dans le but de fournir une preuve d'un fonctionnement correct des services d'horodatage en cas d'enquêtes légales.

e) L'instant précis d'évènements significatifs concernant l'environnement de l'Autorité d'horodatage, la gestion des clés, et la synchronisation de l'horloge doit être enregistré.

f) Les enregistrements relatifs à l'administration du service d'horodatage doivent être gardés, après la date d'expiration de la validité de la clé de signature de l'unité d'horodatage durant une période de temps appropriée pour fournir des éléments de preuves nécessaires tel qu'indiqué dans les conditions générales d'utilisation de l'Autorité d'horodatage.

g) Les événements doivent être enregistrés de telle façon qu'ils ne puissent pas être facilement supprimés ou détruits (sauf s'ils sont transférés sur un support de sauvegarde) durant la période de temps où l'on exige qu'ils soient conservés.

   Nota - Cela peut être réalisé, par exemple, à l'aide de supports qui ne peuvent être écrits qu'une seule fois, l'enregistrement de chaque support amovible utilisé et l'utilisation d'un site de sauvegarde hors-site.

h) Toute information enregistrée au sujet d'un abonné doit être tenue confidentielle sauf lorsqu'un accord est passé avec l'abonné pour une publication plus large.

Gestion des clés

i) Les enregistrements concernant tous les événements touchant au cycle de vie des clés doivent être effectués.

[3] Ce temps de réponse est le délai écoulé entre la réception par le PSHE de la requête et la signature de la contremarque de temps résultante.

j) Les enregistrements concernant tous les événements touchant au cycle de vie des certificats des unités d'horodatage doivent être effectués.

Synchronisation de l'horloge

k) Les enregistrements concernant tous les événements touchant à une synchronisation de l'horloge des unités d'horodatage doivent être effectués. Cela doit inclure l'information concernant des recalibrages ou des synchronisations normales.

l) Les enregistrements concernant tous les événements touchant à la détection de perte de synchronisation doivent être effectués.

VI.2.3. Gestion de la durée de vie de la clé privée

L'Autorité d'horodatage doit garantir que les clés privées de signature des unités d'horodatage ne sont pas employées au-delà de la fin de leur cycle de vie. En particulier :

a) Des procédures opérationnelles ou techniques doivent être mises en place pour assurer qu'une nouvelle paire de clés est mise en place quand la fin de la période d'utilisation d'une clé privée d'unité d'horodatage a été atteinte.

b) Le système d'horodatage doit détruire la clé privée si la fin de la période d'utilisation de cette clé privée a été atteinte.

VI.2.4. Synchronisation de l'horloge

L'Autorité d'horodatage doit garantir que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée. En particulier :

a) Le calibrage de chaque horloge d'unité d'horodatage doit être maintenu de telle manière que les horloges ne puissent pas normalement dériver à l'extérieur de l'exactitude déclarée.

b) Les horloges des unités d'horodatage doivent être protégées contre les menaces relatives à leur environnement qui pourraient aboutir à une désynchronisation avec le temps UTC en dehors de l'exactitude déclarée.

Nota - Une analyse des risques doit être conduite sur le système afin d'identifier les menaces contre lesquelles les horloges des unités d'horodatage doivent se protéger. Les menaces peuvent inclure des modifications par du personnel non autorisé, des ondes radio ou des chocs électriques.

c) L'Autorité d'horodatage devra garantir que, que si son horloge interne ne respecte plus l'exactitude déclarée, alors cela sera détecté.

Nota - L'information sur de tels événements doit être publiée à destination des utilisateurs de contremarques de temps.

d) Si l'horloge d'une unité d'horodatage est détectée comme étant en dehors de l'exactitude annoncée, alors les contremarques de temps ne doivent plus être générées.

e) L'Autorité d'horodatage doit garantir que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé comme notifié par l'organisme approprié. Le changement pour tenir compte du saut de seconde doit être effectué durant la dernière minute du jour où le saut de seconde est programmé. Un enregistrement du temps exact (selon l'exactitude déclarée) de l'instant de ce changement doit être effectué.

Nota - Un saut de seconde est un ajustement par rapport au temps UTC effectué en sautant ou en ajoutant une seconde durant la dernière minute d'un mois UTC. On donne la première préférence à la fin de décembre et juin et on donne la seconde préférence à la fin de mars et septembre.

VI.2.5. Exigences du contenu d'une contremarque de temps

L'Autorité d'horodatage doit garantir que les contremarques de temps sont générées en toute sécurité et incluent le temps correct. En particulier :

a) La contremarque de temps doit inclure l'identifiant du certificat de l'unité d'horodatage. Ce certificat doit inclure :

- un identifiant du pays dans lequel l'Autorité d'horodatage est établie,
- un identifiant de l'Autorité d'horodatage,
- une identification de l'unité d'horodatage qui génère les contremarques de temps.

b) La contremarque de temps doit inclure un identifiant de la politique d'horodatage.

c) Chaque contremarque de temps doit comporter un identifiant unique.

d) Les informations de temps portées dans les contremarques de temps doivent pouvoir être reliées à au moins un temps fourni par un laboratoire UTC (k).

