



KEYNECTIS

■ POLITIQUE D'HORODATAGE

K•Stamp®

© 2007-2010. KEYNECTIS. Tous droits réservés.

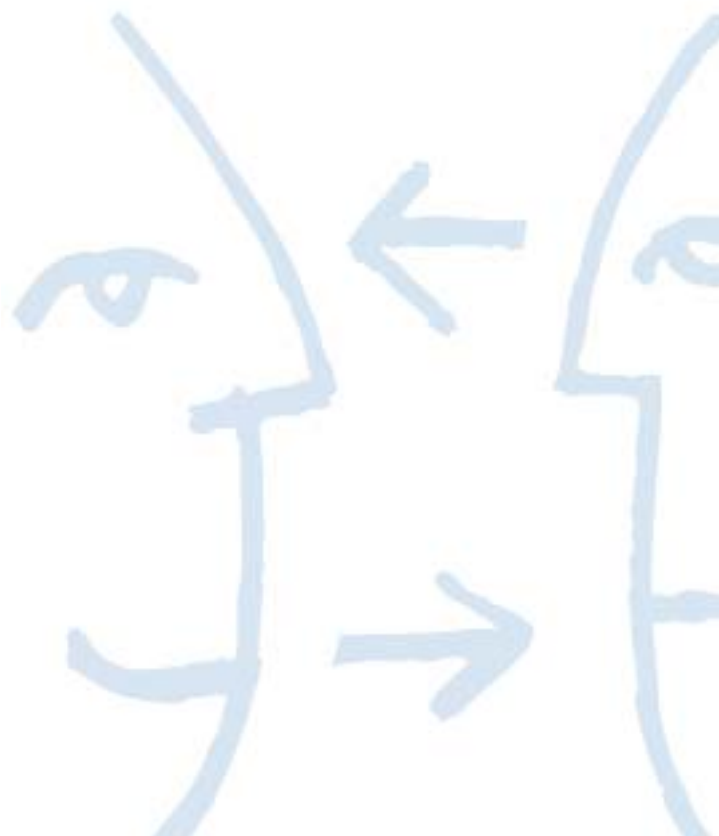
Date :	23 novembre 2009
Référence :	PH/KEY/K.Stamp
OID :	1.3.6.1.4.1.22234.2.6.5.1.1

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

HISTORIQUE DES MODIFICATIONS

Historique du document :


Date	Version	Rédacteur	Commentaires	Statut
05/03/2003	0.1	JYF	Création initiale	Projet
13/06/2003	0.2	JYF	Corrections	Projet
24/05/2007	0.3	EM/JYF/RB/TdV	Intégration des commentaires	Projet
07/06/2007	0.4	JYF/EM/MQ	Commentaires internes	Projet
29/06/2007	0.5	MQ/EM	Mise en forme pour diffusion et commentaires	Projet
01/10/2007	0.6	JYF	Relecture mise en forme	Projet
02/10/2007	1	MQ/JYF	Intégration commentaires	Diffusable
23/11/2009	1.1	MQ	Modification du siège social de KEYNECTIS et remplacement des termes CGU par Contrat	Diffusable



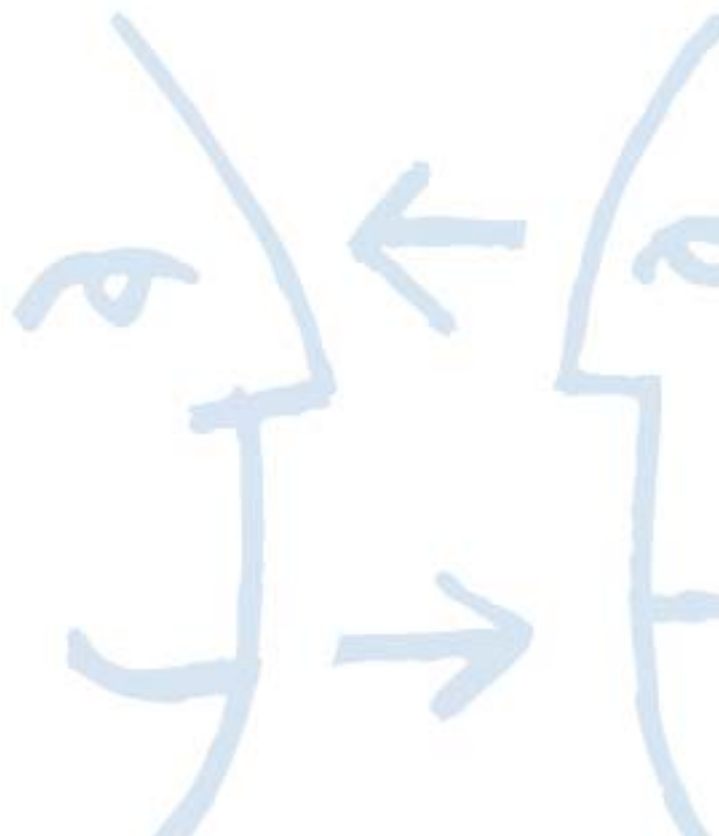



SOMMAIRE

AVERTISSEMENT	5
1 INTRODUCTION	6
1.1 Présentation générale	6
1.2 Identification du document	6
1.3 Gestion de la PH et de la DPH	6
1.3.1 Elaboration de la PH et de la DPH	6
1.3.2 Délai de préavis	7
1.3.3 Forme de diffusion des avis	7
1.3.4 Modifications nécessitant l'adoption d'une nouvelle politique	7
1.3.5 Point de contact	7
1.4 Contrat de service d'horodatage	7
1.5 Qu'est-ce que l'horodatage ?	7
2 GÉNÉRALITÉS	9
2.1 Définitions	9
2.2 Acronymes	10
3 DISPOSITIONS GENERALES	11
3.1 Obligations	11
3.1.1 Obligations de l'Autorité d'horodatage	11
3.1.2 Obligations du Client	11
3.1.3 Obligations de l'utilisateur de contremarques de temps	11
3.1.4 Obligations pour les ACH fournissant les certificats aux unités d'horodatage	12
3.2 Déclarations des pratiques d'horodatage	12
3.3 Contrat de service d'horodatage	12
3.4 Conformité avec les exigences légales	13
3.4.1 Loi applicable et juridictions compétentes	13
3.4.2 Droits de propriété intellectuelle	13
3.4.3 Protection des données à caractère personnel	13
3.5 Limite de responsabilité	13
4 EXIGENCES OPERATIONNELLES	14
4.1 Gestion des requêtes de contremarques de temps	14
4.1.1 Engagements de qualité de service	14
4.1.2 Demande de contremarques de temps	14
4.2 Fichiers d'audit	14
4.2.1 Evènements liés à la mise en œuvre des système d'horodatage	14
4.2.2 Evènements liés à la gestion des clés d'UH	14
4.2.3 Evènements liés à la synchronisation de l'horloge	15
4.3 Gestion de la durée de vie de la clé privée et du certificat d'UH	15
4.4 Synchronisation de l'UH	15
4.5 Exigences du contenu d'une contremarque de temps	16
4.6 Compromission de l'AH	16
4.7 Fin d'activité	16
5 EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES, PROCEDURALES ET ORGANISATIONNELLES	17
5.1 Exigences physiques et environnementales	17
5.2 Exigences procédurales	17
5.2.1 Manipulation et sécurité des supports	18

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

5.2.2	Planification de Système.....	18
5.2.3	Rapport d'incident et réponse	18
5.2.4	Procédures de fonctionnement et responsabilités.....	18
5.2.5	Gestion d'Accès au Système	19
5.2.6	Déploiement et Maintenance	19
5.3	Exigences organisationnelles.....	19
6	EXIGENCES DE SECURITE TECHNIQUES	20
6.1	Exactitude du temps	20
6.2	Génération de bi-clé.....	20
6.3	Certification des bi-clés de l'unité d'horodatage	20
6.4	Protection des clés privées des unités d'horodatage	21
6.5	Installation des clés d'UH.....	21
6.6	Exigences de sauvegarde des clés des unités d'horodatage	22
6.7	Destruction des clés des unités d'horodatage.....	22
6.8	Algorithmes obligatoires	22
6.9	Vérification des contremarques de temps.....	22
6.10	Durée pendant laquelle les contremarques de temps sont vérifiables	22
6.11	Durée de validité des certificats de clé publique des unités d'horodatage	22
6.12	Durée d'utilisation des clés privées des unités d'horodatage.....	23
7	ANNEXE 1 : DOCUMENTS CITES EN REFERENCE	24
7.1	Réglementation.....	24
7.2	Documents techniques	24
8	ANNEXE 2 : FORMATS DES CONTREMARQUES DE TEMPS	25



