Politique Horodatage Almerys

Infrastructure de confiance

PL
Politique

Référentiel :	Sous-Référentiel :	Référence :	Statut :
Sécurité	PKI	PKA026 1.2.250.1.16.12.5.20.1	Validé
Approuvé par :	**Fonction :**	**Date :**	**Signature :**
MMI	Responsable sécurité services de confiance	07/06/2013	
Validé par :	Fonction :	**Date[•] :**	**Signature :**
JMT	Autorité de Gouvernance	07/06/2013	
Diffusion auprès de :			
En accès pour :	Public.		
Localisation :			

Sommaire

Date de péremption		Responsable de l'actualisation	
Version	**Date**	**Modifications**	**Auteur**
v1.2	01/03/2013	Modification suite à migration system horodatage	Mustapha Miraoui
V1.3	07/06/2013	Modification suite à audit interne	Mustapha Miraoui

[•] Date d'entrée en vigueur

Documents de référence

Référence	Version	Titre du document

Sommaire détaillé

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 d'Almerys.

La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par Almerys 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 collectiv*e » 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.

1. INTRODUCTION

1.1 PRESENTATION GENERALE

Le Service d'horodatage d'Almerys peut être utilisé par ses clients de 2 façons différentes :

- directement, en tant que service à part entière.
  L'utilisation et la gestion des Contremarques de temps fournies par le Service est alors du ressort des Clients d'Almerys.
- inclus dans une offre de service Almerys dépassant la seule mise à disposition d'un Service d'horodatage. Illustration :
  - le Service d'horodatage peut fournir des dates fiables dans le cadre d'un Service de signature électronique, assurant ainsi une bonne assurance sur la qualité des dates associées aux actes de signature.

La structure de la présente Politique d'Horodatage est basée sur la Politique d'Horodatage Type du Référentiel Général de Sécurité (RGS) émis par la Direction Générale de la Modernisation de l'État (DGME) et l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), réf. 1.2.250.1.137.2.2.1.2.2.4.

L'objectif de ce document est de définir les engagements d'almerys, 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 des Conditions Générales d'utilisation du service d'horodatage (CGU).
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 d'almerys met en œuvre plusieurs UH pour supporter son service d'horodatage.

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. Cette vérification est à la charge de l'utilisateur du service d'horodatage.

1.2 IDENTIFICATION

1.2.1. Identification du document PH

La présente Politique d'Horodatage (PH) est dénommée « Politique d'Horodatage Almerys ». Elle peut être identifiée par son numéro d'identifiant d'objet (OID - cf. page de garde et en-tête de chaque page).

Le numéro d'OID du présent document est : 1.2.250.1.16.12.5.20.1
La référence du document au sein d'Almerys est la suivante : PKA026.

1.2.2. Identification de l'OID politique d'horodatage almerys

L'OID Contremarques de temps émises par l'AH Almerys avec cette politique est :
1.2.250.1.16.12.5.20.1.1
En cas de changement de politique l'OID des Contremarques de temps, le nouvel OID sera :
1.2.250.1.16.12.5.20.1.2

1.3 PUBLICATION DU DOCUMENT

La présente Politique d'Horodatage est publiée sur l'URL : pki.almerys.com/timestamp.html

1.3.1. Circonstances rendant une mise à jour nécessaire

La mise à jour de la Politique d'Horodatage est un processus impliquant l'AG, et le responsable de sécurité des services de confiance, et le service juridique almerys. Il est enclenché essentiellement pour :

- procéder à des modifications importantes,
- prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique,
- prendre en compte les MAJ suite aux audites de surveillance LSTI.

Toutes les remarques, ou souhaits d'évolution, sur la présente politique sont à adresser par courriel à l'adresse indiqué dans le paragraphe 1.6.

1.4 ENTITE DETERMINANT LA CONFORMITE DES PRATIQUES AVEC LA PH

L'entité en charge de l'administration et de la gestion de la politique d'horodatage est l'AG, et le Responsable Sécurité des Services de Confiance.
Le responsable des services de confiance s'appuie sur les ressources d'almerys, ou ressources externes ayant une expertise dans le domaine pour l'évaluation de la conformité des pratiques avec la PH.
Le responsable de sécurité des services de confiance est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PH.
A cette fin, le responsable de sécurité des services de confiance met en œuvre et coordonne les prestations pour l'évaluation de la conformité DPH, et PH.
La Politique d'Horodatage est réexaminée à minima tous les deux (2) ans.