Nota - Le Bureau des International Poids et Mesures (BIPM) calcule UTC sur la base des représentations locales UTC (k) d'un grand ensemble de montres atomiques dans des instituts de métrologie nationaux et des observatoires nationaux astronomiques autour du monde. Le BIPM dissémine le temps UTC par sa Circulaire mensuelle T. Celle-ci est disponible sur le site Web BIPM (www.BIPM.org) qui identifie officiellement tous les instituts ayant des échelles de temps UTC (k) reconnues.

e) Le temps inclus dans une contremarque de temps doit être synchronisé avec le temps UTC au moins avec l'exactitude définie dans la DPH.

f) Si une contremarque de temps inclut un temps qui est synchronisé avec le temps UTC avec une exactitude différente de la seconde, alors cette exactitude doit être indiquée dans la contremarque de temps.

g) La contremarque de temps doit inclure une représentation de la donnée à horodater (c'est-à-dire la valeur de hachage et l'identifiant d'algorithme de hachage) telle que fournie par le demandeur.

h) La contremarque de temps doit être signée en employant une clé produite exclusivement à cette fin.

i) La contremarque de temps doit, de plus, respecter les exigences du chapitre VIII ci-dessous.

Nota - Dans le cas de demandes d'horodatage survenant durant un intervalle de temps correspondant à l'exactitude de l'horloge de l'unité d'horodatage, l'ordonnancement des contremarques de temps à l'intérieur de cet intervalle n'est pas requis.

VI.2.6. Compromission de l'AH

L'Autorité d'horodatage doit garantir dans le cas d'événements qui affectent la sécurité des services d'horodatage, incluant la compromission de la clé privée de signature d'une unité d'horodatage ou la perte détectée de calibrage qui pourrait affecter des contremarques de temps émises, qu'une information appropriée est mise à la disposition des abonnés et des utilisateurs de contremarques de temps. En particulier :

a) Le plan de secours de l'Autorité d'horodatage doit traiter le cas de la compromission réelle ou suspectée de la clé privée de signature d'une unité d'horodatage ou la perte de calibrage de l'horloge d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises.

b) Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises, l'Autorité d'horodatage mettra à la disposition de tous les abonnés et utilisateurs de contremarques de temps une description de la compromission qui est survenue.

c) Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises, l'Autorité d'horodatage prendra les mesures nécessaires pour que les contremarques de temps de cette unité ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.

d) En cas d'un évènement majeur dans le fonctionnement de l'Autorité d'horodatage ou d'une une perte de calibrage, qui pourrait affecter des contremarques de temps émises, chaque fois que cela sera

possible, l'Autorité d'horodatage mettra à la disposition de tous ses abonnés et des utilisateurs de contremarques de temps toute information pouvant être utilisée pour identifier les contremarques de temps qui pourraient avoir été affectées, à moins que cela ne contrevienne à la vie privée des abonnés ou à la sécurité des services d'horodatage.

e) L'AH doit également prévenir directement et sans délai le point de contact de la DGME identifié sur le site : http://www.references.modernisation.gouv.fr.

Nota - Dans le cas où une clé privée serait réellement compromise, un fichier d'audit de toutes les contremarques de temps produites par l'unité d'horodatage peut fournir le moyen de distinguer entre des contremarques de temps véritables et des fausses contremarques de temps antidatées. Deux contremarques de temps de deux unités d'horodatage différentes de la même Autorité d'horodatage ou, mieux, de deux Autorités d'horodatage différentes peuvent être une autre façon de résoudre ce problème (voir chapitre X ci-dessous).

VI.2.7. Fin d'activité

Il est nécessaire de définir les procédures de fin d'activité ou de reprise par un tiers. Dans ce cadre, l'Autorité d'horodatage doit garantir que les dérangements potentiels aux abonnés et aux utilisateurs de contremarques de temps seront réduits au minimum suite à la cessation d'activité du service d'horodatage et assurer en particulier la maintenance continue des informations nécessaires pour vérifier la justesse de contremarques de temps. En particulier :

a) Avant que l'Autorité d'horodatage ne termine ses services d'horodatage les procédures suivantes doivent être exécutées au minimum :

- l'Autorité d'horodatage rendra disponible à tous ses abonnés et aux utilisateurs de contremarques de temps l'information concernant sa fin d'activité ;

- l'Autorité d'horodatage doit abroger les autorisations données aux sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de génération des contremarques de temps ;

- l'Autorité d'horodatage transférera à un organisme fiable ses obligations de maintien des fichiers d'audit et des archives nécessaires pour démontrer son fonctionnement correct durant une période raisonnable ;

- l'Autorité d'horodatage maintiendra ou transférera à un organisme fiable ses obligations de rendre disponible aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats ;

- les clés privées des unités d'horodatage doivent être détruites de telle façon que les clés privées ne puissent pas être recouvrées.

b) L'Autorité d'horodatage doit prendre les mesures nécessaires pour couvrir les dépenses pour accomplir ces exigences minimales dans le cas où l'Autorité d'horodatage tomberait en faillite ou pour d'autres raisons serait incapable de couvrir les dépenses par elle-même.

c) L'Autorité d'horodatage doit indiquer dans sa PH les dispositions prises pour la fin du service. Cela doit inclure :

- un avis aux abonnés et aux utilisateurs de contremarques de temps ;

- un transfert des obligations de l'Autorité d'horodatage à d'autres organismes.

e) L'AH doit également prévenir directement et sans délai le point de contact de la DGME identifié sur le site : http://www.references.modernisation.gouv.fr.