 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

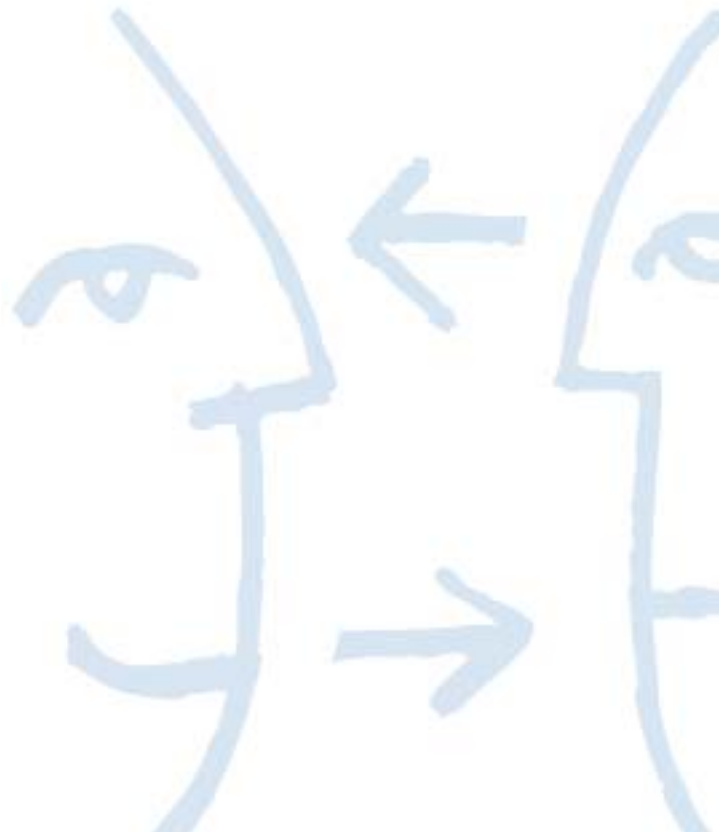
AVERTISSEMENT


La présente politique d'horodatage est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de KEYNECTIS.

La reproduction, la représentation (hormis la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement de manière expresse par KEYNECTIS ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'Article L.122-5, d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (Article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les Articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.



 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

1 INTRODUCTION

1.1 Présentation générale

KEYNECTIS se positionne en tant qu'Autorité d'Horodatage (ci-après « AH ») et délivre des contremarques de temps dans le cadre de ses besoins internes de KEYNECTIS et des besoins des ses clients. Le présent document constitue la politique d'horodatage de KEYNECTIS (ci-après « PH ») pour le service d'horodatage de KEYNECTIS dénommé « Service K.Stamp® ».

Dans le cadre de la présente PH, un client est une entité légale qui soumet ou fait soumettre par sa communauté d'utilisateurs des demandes de contremarques de temps pour ses besoins propres.

Une contremarque de temps permet d'attester de la réalité, à une date et une heure donnée, de l'existence d'une empreinte numérique (ou « hash ») qui est soumise au service d'horodatage de KEYNECTIS. Les contremarques de temps sont délivrées et signées électroniquement par l'AH à l'aide d'Unité(s) d'Horodatage (ci-après « UH »). Cette PH n'impose pas d'exigences sur le lien entre l'empreinte numérique à horodater et le contenu de la donnée électronique qui en est à l'origine.

Dans le cadre de cette PH, la date et le temps de chaque contremarque de temps sont synchronisés avec le temps UTC avec une **précision de 1 seconde**. La présente PH applique un format de contremarque de temps standard défini par le [RFC 3161].

L'objectif de ce document est de définir les engagements que KEYNECTIS, en tant qu'AH, respecte dans la délivrance et la gestion de contremarques de temps, ainsi que les obligations des autres participants.

Le présent document est complété dans sa partie mise en œuvre par une Déclaration des Pratiques d'Horodatage (DPH) et du contrat de service conclu entre Keynectis et le client ayant souscrit au Service K. Stamp® (Contrat).

Une DPH expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la PH, en particulier les processus qu'une UH emploiera pour la création des contremarques de temps et le maintien de l'exactitude de ses horloges. L'AH de KEYNECTIS peut mettre en œuvre plusieurs UH pour supporter son service d'horodatage.

En raison de la confidentialité d'une partie de son contenu, la DPH est un document à diffusion restreinte, il n'est disponible à la consultation qu'aux personnes habilitées à en prendre connaissance. Toute demande de consultation devra être adressée au Comité des politiques de certification et d'horodatage de KEYNECTIS.

La présente PH et la DPH associée sont élaborées sur la base des documents issus de l'ETSI [ETSI_PH] et de la PRIS v2.1 [PRIS_AH].

1.2 Identification du document

La présente PH est dénommée « politique d'horodatage ». Elle est identifiée par un numéro d'identifiant d'objet (OID) dont la valeur est : 1.3.6.1.4.1.22234.2.6.5.1.1.


Le numéro d'OID de cette PH est indiqué à titre de gestion documentaire et pour utilisation dans les contremarques de temps qui sont générés par les UH pour l'AH.

1.3 Gestion de la PH et de la DPH

1.3.1 Elaboration de la PH et de la DPH

La PH et la DPH associée sont rédigées et approuvées par KEYNECTIS.

La DPH qui supporte la présente PH est approuvée par le comité des politiques de certification et d'horodatage de KEYNECTIS auquel toute demande de renseignements est à adresser (Cf. § 1.3.5). Ce comité a entre autres la responsabilité de veiller à la conformité de la DPH avec la présente PH. Ce comité veille également à la complétude du Contrat (voir § 1.4 ci-dessous) au regard du service d'horodatage de KEYNECTIS.

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

1.3.2 Délai de préavis

KEYNECTIS informera les clients du Service K.Stamp® en respectant un préavis de trente (30) jours calendaires avant de procéder à tout changement de la présente politique susceptible de produire un effet majeur sur lesdits clients.

KEYNECTIS informera les clients du Service K.Stamp® en respectant un préavis de quinze (15) jours calendaires avant de procéder à tout changement de la présente politique susceptible de produire un effet mineur sur lesdits clients.

KEYNECTIS peut modifier la présente politique sans préavis lorsque, selon l'évaluation du responsable de la Politique d'horodatage, ces modifications n'ont aucun impact sur eux. Toutefois il informera le client de la nature de la modification.

1.3.3 Forme de diffusion des avis

Dans les cas de modification soumise à préavis, KEYNECTIS avise les clients des modifications apportées à la présente politique d'horodatage gestion de preuves, par tous moyens à sa convenance dont notamment le site web de KEYNECTIS et la messagerie électronique, en fonction de la portée des modifications.

1.3.4 Modifications nécessitant l'adoption d'une nouvelle politique

Si un changement apporté à la présente politique d'horodatage a, selon l'évaluation du responsable de la politique, un impact majeur sur un nombre important de clients, le responsable de la politique peut, à sa discrétion, instituer une nouvelle politique avec un nouvel identificateur d'objet (OID).

1.3.5 Point de contact

Toute demande relative à la présente PH doit être adressée à :

Monsieur Jean-Yves Faurois
 Directeur Qualité & Sécurité de KEYNECTIS
 KEYNECTIS – 11-13 rue René Jacques – 92131 Issy les Moulineaux Cedex
 Téléphone : (33) (0)1.55.64.22.00
 Fax : (33) (0)1.55.64.22.01.

Toute demande de consultation de la DPH de KEYNECTIS devra faire l'objet d'une demande motivée. Cette demande est instruite en tenant compte des éléments de motivation de la demande et la transmission éventuelle aura lieu conformément aux règles de protection de l'information appliquées par KEYNECTIS.

1.4 Contrat de service d'horodatage


La PH de KEYNECTIS est complétée par le Contrat relatif au service d'horodatage fourni par KEYNECTIS. Le Contrat prévoit les conditions d'utilisation du service d'horodatage de KEYNECTIS pour ses clients et leurs communautés d'utilisateurs.

1.5 Qu'est-ce que l'horodatage ?

L'horodatage permet d'attester qu'une donnée électronique existe à une date et une heure donnée. Les date et heure sont garanties par une AH.

En pratique, la personne ou l'entité qui souhaite disposer d'une contremarque de temps transmet une demande de contremarque de temps à l'AH par l'intermédiaire de l'UH après avoir calculé une empreinte numérique de la donnée électronique à horodater. L'AH appose une signature électronique, par l'intermédiaire d'une UH synchronisée par rapport au temps UTC, sur l'empreinte qui lui a été fournie et retourne cette empreinte à la personne ou à l'entité demandeuse.