1.5 PROCEDURES D'APPROBATION DE LA CONFORMITE DE LA DPH

L'approbation de conformité de la DPH par rapport à cette PH est à la charge de l'AG, et du responsable de sécurité des services de confiance.
Le responsable de sécurité des services de confiance est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPH doit suivre le processus d'approbation mis en place.

1.6 POINT DE CONTACT

Le représentant habilité à contacter pour toutes questions concernant la présente Politique d'horodatage est :
Autorité de Gouvernance IGC almerys
Téléphone : 04 73 74 82 98- Fax : 01 48 78 98 71
Almerys – 46 rue du Ressort – 63967 CLERMONT-FERRAND CEDEX 9

1.7 GENERALITES

1.7.1. 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. Cette notion est valable pour les hypothèses où la Contremarque de temps est demandée directement à l'AH.

Autorité de Certification (AC) – Entité qui délivre et est responsable des Certificats électroniques signés en son nom.

Autorité d'Horodatage (AH) –
Entité en charge de l'émission et de la gestion des Contremarques de temps conformément à une Politique d'horodatage.

Client - Entité cliente qui met à la disposition de ses Utilisateurs le service de signature électronique d'Almerys.

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) – Document qui 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.

Horodatage - Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé.

Jeton d'horodatage – Voir Contremarque de temps.

Liste de Certificats Révoqués (**LCR**) – Liste de certificats ayant fait l'objet d'une révocation avant la fin de leur période de validité.

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.

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).

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 Utilisateur de Contremarques de temps.

1.7.2. 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-LCR	Liste de Certificats Révoqués partielle
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion de Clés
LCR	Liste des Certificats Révoqués
OID	Object Identifier
PH	Politique d'Horodatage
PSHE	Prestataire de Services d'Horodatage
UH	Unité d'Horodatage
UTC	Coordinated Universal Time

2. DISPOSITIONS GENERALES

2.1 OBLIGATIONS DE L'AUTORITE D'HORODATAGE

L'AH génère et signe les Contremarques de temps conformément aux documents suivants : la présente PH, la DPH associée et les CGU.
L'AH garantit la conformité pour tout acteur intervenant dans la gestion des Contremarques de temps par rapport aux exigences et aux procédures prescrites dans cette PH et dans la DPH associée.
L'AH remplit tous ses engagements tels que stipulés dans ses Conditions générales d'utilisation.
L'AH garantit la conformité des exigences et procédures définies dans sa DPH avec la présente PH.
L'AH met à la disposition des Abonnés, Utilisateurs et Clients l'ensemble des informations nécessaires à la vérification des Contremarques de temps.
L'AH respecte les conditions de disponibilité du Service d'horodatage convenues contractuellement avec les Clients et les Abonnés.
L'AH maintient une information sur la compromission de la Bi-clé des UH.

2.2 OBLIGATIONS DU CLIENT

Le Client respecte les obligations de la présente PH et des CGU qui lui sont applicables.
Le Client transmet les CGU à ses Utilisateurs ou fait figurer les obligations à la charge de l'Abonné dans un document opposable aux Utilisateurs du service de signature électronique.

2.3 OBLIGATIONS DE L'ABONNE

L'Abonné, au moment de l'obtention d'une contremarque de temps, doit vérifier la signature numérique de la contremarque, et que le certificat de l'Unité d'Horodatage n'est pas révoqué. L'AH met à disposition de l'Abonné les éléments lui permettant de faire cette vérification.

2.4 OBLIGATIONS DE L'UTILISATEUR DE CONTREMARQUES DE TEMPS

Pour faire confiance à une Contremarque de temps, l'Utilisateur devra :

a) Vérifier que la Contremarque de temps a été correctement signée, et que le certificat de l'UH est valide à l'instant de la vérification.
b) tenir compte des limitations sur l'utilisation de la Contremarque de temps indiquées dans la PH, la DPH et les conditions générales d'utilisation.
c) Comparer le condensé contenu dans la Contremarque de temps et celui de la donnée horodatée.