VI.3. Exigences physiques et environnementales, procédurales et organisationnelles

VI.3.1. Exigences physiques et environnementales

L'Autorité d'horodatage doit garantir que l'accès physique aux services critiques est contrôlé et que les risques physiques d'atteinte à ses actifs sont réduits au minimum. En particulier :

a) A la fois pour la fourniture du service d'horodatage et la gestion de l'horodatage :

- l'accès physique aux équipements concernés par les services d'horodatage doit être limité aux individus autorisés ;

- des contrôles doivent être mis en oeuvre pour éviter la perte, des dégâts ou la compromission d'actifs et l'interruption des activités et ;

- des contrôles doivent être mis en oeuvre pour éviter la compromission ou le vol d'informations ou d'équipements informatiques.

b) Des contrôles d'accès doivent être appliqués aux modules d'horodatage pour remplir les exigences de sécurité des modules d'horodatage. Les contraintes sur l'environnement d'exploitation, identifiées dans la documentation liée à la certification du module (PP, cible de sécurité,… ; cf. chapitre IX ci-dessous) doivent être remplies.

c) Les contrôles suivants complémentaires doivent être appliqués à la gestion du service d'horodatage :

- le système d'horodatage doit fonctionner dans un environnement qui protège physiquement les services de la compromission au moyen d'un accès non autorisé aux systèmes ou aux données ;

- la protection physique doit être réalisée par la création d'un périmètre de sécurité dédié clairement défini (c'est-à-dire des barrières physiques) autour des unités d'horodatage ;

- des contrôles de sécurité physique et environnementale doivent être mis en oeuvre pour protéger l'environnement qui abrite les ressources du système, les ressources du système elles-mêmes et les équipements utilisés pour remplir leur fonction ; la politique de sécurité physique et environnementale de l'Autorité d'horodatage pour les systèmes concernés par la gestion de l'horodatage doit au minimum concerner le contrôle d'accès physique, la protection vis à vis des catastrophes naturelles, les facteurs de sécurité liés au feu, la défaillance des services de base (par exemple le secteur, les télécommunications), l'écroulement de la structure, des fuites de plomberie, la protection contre le vol, la casse et la pénétration et, le rétablissement de la sécurité après un désastre ;

- des contrôles doivent être mis en œuvre pour empêcher des équipements, de l'information, des médias et du logiciel touchant aux services d'horodatage d'être enlevés du site sans autorisation.

VI.3.2. Exigences procédurales

L'Autorité d'horodatage doit garantir que les composants du système d'Horodatage sont sûrs et correctement opérés, avec un risque minimal d'échec. En particulier :

a) L'intégrité des composants du système d'horodatage et l'information doivent être protégés contre les virus, les logiciels malveillants et non autorisés.

b) Un rapport d'incident et des procédures de réponse aux incidents doivent être employés d'une telle façon que les dégâts liés aux incidents de sécurité et aux défaillances soient réduits au minimum.

c) Les supports employés dans les systèmes d'horodatage doivent être manipulés de manière sécuritaire pour les protéger des dégâts, du vol, de l'accès non autorisé et de l'obsolescence.

Nota - Chaque membre du personnel avec des responsabilités de gestion est responsable de la planification et de l'exécution effective de la politique d'horodatage et des pratiques d'horodatage.

d) Des procédures doivent être établies et mises en oeuvre pour tous les rôles de confiance et administratifs qui impactent la fourniture des services d'horodatage.

Manipulation et sécurité des supports

e) Tous les supports doivent être traités de manière sécuritaire conformément aux exigences de la classification de l'information. Les supports contenant des données sensibles doivent être retirés de manière sécuritaire quand ils ne sont plus utiles.

Planification de Système

f) Les charges doivent être contrôlées et des projections de charge dans le futur doivent être effectuées pour garantir que des puissances de traitement et des stockages adéquats seront disponibles.

Rapport d'incident et réponse

g) L'Autorité d'horodatage agira d'une façon opportune et coordonnée pour répondre rapidement aux incidents et limiter l'impact des infractions à la sécurité. Tous les incidents doivent être rapportés aussitôt que possible après l'incident.

Les contrôles complémentaires suivants doivent être appliqués à la gestion de l'horodatage :

Procédures de fonctionnement et responsabilités

h) Les opérations de sécurité doivent être séparées des autres opérations.

Nota - Les opérations de sécurité incluent :

• les procédures opérationnelles et les responsabilités ;

• la planification et la qualification des systèmes sécurisés ;

• la protection vis-à-vis du logiciel malveillant ;

• la maintenance ;

• la gestion du réseau ;

• le contrôle actif des journaux d'audit, l'analyse des événements et les suites à donner ;

• le traitement et la sécurité des médias ;

• l'échange des données et du logiciel.