La signature générée par l'UH lie de manière sûre l'empreinte numérique, et non la donnée électronique elle-même, à la date et l'heure de génération de la contremarque de temps avec une précision donnée par rapport au temps UTC. Cette signature est vérifiable pendant une période qui débute dès la génération de la contremarque de temps et dont la durée est fixée par l'AH dans la présente PH.

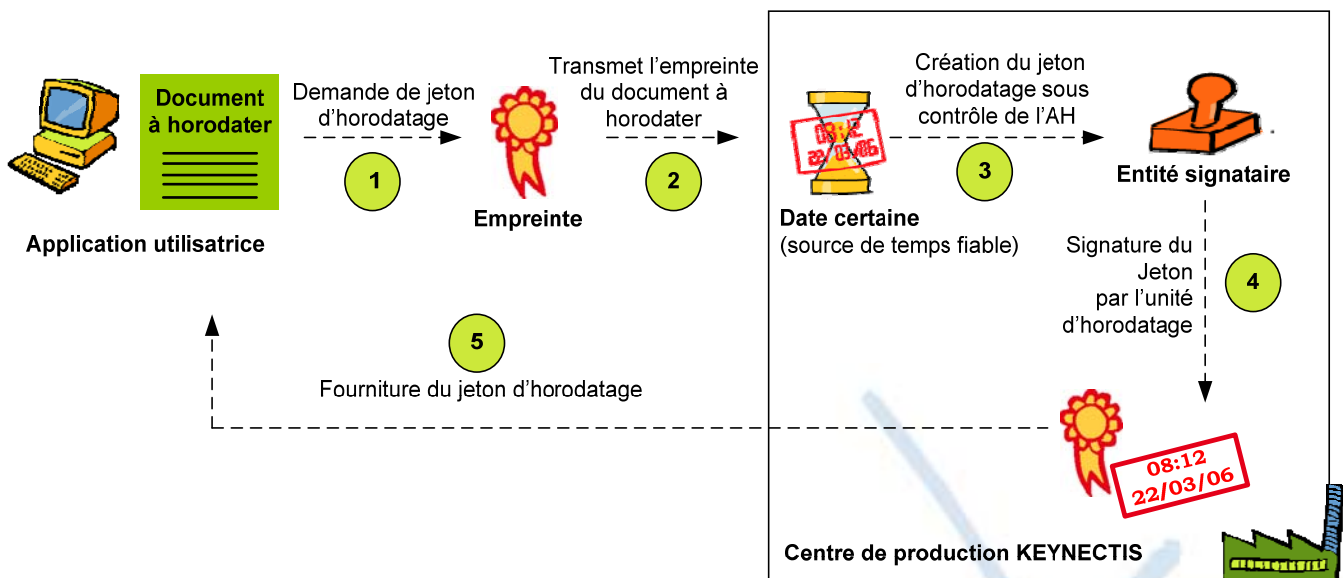
 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1


L'AH tient à disposition des utilisateurs de ses services les informations nécessaires à la vérification de la validité des contremarques de temps, parmi celles-ci les informations relatives aux états de validité des certificats d'horodatage (chaîne de certification, LCR, ...).

Les demandeurs de contremarques de temps qui établissent des demandes de contremarques de temps sont authentifiés par l'AH.

La clé privée ou les clés privées utilisées pour générer les contremarques de temps sont gérées par l'AH conformément aux exigences définies dans sa PH. Une AH peut gérer plusieurs UH. Chaque UH dispose d'une clé de signature. Chaque UH signe les contremarques de temps pour le compte de l'AH à l'aide d'une clé privée dont la clé publique correspondante a été certifiée au préalable par l'autorité de certification (AC) dénommée ACH conformément à [PC_KEYNECTIS_KACH]. Les UH disposent donc de certificats d'UH qui permettent de les identifier.

Le schéma ci-dessous résume la cinématique d'horodatage entre les différents acteurs impliqués dans la génération de contremarques de temps.



 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

2 GÉNÉRALITÉS

2.1 Définitions

Autorité de Certification d'Horodatage (ACH) : désigne une entité qui délivre les certificats électroniques aux UH mises en œuvre par l'AH et rattachées à cette dernière. Cette ACH gère aussi les listes de certificats révoqués pour les certificats d'UH. L'ACH applique la politique de certification (PC) [PC_KEYNECTIS_KACH] pour la gestion des certificats d'UH.

Autorité d'horodatage (AH) : désigne une entité qui a en charge l'application d'au moins une politique d'horodatage en s'appuyant sur une ou plusieurs Unités d'Horodatage. L'AH délivre des contremarques de temps avec une précision donnée et à partir de source de temps choisies.

Calcul d'empreinte numérique : désigne le processus algorithmique qui consiste à obtenir une empreinte numérique à partir d'une donnée électronique.

Client : désigne l'entité ayant contracté avec KEYNECTIS pour bénéficier du service d'horodatage de KEYNECTIS dans le cadre de son activité professionnelle.

Contremarque de temps : désigne la donnée qui lie une empreinte numérique à une date et une heure d'UH. Cette contremarque de temps est signée électroniquement par une unité d'horodatage (UH). Une contremarque de temps permet d'établir la preuve que l'empreinte numérique existe à la date et l'heure qui y figure.

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

Date et heure d'UH : désigne une date et une heure locale qui sont créées par la source de temps interne de l'UH. Cette UH est synchronisée avec une ou des source(s) de temps externe(s) afin de créer une date et une heure avec une précision donnée au regard du temps UTC. Dans le cadre des présentes, la date et l'heure d'UH de KEYNECTIS est la date et l'heure légale française, construite à Paris (France), par le laboratoire UTC(OP)¹.

Déclaration des pratiques d'horodatage (DPH) : désigne les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AH applique, par l'intermédiaire d'une UH, 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.

Demande de contremarque de temps : désigne la requête qui est soumise par un client à l'AH pour l'émission d'une contremarque de temps. Cette requête contient au minimum l'empreinte numérique à horodater.


Données électroniques : désigne un ensemble de données structurées pouvant faire l'objet de traitement informatique par les applications informatiques du Client. Le calcul de l'empreinte numérique est effectué à partir de cet ensemble de données.

Empreinte numérique (ou Hash) : désigne le résultat, d'une fonction de hachage à sens unique, c'est-à-dire d'une fonction calculant une empreinte d'un message de telle sorte qu'une modification même infime du message entraîne la modification de l'empreinte et permet donc de détecter que le message a été modifié.

Jeton d'horodatage : Voir contremarque de temps.

Liste de certificats révoqués (LCR) : désigne la liste signée électroniquement par l'ACH et qui contient l'ensemble des identifiants des certificats d'UH qui ont été révoqués avant leur date d'échéance.

¹ OP pour Observatoire de Paris

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

Politique de Certification (PC) : désigne l'ensemble des règles et engagements énoncées et publiées par l'ACH décrivant les caractéristiques générales des services de certification et des certificats d'UH qu'elle délivre.

Politique d'horodatage (PH) : désigne l'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 clients et les utilisateurs de contremarques de temps.

Précision : désigne la différence maximale autorisée entre la date et l'heure UTC fournie par la source de temps externe et la date et heure (Cf. Date et heure d'UH) de la source interne de l'UH qu'il utilise pour générer les contremarques de temps.

Ressource cryptographique : désigne le produit de sécurité comportant une ressource cryptographique matérielle 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.

Service d'horodatage : désigne l'ensemble des prestations réalisées par KEYNECTIS nécessaires à la génération et le cas échéant à la gestion de contremarques de temps.

Source de temps : désigne la composante qui fournit une date et une heure (temps). On distingue deux sortes de sources de temps :

- La source de temps externe : Source extérieure au système d'information, qui fournit un temps UTC reconnu comme sûr (antenne GPS, onde radio, serveur NTP, ...) ;
- La source de temps interne : Source interne au système d'horodatage, qui fournit un temps (Cf. date et heure UH) sur la base d'éléments uniquement internes au système d'information.

Synchronisation : désigne l'opération qui consiste pour une UH à comparer la date et l'heure issue de sa source de temps interne à la date et l'heure fournie par une ou des source(s) de temps externes. Cette comparaison sert à garantir dans temps que sa source de temps interne délivre une date et une heure avec un écart maximal correspondant à la précision de l'heure l'AH par rapport au temps UTC.

Système d'horodatage : désigne l'ensemble des UH et des composants d'administration et de supervision utilisés pour fournir des services d'horodatage.

Unité d'Horodatage (UH) : désigne l'ensemble de matériels et de logiciels utilisés pour la création de contremarques de temps. L'UH est caractérisée par un identifiant délivré par une AC et une clé unique de signature de contremarques de temps. L'UH construit une date et une heure d'UH qu'elle utilise pour les contremarques de temps qu'elle signe.