2.5 OBLIGATIONS POUR LES AC FOURNISSANT LES CERTIFICATS DES UHS

Les certificats doivent être délivrés par l'AC : ALMERYS CUSTOMER SERVICES CA NB faisant l'objet d'une certification ETSI 101042.
Le certificat de l'UH utilisé pour signer les demandes de Contremarques de temps devra contenir l'OID correspondant de l'AC.

2.6 DECLARATIONS DES PRATIQUES D'HORODATAGE

L'AH garantit qu'elle possède la fiabilité nécessaire pour fournir des Services d'horodatage. En particulier :

a) L'AH a une Déclaration des pratiques et des procédures utilisées pour adresser toutes les exigences identifiées dans chaque PH supportée.
b) La DPH identifie 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 UH.
c) Le responsable opérationnel de l'AH garantit que les pratiques sont correctement mises en œuvre.
d) L'AH définit une procédure de contrôle périodique de la conformité des pratiques, y compris les responsabilités, à la déclaration des pratiques d'horodatage.
e) L'AH doit informer au préalable les Abonnés et les Clients pour tout changement qu'elle a l'intention de faire dans la partie publique de sa DPH et, après l'approbation, immédiatement mettre à la disposition des Abonnés, des Clients et des Utilisateurs de contremarques de temps la partie publique révisée de la DPH.
f) Si l'AH a été évaluée pour être en conformité avec la présente PH et si une modification envisagée à l'initiative de l'AH pouvait entraîner une non-conformité avec ladite PH ou avec la DPH, alors l'AH doit indiquer qu'elle soumettra cette modification à l'organisme évaluateur indépendant pour avis.

2.7 CONDITIONS GENERALES D'UTILISATION

L'AH définit des CGU qui reprennent les grands principes décrits dans la présente PH. Ces CGU sont basées sur le modèle défini dans l'annexe B de l'ETSI 102023.

2.8 CONFORMITE AVEC LES EXIGENCES LEGALES

L'AH garantit la conformité avec les exigences légales. En particulier :

a) Des mesures techniques appropriées et organisationnelles sont prises contre le traitement non autorisé ou illégal des données à caractère personnel (cf. [CNIL]), contre la perte accidentelle, la destruction de données à caractère personnel ou les dégâts commis aux données à caractère personnel.
b) Les informations fournies par les Abonnés à l'AH ne sont pas divulguées, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.
c) Elle rédige des CGU applicables pour les Abonnés ou portent à la connaissance les obligations opposables aux Clients, aux Abonnés et aux Utilisateurs de contremarques de temps.

2.8.1. Droit applicable

Le présent document est régi par la loi française.

2.8.2. Règlement des différends

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux compétents de la cour d'appel de Clermont Ferrand.

2.8.3. Propriété intellectuelle

Sur le plan de la propriété intellectuelle, les produits mis en œuvre par almerys dans le service d'horodatage appartiennent aux éditeurs de ces produits.
Les utilisateurs de ces services ne disposent d'aucun droit de propriété intellectuelle sur ces différents éléments. Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils

contiennent, par quelque procédé que ce soit, est strictement interdite et constitue une contrefaçon sanctionnée par le Code de la propriété intellectuelle, sauf accord préalable et écrit par almerys.

2.8.4. Données nominatives

En conformité avec les dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le traitement automatisé des données nominatives, réalisé à partir des plates-formes almerys a fait l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés [CNIL].

Conformément à l'article 32 de la loi n° 78-17 du 6 janvier 1978, les utilisateurs sont informés que les données personnelles qu'ils communiquent pourront être transmises et exploitées par almerys et les différents partenaires intervenant dans les échanges concernés.

Les utilisateurs sont informés qu'ils disposent d'un droit d'accès, de rectification et d'opposition portant sur les données le concernant en écrivant à almerys, Service Correspondant Informatique et Liberté, 46 Rue du Ressort, 63967 Clermont-Ferrand Cedex 9.