Ces opérations doivent être gérées par du personnel de confiance de l'Autorité d'horodatage, mais, peuvent aussi être exécutées par du personnel opérationnel non-spécialiste (sous surveillance), comme défini dans la politique de sécurité appropriée et, les documents sur les rôles et les responsabilités.

Gestion d'Accès au Système

L'Autorité d'horodatage doit garantir que l'accès au système d'horodatage est limité aux individus dûment autorisés. En particulier :

a) Des contrôles (par exemple, des pares-feux (firewalls)) doivent être mis en oeuvre pour protéger le réseau interne de l'Autorité d'horodatage d'accès non autorisés incluant l'accès par des abonnés et des tierces personnes.

Nota - Les pares-feux (firewalls) devraient aussi être configurés pour bloquer tous les protocoles et les accès non nécessaires au fonctionnement de l'Autorité d'horodatage.

b) L'Autorité d'horodatage doit garantir une administration efficace des utilisateurs (cela inclut les opérateurs, les administrateurs et les auditeurs), pour maintenir la sécurité du système, y compris la gestion des comptes des utilisateurs, l'audit, et la modification ou le retrait rapide d'accès.

c) L'Autorité d'horodatage doit garantir que l'accès aux fonctions du système, à l'information et aux applications est limité conformément à la politique de contrôle d'accès et que le système d'horodatage possède les contrôles informatiques de sécurité suffisants pour la séparation des rôles de confiance identifiés dans les pratiques d'horodatage, y compris la séparation des fonctions d'administrateur de sécurité et des fonctions opérationnelles. En particulier, l'utilisation de programmes systèmes utilitaires sera limitée et très contrôlée.

d) Le personnel de l'Autorité d'horodatage doit être correctement identifié et authentifié avant d'utiliser des applications critiques liées à l'horodatage.

e) Le personnel de l'Autorité d'horodatage sera tenu responsable de ses activités, par exemple en conservant des fichiers d'audit.

Les contrôles complémentaires suivants doivent être appliqués à la gestion de l'horodatage :

f) L'Autorité d'horodatage doit garantir que des composants de réseau locaux (par exemple les routeurs) seront mis dans un environnement physiquement sûr et que leurs configurations sont périodiquement vérifiées pour la conformité avec les exigences indiquées par l'Autorité d'horodatage.

g) Une surveillance permanente et des équipements d'alarme doivent être mis en œuvre pour permettre à l'Autorité d'horodatage de détecter, d'enregistrer et de réagir rapidement à n'importe quelle tentative non autorisée et/ou irrégulière d'accès à ses ressources.

Nota - On peut employer, par exemple, un système de détection d'intrusion, une surveillance de contrôle d'accès et des équipements d'alarme.

Déploiement et Maintenance

L'Autorité d'horodatage emploiera des produits et systèmes de confiance. Concernant les modules d'horodatage ils répondront aux exigences du chapitre IX ci-dessous.

Nota - L'analyse de risque effectuée sur les services d'horodatage devrait identifier les services critiques exigeant des systèmes évalués et les niveaux d'assurance exigés.

En particulier :

a) Une analyse des exigences de sécurité doit être effectuée au moment de la conception et de l'étape de spécification des exigences pour tout projet de développement de systèmes entrepris par l'Autorité d'horodatage ou pour le compte de l'Autorité d'horodatage pour assurer que la sécurité fait partie du système d'information.

b) Des procédures de contrôle de changement doivent être appliquées pour les nouvelles versions, les modifications et les corrections d'anomalies de n'importe quel logiciel opérationnel.

VI.3.3. Exigences organisationnelles

L'Autorité d'horodatage doit garantir que le personnel et des pratiques d'embauche améliorent et concourent à la fiabilité des opérations de l'Autorité d'horodatage.

En particulier :

a) L'Autorité d'horodatage doit employer un personnel qui possède l'expertise, l'expérience et les qualifications nécessaires pour les services offerts, tels que l'exige la fonction.

Nota - Le personnel de l'Autorité d'horodatage devrait être en mesure de remplir l'exigence de "l'expertise, l'expérience et des qualifications" au moyen de la formation professionnelle et d'attestations professionnelles, de l'expérience réelle, ou d'une combinaison des deux.