Utilisateur de contremarque de temps : désigne l'entité (personne ou système) qui valide une contremarque de temps émise sous une PH et DPH données par une AH donnée afin de s'assurer de l'existence d'une donnée électronique à une date et une heure données.

Vérification d'une contremarque de temps : désigne l'action de l'utilisateur de contremarque de temps qui consiste à vérifier que la contremarque est valide.

2.2 Acronymes

Pour le présent document, les acronymes suivants s'appliquent :

AC	Autorité de Certification
AH	Autorité d'horodatage
DPH	Déclaration des Pratiques d'Horodatage

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

ETSI	European Telecommunications Standards Institute
LCR	Liste des Certificats Révoqués
OID	Object Identifier
PH	Politique d'Horodatage
SGDN/ANSSI	Secrétariat Général de la Défense Nationale / Direction Centrale de la Sécurité des Systèmes d'Information
UH	Unité d'Horodatage
UTC	Coordinated Universal Time

3 DISPOSITIONS GENERALES

3.1 Obligations

3.1.1 Obligations de l'Autorité d'horodatage

Dans le cadre de la présente PH, l'AH :

- Génère et signe les contremarques de temps conformément à la PH et à la DPH de KEYNECTIS, ainsi qu'au Contrat ;
- Respecte et se conforme aux exigences et procédures définies dans la présente PH et la DPH qui la supporte ;
- Garantit la conformité des exigences et des procédures décrites dans sa DPH avec la présente PH ;
- Met à disposition de ses clients l'ensemble des informations nécessaire à vérifier les contremarques de temps qu'elle aura émises, selon les modalités indiquées au paragraphe 6.9 et le cas échéant précisées dans le Contrat ;
- Respecte, les conditions de disponibilité du service d'horodatage convenues contractuellement avec ses Clients ;
- Maintient une information sur la compromission de la bi-clé des UH, même après la date de fin de validité des certificats des UH ;
- Utilise des certificats pour les UH sous sa responsabilité qui sont délivrés par l'ACH dénommée « AC_KEYNECTIS_KH » conformément à la [PC_KEYNECTIS_KACH] ;
- Authentifie les demandes de contremarques de temps à l'aide des certificats déclarés par le Client auprès de l'AH.

3.1.2 Obligations du Client

Dans le cadre de la présente PH, le Client :

- Identifie et habilite les entités qui vont demander des contremarques de temps auprès d'une ou des UH de l'AH ;
- déclare les AC et les certificats que l'AH utilise pour authentifier les entités qui soumettent des demandes de contremarques de temps ;
- Respecte les obligations de la présente PH;
- Indique à l'AH l'algorithme qu'il utilise pour calculer les empreintes numériques des données électroniques qu'il souhaite faire horodater ;
- Vérifie, au moment de l'obtention d'une contremarque de temps, que le certificat de l'UH n'est pas révoqué et qu'il est délivré par l'ACH ;
- Respecte les modalités applicables de la politique de certification de l'AC ayant délivré les certificats utilisés pour s'authentifier lors de la demande de contremarque de temps.

3.1.3 Obligations de l'utilisateur de contremarques de temps

Les utilisateurs de contremarques de temps :

- Vérifient que la contremarque de temps a été correctement signée et que le certificat de l'UH est valide à l'instant de la vérification ;

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

- Tiennent compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la PH.

3.1.4 **Obligations pour les ACH fournissant les certificats aux unités d'horodatage**

L'ACH respecte la [PC_KEYNECTIS_KACH].

L'ACH délivrant des certificats de clés publiques pour les UH fournit un service de révocation mis à jour sur une base quotidienne en employant au moins un mécanisme de publication de LCR.

L'ACH s'engage à conserver pendant au moins 1 an après expiration des certificats des UH, tous les journaux d'événement liés à la délivrance des certificats d'UH.

3.2 **Déclarations des pratiques d'horodatage**


Au titre de ses pratiques d'horodatage, l'AH réalise les actions suivantes :

- Mène une analyse de risques afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles d'émission des contremarques de temps par les UH ;
- Possède une DPH et des procédures associées pour adresser toutes les exigences identifiées dans la présente PH ;
- Identifie, dans la DPH, les obligations des organisations participant à la fourniture des services d'horodatage, y compris la politique et les pratiques applicables. Cela inclut l'ACH fournissant les certificats aux unités d'horodatage ;
- Met à la disposition des utilisateurs de contremarques de temps les éléments publics de sa DPH, s'il y a lieu, et toute autre documentation appropriée ;
- S'assure que les pratiques mentionnées dans la DPH sont correctement mises en œuvre ;
- Définit une procédure de contrôle périodique de la conformité des pratiques mentionnées dans la DPH au regard de la présente PH ;
- Informe préalablement les Clients de tout changement auquel elle a l'intention de procéder dans la partie publique de sa DPH et après mise en place du changement, met immédiatement à la disposition des Clients et des utilisateurs de contremarques de temps la partie publique révisée de la DPH ;
- Si elle est reconnue conforme à un référentiel réglementaire ou technique, comme par exemple le référentiel [ETSI_PH], l'AH s'engage à porter à la connaissance des organismes en charge d'établir cette conformité le contenu de modification apportée.

3.3 **Contrat de service d'horodatage**

Des conditions d'utilisation complémentaires du Service d'horodatage K.Stamp® sont déterminées plus précisément dans le Contrat conclu entre l'AH et chacun de ses clients et comprennent au moins les éléments suivant:

- La référence de la PH appliquée (OID) ;
- Les conditions d'accès et de disponibilité du service ;
- La période de temps, hors cas de révocation de certificat d'UH, durant laquelle les contremarques de temps seront vérifiables ;
- L'exactitude du temps utilisé dans les contremarques de temps par rapport au temps UTC ;
- Toute limitation s'appliquant à l'utilisation du service d'horodatage ;
- Les obligations des Clients et des utilisateurs ;
- L'information sur la manière de vérifier les contremarques de temps de telle façon que l'utilisateur de contremarques de temps puisse faire confiance aux contremarques de temps (voir § 6.9 ci-dessous) ;
- La période de temps pendant laquelle les fichiers d'audit de l'AH sont conservés (voir § 4.2 ci-dessous) ;
- Les limitations de responsabilité de l'AH ;
- Les procédures prévues pour le règlement des différends et des litiges ;
- L'identification du droit applicable ;
- Le nom du pays dans lequel l'Autorité d'horodatage a son siège social et l'identifiant de l'Autorité d'horodatage (tel que figurant dans le certificat de l'unité d'horodatage).

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

3.4 Conformité avec les exigences légales

L'AH a mis en place et maintient au sein des ses composantes et systèmes des mesures techniques et organisationnelles 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 ; et ce afin d'assurer que les informations personnelles des clients et leurs UF ne sont pas divulguées, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.

3.4.1 Loi applicable et juridictions compétentes

Les dispositions de la Politique d'horodatage sont régies par le droit français.

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente Politique, et faute de parvenir à un accord amiable, tout différend sera porté devant les tribunaux compétents de Paris.

3.4.2 Droits de propriété intellectuelle

Tous les droits de propriété intellectuelle relatifs au Service K.Stamp® détenus par KEYNECTIS et ses fournisseurs sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, ...etc.) est sanctionnée par les articles L 716-1 et suivants du Code de la propriété intellectuelle.

3.4.3 Protection des données à caractère personnel

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique au contenu de toutes les données collectés, détenues ou transmises par le Client et/ou l'Utilisateur dans le cadre du Service K.Stamp®.

En vertu des articles 323-1 à 323-7 du Code pénal applicable lorsqu'une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc. Les peines encourues varient de 1 à 3 ans d'emprisonnements assortis d'une amende allant de 15.000 à 225.000 euros pour les personnes morales.

3.5 Limite de responsabilité

La présente PH ne traite que le cas de la vérification des contremarques de temps pendant la période de validité du certificat de l'UH émettrice des contremarques de temps. La vérification en dehors de la période de validité d'un certificat d'UH n'est pas prise en compte dans le cadre de la présente PH.

L'AH n'est pas responsable de la conservation des contremarques de temps.

De même, le Client et les utilisateurs de contremarques de temps sont responsable de leurs politiques d'utilisation de contremarques de temps émises par l'AH, de la vérification de l'état de validité et de la conservation éventuelle des données électroniques et des contremarques de temps associées.


En cas de perte d'une contremarque de temps, le Client ne peut pas demander à l'AH de lui fournir de nouveau la contremarque de temps perdue.