Les utilisateurs des services almerys sont tenus de respecter les dispositions de la loi relative à l'informatique, aux fichiers et aux libertés, dont la violation est passible de sanctions disciplinaires et pénales.

Ils doivent notamment s'abstenir, s'agissant des informations nominatives auxquelles ils accèdent, de toute collecte, de toute utilisation détournée et, d'une manière générale, de tout acte susceptible de porter atteinte à la vie privée ou à la réputation des personnes.

3. EXIGENCES OPERATIONNELLES

3.1 GESTION DES REQUETES DE CONTREMARQUES DE TEMPS

L'AH almerys génère la contremarque de temps à partir du condensat des données qui lui est transmis par les applications clientes (empreinte de la donnée à horodater) et la lui retourne.
La fourniture d'une Contremarque de temps en réponse à une demande n'excède pas quelques secondes[1], ceci afin de ne pas nuire ni dégrader l'ergonomie de l'application appelante.
L'AH almerys ne conserve pas la contremarque de temps générée.

3.2 FICHIERS D'AUDIT

L'AH enregistre les informations appropriées concernant le fonctionnement du Service d'horodatage, en particulier :

a) Les enregistrements d'audit relatifs à l'administration des Services d'horodatage.
b) Les enregistrements d'audit relatifs au fonctionnement du Service d'horodatage
c) Les enregistrements d'audit concernant les événements touchant au cycle de vie des clés et certificat d'UH
d) Les enregistrements d'audit concernant les événements touchant à une synchronisation de l'horloge des UH, y compris les événements touchant à la détection de perte de synchronisation.

La confidentialité des enregistrements d'audit est assurée par une gestion d'accès physique, système et réseau appropriée. L'intégrité est assurée par un scellement cryptographique.

Les journaux du service d'horodatage sont conservés pendant 5 ans.

3.3 GESTION DE LA DUREE DE VIE DE LA CLE PRIVEE

L'AH garantit que les clés privées de signature des UH ne sont pas employées au-delà de la fin de leur cycle de vie. En particulier :

a) Des procédures opérationnelles ou techniques assurent qu'une nouvelle paire de clés est mise en place quand la fin de la période d'utilisation d'une clé privée d'UH a été atteinte.
b) Le Système d'horodatage détruit la clé privée si la fin de la période d'utilisation de cette clé privée a été atteinte.

3.4 SYNCHRONISATION DE L'HORLOGE

L'AH garantit que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée de une seconde.
La synchronisation utilise des serveurs de temps qui sont eux-mêmes synchronisés sur plusieurs sources :

- Signal GPS ;
- Signal DCF77 ;
- NTP internet,

En particulier :

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

a) Le calibrage de chaque horloge d'UH est maintenu de telle manière que les horloges ne puissent pas normalement dériver en dehors de l'exactitude déclarée.
b) L'AH s'assure que tout non-respect de l'exactitude déclarée par son horloge interne sera détecté.
c) Si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude annoncée, ou que les serveurs de temps ne sont plus disponibles, alors les Contremarques de temps ne seront plus générées par cette UH.

3.5 EXIGENCES DU CONTENU D'UNE CONTREMARQUE DE TEMPS

Les Contremarques de temps sont conformes à la RFC 3161, les informations contenues dans une contremarque de temps sont :

Champ	***Description***	***Valeur***
version		1
Policy	OID de la PH	1.2.250.1.16.12.5.20.1.1
messageDigest	OID de l'algorithme de hash, et empreinte (hash) des données à horodater (inclue dans la requête d'horodatage)	
serialNumber	Identifiant unique de la contremarque de temps	
GenTime	Heure de génération de la contremarque de temps calculée par rapport à une source UTC(k)	
accuracy	Précision déclaré	1 seconde
Ordering		False
nonce	Identique à celui présenté lors de la demande de génération si celui-ci est présent dans cette dernière	
TSA	champ "subject" du certificat d'horodatage	
Extension	Pas d'extension supplémentaire	

3.6 COMPROMISSION DE L'AH

L'AH garantit, dans le cas d'événements qui affectent la sécurité des Services d'horodatage – incluant la compromission de la clé privée de signature d'une UH 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, des Clients et des Utilisateurs de contremarques de temps.