Nota - Le personnel employé par l'Autorité d'horodatage inclut le personnel individuel contractuellement engagé dans l'exécution des fonctions pour supporter les services d'horodatage. Le personnel qui peut être impliqué dans la surveillance des services de l'Autorité d'horodatage n'a pas besoin de faire partie du personnel de l'Autorité d'horodatage.

b) Les rôles de sécurité et les responsabilités, comme spécifié dans la politique de sécurité de l'Autorité d'horodatage, doivent être documentés dans des descriptions de poste. Les rôles de confiance, sur lesquels la sécurité du fonctionnement de l'Autorité d'horodatage repose, doivent être clairement identifiés.

c) Des descriptions de fonctions doivent être définies pour le personnel de l'Autorité d'horodatage (aussi bien provisoire que permanent) du point de vue de la séparation des responsabilités et du principe du privilège minimum, selon la sensibilité de la fonction sur la base des responsabilités et des niveaux d'accès, et indiquer le type d'enquête à effectuer sur le passé, le type de formation appropriée et les particularités de la fonction. Quand cela est nécessaire, ces descriptions de fonctions doivent faire la différence entre les fonctions générales et les fonctions spécifiques à l'Autorité d'horodatage. Ces descriptions de fonctions devraient inclure des exigences d'expérience et de compétences.

d) Le personnel doit effectuer des procédures administratives et de gestion ainsi que des processus en accord avec les procédures de gestion de sécurité de l'information de l'Autorité d'horodatage.

Les contrôles complémentaires suivants doivent être appliqués à la gestion de l'horodatage :

e) le personnel de gestion employé doit posséder :

- la connaissance de la technologie de l'horodatage et ;

- la connaissance de technologie de la signature numérique et ;

- la connaissance des mécanismes pour le calibrage ou la synchronisation des horloges des unités d'horodatage avec le temps UTC et ;

- pour le personnel avec des responsabilités de sécurité, une bonne connaissance des procédures de sécurité, et ;

- l'expérience avec la sécurité de l'information et l'évaluation des risques.

f) Tout le personnel de l'Autorité d'horodatage dans des rôles de confiance doit être libre de conflit d'intérêt qui pourrait porter préjudice à l'impartialité des opérations de l'Autorité d'horodatage.

g) Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes :

- les officiers chargés de la sécurité : responsabilité complète d'administrer la mise en oeuvre des pratiques de sécurité ;

- les administrateurs système : autorisés à installer, configurer et maintenir les modules d'horodatage de l'Autorité d'horodatage pour la gestion de l'horodatage ;

- les opérateurs système : responsables pour faire fonctionner les modules d'horodatage de l'Autorité d'horodatage de manière quotidienne. Autorisés pour effectuer les opérations de sauvegarde et des secours ;

- les auditeurs de système : autorisés à consulter les archives et les fichiers d'audit des modules d'horodatage.

h) Le personnel de l'Autorité d'horodatage doit être formellement nommé aux rôles de confiance par la direction responsable de la sécurité.

i) L'Autorité d'horodatage ne doit pas nommer aux rôles de confiance ou de gestion toute personne connue pour avoir une condamnation pour un crime sérieux ou une autre infraction qui affecte son adéquation avec la position. Le personnel ne doit pas avoir accès aux fonctions de confiance avant que les contrôles nécessaires ne soient achevés.

VI.4. Exigences de sécurité techniques

VI.4.1. Exactitude temps

Si une unité d'horodatage fournit une exactitude différente de la seconde, alors cette exactitude doit être indiquée dans chaque contremarque de temps générée.

Nota - Ceci permet d'afficher une cohérence avec la politique [ETSI_PH], toutefois, il est possible d'indiquer dans la contremarque de temps l'exactitude de l'unité d'horodatage dans le cas ou celle-ci est d'une seconde.

VI.4.2. Génération de clé

L'Autorité d'horodatage doit garantir que toutes les clés cryptographiques sont produites dans des circonstances contrôlées. En particulier, la génération des clés de signature des unités d'horodatage doit être effectuée dans un module d'horodatage répondant aux exigences du chapitre IX ci-dessous.

VI.4.3. Certification des clés de l'unité d'horodatage

L'Autorité d'Horodatage doit s'assurer que la valeur de la clé publique et l'identifiant de l'algorithme de signature contenus dans la demande de certificat de l'Unité d'Horodatage sont égaux à ceux générés par l'Unité d'Horodatage.

L'Autorité d'Horodatage doit s'assurer qu'une demande de certificat d'Unité d'Horodatage auprès d'une Autorité de Certification contient, en plus des informations exigées dans la PC Type « cachet » pour la partie enregistrement, au moins les informations suivantes :

- le nom (DN) de l'unité d'horodatage pour laquelle la demande de certificat est faite ;
- la valeur de la clé publique (et l'identifiant de l'algorithme) ;
- la durée d'utilisation souhaitée pour la clé privée.

L'Autorité d'Horodatage doit vérifier, lors de l'import du certificat de l'Unité d'Horodatage, qu'il provient bien de l'Autorité de Certification auprès de laquelle la demande de certificat a été effectuée.

L'Autorité d'Horodatage doit s'assurer que l'Unité d'Horodatage ne peut être opérationnelle qu'une fois ces exigences remplies.

VI.4.4. Protection des clés privées des unités d'horodatage

L'Autorité d'horodatage doit garantir que des clés privées des unités d'horodatage restent confidentielles et conservent leur intégrité. En particulier, les clés de signature des unités d'horodatage doivent être gardées et utilisées à l'intérieur d'un module d'horodatage répondant aux exigences du chapitre IX ci-dessous.

VI.4.5. Exigences de sauvegarde des clés des unités d'horodatage

L'autorité d'horodatage doit garantir que la sauvegarde des clés des unités d'horodatage est interdite.