Seul le Client ne peut rechercher la responsabilité de KEYNECTIS au titre du service d'horodatage.

En aucun cas, KEYNECTIS ne sera responsable des dommages indirects ou consécutifs subi par l'Utilisateur serait victime, ceux-ci n'étant en aucun cas préqualifiés par avance par les présentes.

La responsabilité de KEYNECTIS ne saurait être engagée en cas de force majeure, ou de faits qui échappent raisonnablement à son contrôle.

Dans le cas où la responsabilité de KEYNECTIS serait retenue, il est expressément convenu que KEYNECTIS ne serait tenu à réparation que du dommage direct certain et immédiat, dans la limite d'un montant qui ne saurait excéder le montant précisé dans le contrat conclu avec le Client.

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

4 EXIGENCES OPERATIONNELLES

4.1 Gestion des requêtes de contremarques de temps

4.1.1 Engagements de qualité de service

Les engagements de qualité de service relatifs à la fourniture d'une contremarque de temps en réponse à une demande sont définis dans le contrat conclu entre le Client et KEYNECTIS.

4.1.2 Demande de contremarques de temps

Les demandes de contremarques de temps sont réalisées par les UF de l'AH selon le protocole défini par le [RFC 3161]. Ce protocole est conforme à [ETSI_TSP].

Les UF et l'AH s'authentifient mutuellement au préalable de toute transmission de demande de contremarque de temps. Seules les UF de l'AH peuvent s'authentifier et demander des contremarques de temps.

La communication établie garantit l'intégrité et la confidentialité de la demande.

Lorsque l'authentification est positive, l'AH génère la contremarque de temps à partir des données qui lui sont transmises par l'UF et lui retourne.

L'AH ne conserve pas la contremarque de temps générée.

4.2 Fichiers d'audit

Les journaux d'évènements relatifs au du service d'horodatage sont régulièrement enregistrés puis archivés par l'AH et conservés pendant une période de temps précisée dans la DPH notamment dans le but de fournir des éléments de preuve en cas de litige ou en cas d'enquête judiciaire. Toute demande en ce sens est à adresser au service juridique de KEYNECTIS.

Une datation sera fournie pour chacun de ces évènements, ainsi que l'identification de l'entité ayant déclenché ou réalisé l'évènement, ainsi que et le résultat obtenu.

Les informations enregistrées et archivées sont conservées dans des conditions de nature à en assurer la confidentialité et l'intégrité.

La durée garantie de conservation de ces informations est de :

- Au moins 1 an après la fin de période pendant laquelle une contremarque de temps est vérifiable, pour tout évènement lié à la gestion du cycle de vie des contremarques de temps,
- Au moins 1 an après expiration des certificats d'UH, pour tout évènement lié à la gestion du cycle de vie des certificats d'UH et de leurs clés privées.

La liste détaillée des évènements est précisée dans la DPH.

Les évènements sont 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.

Toute information enregistrée au sujet d'un Client est tenue confidentielle sauf lorsqu'un accord est passé avec le Client pour une publication plus large.

4.2.1 Evènements liés à la mise en œuvre des système d'horodatage

Font l'objet de cette collecte d'information les informations suivantes :

- Tous les évènements liés à la mise en œuvre des moyens sur lesquels l'AH de KEYNECTIS s'appuie pour générer et délivrer les contremarques de temps, depuis leur mise en marche jusqu'à leur arrêt définitif ;
- Tous les évènements liés au traitement des demandes de contremarques de temps.

4.2.2 Evènements liés à la gestion des clés d'UH

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

Les enregistrements concernant tous les événements touchant au cycle de vie des clés d'UH sont effectués.

Les enregistrements concernant tous les événements touchant au cycle de vie des certificats des UH sont effectués.

4.2.3 Evènements liés à la synchronisation de l'horloge

Les enregistrements concernant tous les événements touchant à la synchronisation de l'horloge des UH sont effectués. Cela inclut l'information concernant des synchronisations normales et des synchronisations suites à une détection de perte de précision de l'UH.

Les enregistrements concernant tous les événements touchant à la détection de perte de synchronisation sont effectués.

4.3 Gestion de la durée de vie de la clé privée et du certificat d'UH

La durée de vie des clés privées d'UH et des certificats d'UH est fixée en accord avec les recommandations faites par les autorités nationales compétentes en la matière, comme par exemple celles issues du SGDN/ANSSI et précisées dans le document [ANSSI_ALGO].

Les clés privées d'UH sont des éléments sensibles qui font l'objet d'un suivi unitaire de la part de l'AH et bénéficient de mesures de protection particulière afin de les protéger de toute compromission pendant l'ensemble de leur cycle de vie.

Les dates de validité des certificats d'UH sont clairement indiquées dans les certificats d'UH et font l'objet d'une attention particulière de l'AH. Un certificat d'UH reste valide au-delà de la durée d'utilisation opérationnelle de la clé privée associée à la clé publique qu'il certifie.

La période d'utilisation opérationnelle des clés privées d'UH est plus courte que celle du certificat de sa clé publique associée. L'AH de KEYNECTIS procède au renouvellement des clés privées d'UH dans le mois précédent la fin de leur utilisation opérationnelle. Lorsqu'une nouvelle clé privée d'UH est générée, un nouveau certificat d'UH est demandé à l'ACH.


Les clés privées d'UH sont détruites dès que la fin d'utilisation opérationnelle de cette clé privée a été atteinte.

4.4 Synchronisation de l'UH

Pour maintenir la précision et la synchronisation de ses horloges, l'AH de KEYNECTIS :

- Utilise une ou plusieurs sources de temps synchronisée(s) avec le temps UTC pour s'assurer qu'aucune dérive n'est à même de faire varier la précision des horloges des UH au delà d'1s (une seconde),
- Synchronise uniquement ses horloges avec une ou des source(s) de temps externe(s) identifiée(s) dans sa DPH ;
- S'assure de la sécurité des communications entre la source de temps interne et la ou les source(s) de temps externe(s) ;
- S'assure que le mécanisme de synchronisation, qui garanti la précision déclarée, n'altère pas le temps UTC fourni par la ou les sources de temps externe(s) ;
- Protège les horloges des UH contre les menaces relatives à leur environnement qui pourraient aboutir à une désynchronisation avec le temps UTC en dehors de la précision déclarée.

Dans la mesure où un événement de nature à ne plus permettre à l'AH de KEYNECTIS d'assurer une précision de 1s aux horloges de ses UH, un mécanisme d'information des utilisateurs est alors mis en œuvre et la fourniture de contremarques de temps est interrompue. L'AH de KEYNECTIS s'engage à ce que la mise à disposition de contremarques de temps ne puisse reprendre que lorsque la précision de ses horloges aura été restaurée. De même, les utilisateurs des services d'horodatage de l'AH de KEYNECTIS seront informés de la reprise de service.

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

L'AH garantit que la synchronisation de la source interne est maintenue lorsqu'un saut de seconde est programmé comme notifié par l'organisme approprié. Le changement pour tenir compte du saut de seconde est 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 est effectué.

Les conditions détaillées de synchronisation par rapport au temps UTC et de maintien de la précision des horloges de l'AH de KEYNECTIS sont détaillées dans la DPH qui supporte la présente politique d'horodatage.

4.5 Exigences du contenu d'une contremarque de temps

Les contremarques incluent une date et une heure d'UH avec une précision donnée au regard du temps UTC.

Les contremarques de temps sont conformes au [RFC 3161] et leur contenu est décrit au § 8 ci-dessous. Les champs d'une contremarque de temps incluent au moins les informations suivantes :

- Le numéro de version selon laquelle elle a été générée, à savoir V1 ;
- L'identifiant du certificat de l'unité d'horodatage qui génère les contremarques de temps ;
- L'identifiant de la politique d'horodatage ;
- Un identifiant unique pour chaque Contremarque de temps (numéro de série) ;
- L'heure de génération de la contremarque de temps ;
- La précision de synchronisation par rapport au temps UTC ;
- Une représentation de la donnée électronique à horodater (c'est-à-dire la valeur de hachage et l'identifiant d'algorithme de hachage) telle que fournie par l'Application cliente ;
- Le champ "NONCE" identique à celui présenté dans la demande de génération de Contremarque de temps, si celui-ci est présent dans la demande de génération.

Les contremarques de temps ne comportent pas d'extension. Dans tous les cas, seules les extensions définies dans [RFC 3161] seront incluses dans une contremarque de temps.

Pour rappel, les certificats d'UH incluent :

- L'identifiant du pays dans lequel l'Autorité d'horodatage est établie ;
- L'identifiant de l'Autorité d'horodatage de KEYNECTIS.

4.6 Compromission de l'AH

L'AH informe les clients et les utilisateurs de contremarques de temps des d'événements qui affectent la sécurité des services d'horodatage, incluant la compromission de la clé privée de signature d'une unité d'horodatage.

Le plan de secours développé par l'AH traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une UH.

Dans le cas d'une compromission, réelle ou suspectée, la génération de contremarques de temps à l'aide de l'UH en question est arrêtée. La reprise de la génération de contremarques de temps par cette UH ne sera autorisée que lorsque l'ensemble des conditions normales d'exploitation sera restauré.

En cas d'un évènement majeur dans le fonctionnement de l'AH qui affecte des contremarques de temps émises, l'AH met à la disposition de ces clients les informations permettant d'identifier les contremarques de temps qui pourraient avoir été affectées ou une liste des contremarques de temps qui ne sont pas affectées, à moins que cela ne contrevienne au respect des règles de protection de la vie privée des abonnés ou à la sécurité des services d'horodatage. Des détails sur les moyens prévus par l'AH sont donnés dans le DPH.

4.7 Fin d'activité

L'AH de KEYNECTIS s'engage à informer ses clients et les utilisateurs de contremarques de temps, avec un préavis d'au moins 3 (trois) mois, de sa décision d'arrêter ses activités de délivrance de services d'horodatage.

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

Avant que l'AH ne mette fin à ses services d'horodatage l'AH :

- Met fin aux éventuelles autorisations données à des sous-traitants dans l'exécution d'une des fonctions relatives au processus de génération des contremarques de temps ;
- Transfère à une entité qu'elle désigne ses obligations de maintien des fichiers d'audit et des archives nécessaires à démontrer son fonctionnement correct pour assurer le respect des modalités prévues au § 4.2 ci-dessus, si elle ne les maintient pas elle-même;
- Transfère à une entité qu'elle désigne ses obligations de rendre disponible aux utilisateurs de contremarques de temps ses clés publiques ainsi que ses certificats d'UH pour assurer le respect des modalités prévues au § 4.2 ci-dessus, si elle ne les maintient pas elle-même ;
- Demande à l'ACH la révocation de ses certificats d'UH dès la dernière contremarque de temps émise ;
- Détruit les clés privées des UH de telle façon que ces clés ne puissent pas être recouvrées.

L'AH indique dans sa DPH les dispositions précises prises pour assurer la fin du service d'horodatage.

5 EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES, PROCEDURALES ET ORGANISATIONNELLES

5.1 Exigences physiques et environnementales

L'ensemble des opérations de génération et de délivrance des contremarques de temps par l'AH de KEYNECTIS au titre de la présente Politique d'horodatage sont réalisées au sein des locaux sécurisés de KEYNECTIS, par des personnels habilités de KEYNECTIS.

En particulier :

- L'accès physique aux équipements concernés par les services d'horodatage est limité aux personnels autorisés ;
- Des moyens de prévention et des contrôles sont mis en oeuvre pour éviter la perte, des dégâts ou la compromission de bien sensibles et l'interruption des activités ;
- Des moyens de préventions et des contrôles sont mis en oeuvre pour éviter la compromission ou le vol d'informations ou d'équipements informatiques ;
- les installations d'infrastructures sont bâties, installées et mise en œuvre de telle manière que les systèmes se voient fournir les informations et éléments nécessaires à leur bon fonctionnement dans le respect les conditions d'engagement de service de l'AH de KEYNECTIS.


La politique de sécurité physique et environnementale de l'AH pour les systèmes concernés par la gestion de l'horodatage concerne au minimum 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 inondations ou suintement, la protection contre le vol, la casse et l'intrusion. En outre le maintien et le rétablissement de la sécurité après un désastre fait l'objet d'une attention particulière.

5.2 Exigences procédurales

L'ensemble des opérations menées par l'AH de KEYNECTIS pour générer et délivrer des contremarques de temps sont soumises au respect de la politique de sécurité de KEYNECTIS, ainsi que de l'ensemble des politiques et procédures qui s'y rattachent.

En particulier, font l'objet d'une attention toute particulière pendant toute la durée de vie des contremarques de temps et des UH :

- Les informations et supports d'informations nécessaires à la bonne conduite des opérations de l'AH de KEYNECTIS ;

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

- Les informations confiées à l'AH de KEYNECTIS à des fins de délivrance de ses services d'horodatage, notamment les informations à caractère personnel ;
- La mise en œuvre des matériels nécessaires à la conduite des opérations d'horodatage ;
- Les personnels en charge de la conduite des opérations d'horodatage.

L'AH de KEYNECTIS a dans cette optique adopté une organisation avec séparation des rôles du même type que celle mise en œuvre par KEYNECTIS dans la délivrance de services de certification.

Le comité des politiques de certification et d'horodatage de KEYNECTIS est supporté par une entité interne d'audit afin de vérifier la bonne application des pratiques d'horodatage supportant la présente politique. Cette entité d'audit a notamment pour rôle d'identifier toute information de nature à mettre en évidence les non-conformités éventuelles et les événements de sécurité, ainsi que de faire procéder aux vérifications nécessaires et corrections éventuelles.

En complément de ces mesures et afin d'assurer un fonctionnement cohérent, sûr et auditable de l'AH de KEYNECTIS, celle-ci s'engage à ce que soient formalisées et respectées les règles internes relatives à :

- La mise en place, le fonctionnement et la maintenance des systèmes ;
- La protection et le service des systèmes ;
- La prise en compte des incidents et la mise en œuvre des mesures nécessaires à en limiter les impacts sur le service d'horodatage ;
- La traçabilité des événements ;
- Les rôles et responsabilités des personnes en charge des opérations ;
- La mise en œuvre et le contrôle d'accès aux systèmes et installations.

5.2.1 Manipulation et sécurité des supports

Les supports d'information utilisés dans le cadre de la délivrance du service d'horodatage de l'AH de KEYNECTIS dont l'objet d'un suivi qui tient notamment compte du niveau de sensibilité des informations qu'ils renferment.

Le cycle de vie des supports contenant des informations sensibles fait l'objet est soumis au respect de principes et procédures qui sont précisés dans la DPH. Seuls les personnels habilités de KEYNECTIS est dûment affectés aux rôles de confiance du service d'horodatage ont accès à ces supports, selon le besoin d'en connaître.

5.2.2 Planification de Système

Les charges sont contrôlées et des projections de charge dans le futur sont effectuées pour garantir que des puissances de traitement nécessaires, les stockages adéquats et les engagements de services sont disponibles et atteints.

5.2.3 Rapport d'incident et réponse

Le traitement des incidents est assuré au sein de l'AH de KEYNECTIS par une entité spécialisée dont le rôle est de centraliser la prise en compte, le suivi des incidents et la communication auprès des entités concernées.

Chaque incident est clairement identifié, est affecté à une entité de l'AH et fait l'objet d'une fiche de suivi. En fin de traitement, l'incident est clos si la vérification est faite que les systèmes d'horodatage sont revenus dans une configuration normale de fonctionnement.


dans Les interventions correctives sur les systèmes d'horodatage font également l'objet de fiches de traitement. Les détails du processus de traitement des incidents sont précisés dans le DPH.

5.2.4 Procédures de fonctionnement et responsabilités

Les opérations de sécurité sont séparées des autres opérations.

Les opérations de sécurité incluent :

- Les procédures opérationnelles et les responsabilités ;

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

- La planification et la qualification des systèmes sécurisés ;
- La protection vis-à-vis des codes logiciels malveillants ;
- 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 sont gérées par du personnel habilité et dûment désigné de l'AH, selon les règles relatives au partage des rôles et des responsabilités au sein de KEYNECTIS.

5.2.5 Gestion d'Accès au Système

Seuls les personnels habilités et dûment désigné de KEYNECTIS ont accès aux systèmes d'horodatage. Les accès sont donnés au regard des rôles qui leurs sont confiés.

L'accès aux fonctions du système, à l'information et aux applications est limité conformément à la politique de contrôle d'accès. Les systèmes d'horodatage possèdent des contrôles informatiques de sécurité qui permettent la mise en œuvre de la séparation des rôles de confiance identifiés, y compris la séparation des fonctions de responsable de sécurité et des fonctions de mise en œuvre opérationnelle. En particulier, l'utilisation de programmes systèmes utilitaires est limitée et très contrôlée.

Le personnel de l'AH est identifié et authentifié avant de pouvoir utiliser des applications critiques liées à l'horodatage. Le personnel de l'AH est tenu responsable de ses activités et est soumis au règlement intérieur de KEYNECTIS.

Une surveillance des équipements de sécurité est maintenue pour permettre à l'AH de détecter, d'enregistrer et de réagir rapidement à n'importe quelle tentative non autorisée et/ou irrégulière d'accès à ses ressources.