VI.4.6. Destruction des clés des unités d'horodatage

L'Autorité d'horodatage doit garantir que les clés de signature des unités d'horodatage sont détruites à la fin de leur cycle de vie.

VI.4.7. Algorithmes obligatoires

L'Autorité d'horodatage doit, dans la limite des algorithmes qu'elle reconnaît :

a) Accepter des valeurs de hachage générées par des clients et employant les algorithmes de hachage conformes aux exigences du chapitre VIII ci-dessous.

b) Générer des contremarques de temps signées selon les algorithmes et les longueurs de clé conformes aux exigences du chapitre VIII ci-dessous.

VI.4.8. Vérification des contremarques de temps

L'Autorité d'horodatage doit garantir que les utilisateurs de contremarques de temps peuvent avoir accès à l'information utilisable pour vérifier la signature numérique des contremarques de temps. En particulier :

a) Les certificats des unités d'horodatage doivent être disponibles, soit joints à la contremarque de temps, soit disponibles par d'autres moyens, par exemple un serveur.

b) Un ou plusieurs certificats utilisables pour valider une chaîne de certificats se terminant par un certificat d'unité d'horodatage doivent être disponibles.

VI.4.9. Durée de validité des certificats de clé publique des unités d'horodatage

La durée de validité des certificats des unités d'horodatage ne doit pas être plus longue que :

- La durée de vie cryptographique de la clé privée associée (cf [RGS_B_1]).
- Fin de validité du certificat d'AC qui l'a émis.

Il est à prendre en considération le fait que plus la durée de vie du certificat sera grande, plus la taille des enregistrements d'audit à conserver sera importante.

VI.4.10. Durée d'utilisation des clés privées des unités d'horodatage

La durée d'utilisation d'une clé privée sera au plus égale à la période de validité du certificat de clé publique correspondant. Toutefois elle sera en pratique réduite afin que la validité des contremarques de temps générées avec cette clé puisse être effectuée durant un laps de temps suffisant. La durée d'utilisation de la clé privée peut être définie soit au moment de l'initialisation du boîtier de l'unité d'horodatage, soit en définissant cette durée dans le certificat (PrivateKeyUsagePeriod).

VII. Annexe 1 : Documents cités en référence

VII.1. Réglementation

Renvoi	Document
[CNIL]	*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004*
[ORDONNANCE]	*Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électronique entre les usagers et les autorités administratives et entre les autorités administratives*
[DécretRGS]	*Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005*

VII.2. Documents techniques

Renvoi	Document
[RGS]	*Référentiel Général de Sécurité – version 1.0*
[RGS_A_14]	*RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3*
[RGS_B_1]	*Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 1.20*
[ETSI_PH]	*ETSI TS 102 023 V1.2.2 (2008-10) Policy requirements for Time-Stamping Authority*
[ETSI_TSP]	*ETSI TS 101 861 V1.2.1 (2002-03) Time Stamping Profile*
[PP_HORO]	*DCSSI - Profil de Protection - Systèmes d'horodatage EAL3+ DCSSI PP 2008/07*
[PROG_ACCRED]	*COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – disponible : www.cofrac.fr*
[RFC3161]	*IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol -08/2001*
[TF.460-5]	*ITU-R Recommendation TF.460-5 (1997) "Standard-Frequency and Time-signal emissions".*
[TF.536-1]	*ITU-R Recommendation TF. TF.536-1(1998): "Time-Scale Notations".*

VIII. Annexe 2 : Exigences sur les formats des contremarques de temps, des certificats et des LCR et sur les algorithmes cryptographiques

VIII.1. Contremarques de temps

Les contremarques de temps fournies par les AH respectant la présente PH Type doivent être une structure TimeStampToken conforme au [RFC3161].

Le tableau ci-dessous reprend l'ensemble des champs d'un TimeStampToken tels que définis dans le [RFC3161]. Une contremarque de temps conforme à cette PH Type doit respecter, de base, les exigences correspondantes du [RFC3161], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Exigences
messageImprint	Cf. chapitre VIII.3 ci-dessous sur les exigences concernant les fonctions de hachage.
accuracy	Si la synchronisation avec le temps UTC est différente de 1 seconde, ce champ doit être présent et doit préciser l'exactitude de la synchronisation. Si la synchronisation est de 1 seconde, il peut être omis.
ordering	Ce champ doit être absent ou bien contenir la valeur false.
tsa	Si ce champ est présent, il doit être identique au champ subject du certificat de l'UH ayant signé la contremarque de temps.
extensions	Des extensions peuvent être incluses par l'AH, mais aucune ne doit être marquée comme critique.

VIII.2. Certificats et LCR

Les gabarits des certificats d'UH doivent être conformes aux exigences des certificats de type « cachet » dont la clé privée associée est utilisée pour signer des jetons d'horodatage décrites dans les documents [RGS_A_14] et [RGS_A_13]. Il est rappelé ici que :

- l'extension "Extended Key Usage" doit être présente, marquée critique, et ne contenir que l'identifiant id-kp-timeStamping à l'exclusion de toute autre.
- Le champ "DN Subject" doit identifier l'AH suivant les mêmes règles que l'identification des AC (cf. chapitre VII.1 de [RGS_A_14]) et l'identifiant propre à l'UH concernée, au sein de l'AH, doit être porté dans l'attribut commonName du DN de ce champ (au sein d'une AH, chaque UH doit avoir un identifiant unique).
- La durée de vie maximale est bornée selon le couple {durée de vie cryptographique de la clé ; fin de validité de la durée de vie de l'AC émettrice}.