5.2.6 Déploiement et Maintenance

Le déploiement des systèmes d'horodatage est contrôlé et fait l'objet d'enregistrement et fiches. Une politique de gestion de la configuration et des changements s'applique aux systèmes d'horodatage.

Les détails des principes et procédures appliqués sont donnés dans la DPH.


5.3 Exigences organisationnelles

Afin de garantir le bon fonctionnement et la sécurité de ses opérations, l'AH de KEYNECTIS met en œuvre une politique d'habilitation des personnels impliqués dans la réalisation des tâches de définition, création, installation, administration, support et maintenance, audit, application et gestion de la sécurité, liées au fonctionnement des UH. Cette politique se traduit notamment par le respect d'une politique d'habilitation des personnels de KEYNECTIS aux rôles de confiance.

La mise en place de profils de personnels pour les rôles de confiance, de principes de répartition des rôles et responsabilités, ainsi que du double contrôle complète ce dispositif. Les politiques et procédures opérationnelles permettent non seulement de définir les principes applicables, mais aussi de détailler les rôles et opérations de chacun dans la délivrance des services d'horodatage.

L'AH emploie un personnel qui possède l'expertise, l'expérience et les qualifications nécessaires pour les services offerts. Le personnel applique la PH et la DPH, pour les parties qui le concerne, conformément à la politique de sécurité de l'AH.

Les rôles de confiance et les responsabilités, comme spécifié dans la politique de sécurité de l'AH, sont documentés dans des descriptions de poste. Les rôles de confiance, sur lesquels la sécurité du fonctionnement de l'AH repose, sont clairement identifiés. Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes :

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

- Les responsables de la sécurité : responsabilité complète d'administrer la mise en oeuvre des pratiques de sécurité ;
- Les personnels d'administration : autorisés à installer, configurer et maintenir les modules d'horodatage de l'AH pour la gestion de l'horodatage ;
- Les personnels d'exploitation : responsables pour faire fonctionner les modules d'horodatage de l'AH de manière quotidienne. Autorisés pour effectuer les opérations de sauvegarde et des secours ;
- Les personnels contrôleurs : autorisés à consulter les archives et les fichiers d'audit des modules d'horodatage.

Le personnel de l'AH est formellement nommé aux rôles de confiance par la direction responsable de la sécurité au sein de l'AH.

L'AH ne nomme pas aux rôles de confiance ou de gestion une personne connue pour avoir une condamnation pour un crime sérieux ou une autre infraction qui affecte son adéquation avec la position. Le personnel n'a pas accès aux fonctions de confiance avant que les contrôles nécessaires ne soient achevés par l'AH.

6 EXIGENCES DE SECURITE TECHNIQUES

6.1 Exactitude du temps

L'exactitude de temps de l'autorité d'horodatage de KEYNECTIS est de 1s (une seconde) par rapport au temps UTC. La précision des UH est assurée par la source de temps interne, le mécanisme de synchronisation et la ou les source(s) de temps externe(s).

La synchronisation de l'UH est effectuée selon un processus mis en œuvre par des personnels habilités de KEYNECTIS dûment affectés à cette tâche. Des précisions quant aux modalités de la synchronisation sont fournies dans la DPH.

L'initialisation de la synchronisation des UH garanti que la source de temps interne des UH :

- Délivrent une date et une heure avec la précision de 1 seconde au regard de la ou des source(s) de temps externes ;
- Est uniquement synchronisée par rapport à la ou aux source(s) de temps externe(s) précisées dans la DPH.

6.2 Génération de bi-clé

La génération des bi-clés cryptographiques des UH est réalisée à l'aide de ressources cryptographiques matérielles. A aucun moment, lors de cette génération, les clés privées d'UH ne sont exportées de ces ressources.

La génération de bi-clés est effectuée par des personnels habilités de KEYNECTIS et dûment affectés à cette tâche, dans des zones dédiées, sous double contrôle et enregistrement vidéo.

Les personnels admis lors de ces cérémonies disposent tous du besoin d'en connaître.

Les clés privées d'UH ont une longueur de 2048 bits pour l'algorithme RSA. Cette longueur est fixée en accord avec les recommandations faites par les autorités nationales compétentes en la matière, comme par exemple celles issues du SGDN/ANSSI et précisées dans le document [ANSSI_ALGO]. Elle pourra être revue si les recommandations faites sont amenées à évoluer.

6.3 Certification des bi-clés de l'unité d'horodatage

L'AH est à l'origine des demandes de certificat d'UH. L'AH permet à l'ACH de vérifier que la demande de certificat pour l'UH est valide, en lui fournissant notamment les informations et documents nécessaires lors de l'enregistrement. Sont notamment fournies les informations suivantes :

- Un identifiant de l'AH : le nom (DN) de l'unité d'horodatage pour laquelle la demande de certificat est faite ;

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

- La valeur de la clé publique (et l'identifiant de l'algorithme) à certifier ;
- La durée d'utilisation souhaitée pour la clé privée (1 an pour les clés privées de UH de l'AH de KEYNECTIS) ;
- Un identifiant du pays dans lequel l'AH est établie (FR pour l'AH de KEYNECTIS) ;
- Une identification de l'unité d'horodatage qui génère les contremarques de temps.

Les certificats d'UH, conformément à la PC de l'ACH [PC_KEYNECTIS_KACH] identifient :

- L'ACH émettrice ;
- L'AH et l'UH. Au sein de l'AH, l'UH a un identifiant unique.

Les certificats d'UH, conformément à la PC de l'ACH, contiennent les extensions suivantes :

- "Key Usage" ;
- "Extended Key Usage" qui ne contient que l'identifiant `id-kp-timeStamping` ;

L'AH respecte les obligations qui lui incombent et qui découlent de la politique de certification de l'ACH.

L'AH vérifie, lors de l'import des certificats d'UH, qu'ils proviennent de l'ACH auprès de laquelle la demande de certificat a été effectuée.

L'AH ne rend opérationnelle l'UH qu'une fois que l'ensemble des exigences liées à la gestion de la bi-clé de l'UH et à la synchronisation sont remplies.

6.4 Protection des clés privées des unités d'horodatage

Les clés de signature des unités d'horodatage sont en permanence supportées par des ressources cryptographiques matérielles qui ont fait l'objet d'une évaluation et d'une certification selon les standards FIPS 140 – 2 au niveau 3 et/ou les Critères Communs au niveau EAL 4+.

Les clés privées des UH font l'objet d'un suivi unitaire pendant toute la durée de leur vie.

Les supports des clés privées d'UH sont positionnés dans des lieux et opérés dans des systèmes dont les accès physique et logique sont contrôlés et protégés.

La détention seule du support des clés privées ne constitue en aucun cas une preuve de détention des clés privées des UH.

6.5 Installation des clés d'UH

Les clés des UH sont générées soit en zone dédiée puis transférées sous surveillance en zone d'exploitation des UH pour activation. Si elles ne sont pas mises en exploitation immédiatement après leur génération, ces clés sont stockées en zone de stockage sécurisé selon des mesures de sécurité au moins équivalentes à celles dont elles bénéficient lors de leur utilisation en zone d'exploitation.

Les clés d'UH ne peuvent être installées sur d'autres moyens que des ressources cryptographiques matérielles (voir § 6.4 ci-dessus).

Les composants accessibles de l'AH sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu (sauf lors des interventions de maintenance ou de sauvegarde).

Les autres composants de l'AH, dont les ressources cryptographiques renfermant les clés privées des UH, font l'objet de mesures de sécurité pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de gardes, de pare-feu et de routeurs filtrants. Les ports et services réseau non utilisés sont coupés. Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système d'horodatage est hébergé refuse tout service, hormis ceux qui sont nécessaires au service d'horodatage.

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

6.6 Exigences de sauvegarde des clés des unités d'horodatage

Aucune copie des clés privées d'UH n'est réalisée par l'Autorité d'horodatage de KEYNECTIS.

6.7 Destruction des clés des unités d'horodatage

Les clés privées des UH de l'AH de KEYNECTIS sont détruites dès lors qu'elles ont dépassé leur fin de période d'utilisation opérationnelle, afin qu'elles ne puissent être recouvrées et employées au delà.

6.8 Algorithmes obligatoires

L'AH, dans la limite des algorithmes qu'elle reconnaît :

- Accepte des valeurs de hachage générées par des clients et employant les algorithmes de hachage conformes aux exigences des autorités compétentes en la matière comme par exemple [ANSSI_ALGO]. Les algorithmes de calcul d'empreinte numérique acceptés sont SHA 1 et SHA 2 ;
- Génère des contremarques de temps signées selon les algorithmes et les longueurs de clé conformes aux exigences des autorités compétentes en la matière comme par exemple [ANSSI_ALGO]. La bi-clé de l'UH est au minimum une bi-clé RSA de 2048 bits.

6.9 Vérification des contremarques de temps

L'AH tient à disposition des clients les informations nécessaires à la vérification de la signature électronique des contremarques de temps. L'ensemble des informations et les moyens de leurs mise à disposition par l'AH seront précisés dans la DPH.

La vérification d'une signature électronique de contremarque de temps consiste en les opérations suivantes :

- Vérification du calcul de la contremarque de temps ;
- Vérification et extraction de la date et de l'heure contenues dans la contremarque de temps ;
- Identification et extraction du certificat de l'UH ayant émis la contremarque de temps ;
- Vérification que la date à laquelle la contremarque de temps a été émise est comprise dans la période de validité du certificat de l'UH ayant émis la contremarque de temps ;
- Vérification de l'état de validité du certificat de l'UH ayant émis la contremarque de temps au moment de la génération de la contremarque de temps ;
- Vérification que la date indiquée par l'AH dans la contremarque de temps est antérieure à la révocation éventuelle du certificat d'UH ayant émis la contremarque de temps.

Si l'ensemble de ces opérations est positif, alors la contremarque de temps est considérée comme valide.

6.10 Durée pendant laquelle les contremarques de temps sont vérifiables

Les contremarques de temps émises par l'AH de KEYNECTIS sont vérifiables pendant une durée fixée à 10 ans à compter de leur émission.

Cette durée est fixée en accord avec les recommandations faites par les autorités nationales compétentes en la matière, comme par exemple celles issues du SGDN/ANSSI et précisées dans le document [ANSSI_ALGO]. Elle pourra être revue si les recommandations faites sont amenées à évoluer.

6.11 Durée de validité des certificats de clé publique des unités d'horodatage

La durée de validité des certificats d'UH est égale à 11 ans.

Cette durée de validité pourra être revue si les recommandations des autorités nationales compétentes sont amenées à évoluer.

 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

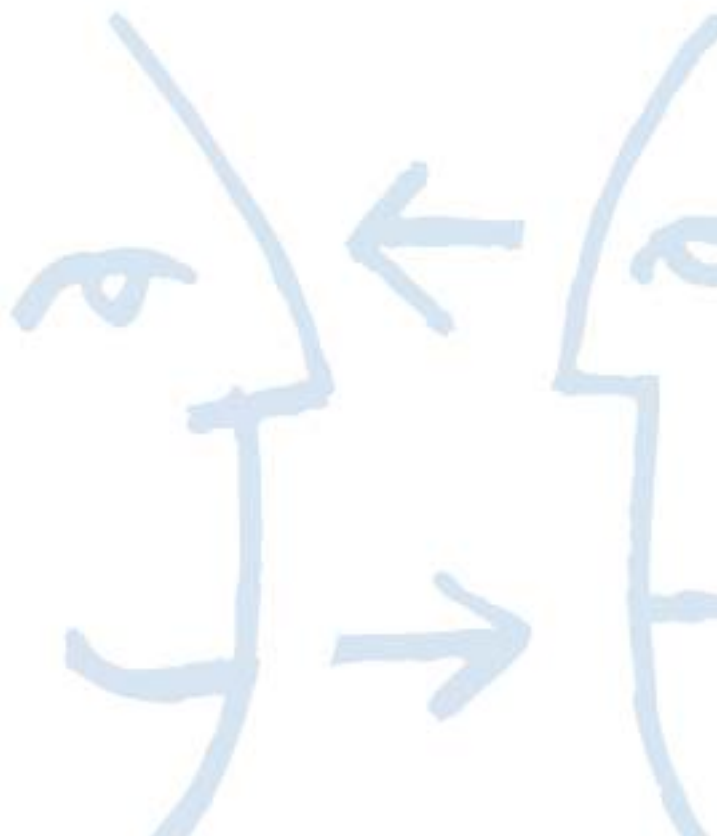
6.12 Durée d'utilisation des clés privées des unités d'horodatage


La durée d'utilisation opérationnelle d'une clé privée d'UH est au plus égale à la période de validité du certificat de clé publique correspondant.

Dans la pratique elle est réduite afin que la fin de période de vérification de la dernière contremarque de temps qu'elle a signé coïncide avec la fin de validité du certificat de clé publique d'UH auquel elle correspond.

La durée d'utilisation opérationnelle des clés privées d'UH est égale à 1 an.

Cette durée de validité pourra être revue si les recommandations des autorités nationales compétentes sont amenées à évoluer.



 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

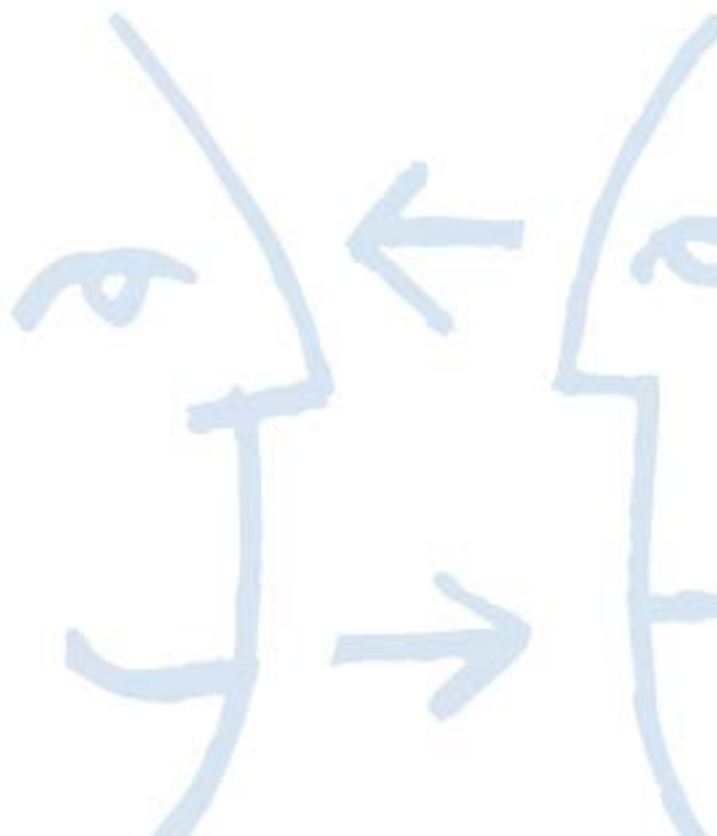
7 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE


7.1 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

7.2 Documents techniques

Renvoi	Document
[ANSSI_ALGO]	Mécanismes cryptographiques, Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 1.11 du 24 octobre 2008
[ETSI_PH]	ETSI TS 102 023 V1.2.2 (2008-10) Policy requirements for Time-Stamping Authority
[ETSI_TSP]	ETSI TS 101 861 V1.3.1 (2006-01) Time Stamping Profile
[PC_KEYNECTIS_KACH]	Politique de certification de l'ACH de KEYNECTIS qui délivre les certificats aux UH de l'AH de KEYNECTIS
[RFC3161]	IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol - 08/2001



 KEYNECTIS	POLITIQUE D'HORODATAGE	Date :	23 novembre 2009
	Service K.Stamp®	OID :	1.3.6.1.4.1.22234.2.6.5.1.1
		Version :	1.1

8 ANNEXE 2 : FORMATS DES CONTREMARQUES DE TEMPS

Les contremarques de temps fournies par les AH respectant la présente PH ont 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 la PRIS respecte, de base, les exigences correspondantes du [RFC3161], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Exigences
<i>version</i>	Pas d'exigence supplémentaire par rapport au [RFC3161].
<i>policy</i>	Pas d'exigence supplémentaire par rapport au [RFC3161].
<i>messageImprint</i>	Cf. chapitre 6.8 ci-dessus relativement aux fonctions de hachage.
<i>serialNumber</i>	Pas d'exigence supplémentaire par rapport au [RFC3161].
<i>genTime</i>	Pas d'exigence supplémentaire par rapport au [RFC3161].
<i>accuracy</i>	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.
<i>ordering</i>	Ce champ doit être absent ou bien contenir la valeur <i>false</i> .
<i>nonce</i>	Pas d'exigence supplémentaire par rapport au [RFC3161].
<i>tsa</i>	Si ce champ est présent, il doit être identique au champ <i>subject</i> du certificat de l'UH ayant signé la contremarque de temps.
<i>extensions</i>	Des extensions peuvent être incluses par l'AH, mais aucune ne doit être marquée comme critique.