VIII.3. Algorithmes cryptographiques

Les algorithmes et fonctions cryptographiques (hachage, signature) mis en œuvre pour la génération des différents certificats, pour la génération des contremarques de temps ainsi que la valeur du champ messageImprint dans les contremarques de temps doivent respecter les exigences correspondantes de [RGS_A_14].

IX. Annexe 3 : Exigences de sécurité du module d'horodatage des UH

IX.1. Exigences sur les objectifs de sécurité

Le module d'horodatage, utilisé par l'AH pour générer et mettre en œuvre les clés de signature des UH et pour générer les contremarques de temps, doit répondre aux exigences de sécurité suivantes :

- garantir que la génération des bi-clés des UH est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- assurer la confidentialité et l'intégrité des clés privées de signature des UH durant tout leur cycle de vie, et permettre leur destruction sûre en fin de vie ;
- garantir l'authenticité et l'intégrité des clés publiques lors de leur export hors du module (à fins de certification par une AC) ;
- lors de son importation dans le module, vérifier la correspondance entre le certificat importé et la clé publique de l'UH contenue dans le module ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests, lors des phases d'initialisation, de personnalisation et d'opération, pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- être capable de détecter les tentatives d'altérations physiques et d'entrer dans un état sûr quand une tentative d'altération est détectée ;
- permettre de créer une signature numérique, pour signer les contremarques de temps générées par l'UH, qui ne révèle pas les clés privées de l'UH et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- empêcher toute importation / exportation des clés privée de l'UH ;
- garantir la synchronisation de son horloge avec le temps UTC suivant la précision définie dans la DPH ;
- fournir des contremarques de temps conformes aux requêtes reçues

IX.2. Exigences complémentaires

Il est recommandé que le module d'horodatage utilisé par l'AH soit qualifié au niveau standard, selon la procédure précisée dans le [DécretRGS], attestant ainsi de sa conformité aux exigences de sécurité du chapitre IX.1 ci-dessus. Le profil de protection [PP_HORO] couvre ces exigences.

Lorsque le PSHE souhaite faire qualifier son offre d'horodatage, selon la procédure décrite dans le [DécretRGS], les fonctions cryptographiques telles que la génération des bi-clés des UH et la signature des contremarques de temps visées au chapitre IX.1 doivent être assurées par un module cryptographique évalué conformément aux exigences spécifiées aux alinéas 7.2.1.b et 7.2.2.a de la norme [ETSI_PH].

X. Annexe 4 - Vérification ou utilisation (informative)

Cette politique d'horodatage prévoit la vérification d'une contremarque de temps, pendant la période de validité du certificat de clé publique de l'unité d'horodatage qui l'a générée.

X.1. Empilement des contremarques de temps

S'il s'avère nécessaire de prolonger la durée de vie d'une contremarque de temps ou d'en conforter la robustesse, il est possible d'ajouter une contremarque de temps supplémentaire fournie par une autre unité d'horodatage.

Pour cela, il convient de pouvoir prouver que le certificat de l'unité d'horodatage référencé dans la contremarque de temps d'origine n'était pas révoqué au moment où la contremarque de temps supplémentaire a été ajoutée.

Après s'être assuré que l'unité d'horodatage qui a généré la première contremarque de temps n'est pas révoquée, une contremarque de temps supplémentaire sera apposée sur la contremarque précédente le demandeur de la nouvelle contremarque

Les LRC des AC en charge de l'unité d'horodatage devront être archivées afin de pouvoir démontrer que l'unité d'horodatage ayant généré la première contremarque de temps n'était pas révoquée à ce moment là.

Lors d'une vérification ultérieure, un utilisateur de contremarque de temps devra vérifier les deux contremarques de temps et s'assurer que l'unité d'horodatage ayant généré la première contremarque n'était pas révoquée à la date où la seconde contremarque de temps a été apposée. L'utilisateur de contremarque de temps devra en outre s'assurer que le certificat de l'unité d'horodatage ayant généré la seconde contremarque de temps n'est pas révoquée à l'instant de la vérification ultérieure.

X.2. Gestion de la révocation par les Autorités de Certification

La gestion de la révocation des certificats des unités d'horodatage doit être assurée comme pour toute AC.

Un service OCSP ferait l'affaire mais cela multiplierait les contraintes d'implémentation et dans le cas présent, étant donné que le risque de compromission d'une clé est minime, l'usage des LCR est tout à fait adapté.

Il est recommandé de mettre en place une AC spécifiquement en charge de la gestion des unités d'horodatage.

XI. Annexe 5 - Précision de la synchronisation de l'horloge

La précision de l'horloge a souvent été ressentie comme un paramètre essentiel. On peut très facilement obtenir des synchronisations par rapport à une horloge de référence UTC avec une précision de 10 microsecondes, mais cette précision n'a pas de sens dans le cadre de l'horodatage pour deux raisons :

- le temps de transit de la requête est largement supérieur à ce temps ;
- l'opération de signature de la contremarque de temps est largement supérieure à ce chiffre et se situe aujourd'hui au mieux dans l'échelle des 10 millisecondes.

Une précision d'une seconde est largement suffisante pour toutes les applications.

Des précisions meilleures peuvent cependant être utiles dans des contextes de liaisons particulières "courtes" (par exemple, réseaux locaux ou à l'intérieur d'un même système informatique). Cela n'a de sens que si elles sont commensurables avec le temps de propagation et de traitement de la demande. En l'état actuel de la technique, un horodatage bien meilleur que 10 millisecondes n'aurait pas grand sens.

Sans changer de politique, il est possible d'avoir une précision meilleure. Quand c'est le cas, cette précision est indiquée à l'intérieur de la contremarque de temps.

La précision est une propriété intrinsèque de l'unité d'horodatage. Certaines unités d'horodatage peuvent donc fournir des précisions meilleures. En s'adressant directement à une unité d'horodatage donnée, on peut donc obtenir une précision meilleure sans qu'il soit nécessaire de changer de politique d'horodatage et sans qu'il soit nécessaire d'utiliser de paramètre spécifique (le protocole défini dans le [RFC3161] ne comporte pas de paramètre spécifique pour ce faire).

XII. Annexe 6 - Protocole d'horodatage

Aucun protocole spécifique n'est requis, en dehors du format de la contremarque de temps (cf VIII.1.) Si la déclaration des pratiques d'horodatage déclare que le protocole d'horodatage est conforme au [RFC3161] ou au standard [ETSI_TSP], alors les sections suivantes s'appliquent.

XII.1. Conformité au RFC 3161

Cette section s'appuie sur le contenu du RFC 2026 (section 4.1.2) [RFC2026].

L'IETF n'a pas "des clauses de conformités". Au lieu de cela l'IETF stipule des tests d'interopérabilité.

Il est requis de démontrer l'interopérabilité avec au moins une mise en oeuvre indépendante réalisée à partir d'un code de base différent.

L'Autorité d'horodatage doit pouvoir fournir une documentation au sujet des tests d'interopérabilité :

1. le test s'applique à toutes les options et les particularités de la spécification ;
2. la documentation doit inclure l'information concernant le support de chacune des options individuelles et des particularités.

XII.2. Conformité au standard ETSI TS 101 861

La norme [ETSI_TSP] inclut dans sa section 5 un profil pour le format de la réponse et dans sa section 6 un profil pour les protocoles de transport à supporter.

XIII. Annexe 7 - Compatibilité avec la politique d'horodatage de l'ETSI

La présente PH Type définie dans ce document est compatible sur la plupart des points avec la politique d'horodatage définie dans le document [ETSI_PH].

Cependant, les points suivants de la politique [ETSI_PH] ne sont pas repris dans cette politique :

TS 101 023 v1.2.1	**PH standard**	**Texte**	**Justificatif**
5.1		The present document defines requirements for a baseline time-stamp policy for TSAs issuing time-stamp tokens, supported by public key certificates, with an accuracy of 1 second or better.	Cette exigence, qui demande une précision d'au moins une seconde, n'a pas été reprise pour pouvoir prendre en compte des précisions moindres.
7.1.2 d)	7.	The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services. This statement shall at least specify for each time-stamp policy supported by the TSA: […] The expected life-time of the signature used to sign the time-stamp token (depends on the hashing algorithm being used, the signature algorithm being used and the private key length). (la durée de vie estimée de la signature utilisée pour signer la contremarque de temps (dépend de l'algorithme de hachage employé pour la signature, de l'algorithme de signature employé et de la longueur de la clé privée))	Cette exigence, sur l'estimation de la durée de vie de la clé de signature, n'a pas été reprise dans la présente politique du fait du caractère non garanti de l'information. De ce fait, l'estimation n'engage en rien l'AH.
7.2.5.c	11.b	The TST generation system SHALL reject any attempt to issue TSTs if the signing private key has expired. (Le système de génération des contremarques de temps doit rejeter toute tentative de génération d'une contremarque de temps si la fin de la période d'utilisation de la clé privée de l'unité d'horodatage a été atteinte.)	L'obligation de destruction de la clé entraîne de facto l'impossibilité de générer de nouvelles contremarques de temps.

Cette politique d'horodatage a été réalisée dans l'optique de permettre à un opérateur, s'il le désire, de fournir un service compatible à la fois avec la présente PH et avec celle de l'ETSI. Il conviendra toutefois à l'AH de vérifier que les exigences des deux politiques sont respectées pour ce prévaloir de cette compatibilité.

Si la conformité aux exigences de la PH de l'ETSI est réalisée, alors l'identifiant d'objet (OID) défini dans le document de l'ETSI peut donc aussi être utilisé :

{itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy(1)}.