En particulier, l'AH traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une UH ou la perte de calibrage de l'horloge d'une UH, qui pourrait affecter des Contremarques de temps émises dans le cadre d'un plan de secours.

a) Dans le cas d'une compromission, réelle ou suspectée, l'AH met à la disposition de tous les Abonnés, Clients et Utilisateurs de contremarques de temps une description de la compromission qui est survenue.
b) Dans le cas d'une perte de calibrage d'une UH, qui pourrait affecter des Contremarques de temps émises, l'AH prendra les mesures nécessaires pour que les Contremarques de temps de cette UH ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.
c) Dans le cas d'une perte de connexion prolongée avec les serveurs de temps, l'AH prendra les mesures nécessaires pour que les Contremarques de temps de cette UH ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.
d) Dans le cas d'un événement majeur dans le fonctionnement de l'AH ou d'une perte de calibrage qui pourrait affecter des Contremarques de temps émises, chaque fois que cela sera possible, l'AH mettra à la disposition de tous ses Abonnés, des Clients 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 des Clients ou à la sécurité des Services d'horodatage.

3.7 FIN D'ACTIVITE

Des procédures de fin d'activité définies par l'AH garantissent que les dérangements potentiels aux Abonnés, aux Clients et aux Utilisateurs de contremarques de temps seront réduits au minimum suite à la cessation d'activité du Service d'horodatage et assurent en particulier la maintenance continue des informations nécessaires pour vérifier la justesse de Contremarques de temps. En particulier :

a) Avant que l'AH ne termine ses Services d'horodatage, les procédures suivantes seront exécutées au minimum :
   - l'AH rendra disponible à tous ses Abonnés, Clients et aux Utilisateurs de contremarques de temps l'information concernant sa fin d'activité via la publication sur son site internet;
   - l'AH abrogera 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'AH transférera à une entité d'Almerys ou 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'AH maintiendra ou transférera à une entité d'Almerys ou à un organisme fiable ses obligations de rendre disponibles aux Utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats;
   - les clés privées des UH seront détruites de telle façon que les clés privées ne puissent pas être recouvrées.
b) L'AH prend les mesures nécessaires pour couvrir les dépenses pour accomplir ces exigences minimales dans le cas où l'AH serait placée en liquidation judiciaire ou pour d'autres raisons serait incapable de couvrir les dépenses par elle-même.

L'AH provisionne les coûts nécessaires et suffisants pour maintenir le site de publication : http://pki.almerys.com/timestamp.html.

4. EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES, PROCEDURALES ET ORGANISATIONNELLES

4.1 EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES

4.1.1. Situation géographique et construction des sites

L'AH s'appuie sur ses locaux sécurisées sur le site de Clermont Ferrand pour héberger ses services d'horodatage.
A ce titre, la mise en sécurité du site du bâtiment de l'AH respecte les mesures de sécurité physique pour la protection périphérique, périmétrique et intérieure et notamment les mesures relatives à :

- l'alimentation électrique et climatisation ;
- la vulnérabilité aux dégâts des eaux ;
- la prévention et protection incendie.

4.1.2. Accès physique

L'AH garantit 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, pour la fourniture du service d'horodatage :

- l'accès physique aux équipements concernés par les Services d'horodatage est limité aux individus autorisés ;
- L'accès aux zones sensibles, salle machines, et bunker est renforcé par un contrôle d'accès biométrique,
- des contrôles sont mis en œuvre pour éviter la perte, des dégâts ou la compromission d'actifs et l'interruption des activités et ;
- des mesures de des contrôles sont mis en œuvre pour éviter la compromission ou le vol d'informations ou d'équipements informatiques.
- La traçabilité des accès est assurée par l'enregistrement des utilisations des badges électroniques.

En dehors des heures ouvrables, des mesures de détection d'intrusion physique sont mises en œuvre.

4.1.3. Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre par almerys de manière à ce qu'une interruption de service ne portent pas atteinte aux engagements pris par l'AH en matière de disponibilité (signature et délivrance des contremarques de temps)

- alimentation électrique : mise en œuvre de moyens techniques tels que des onduleurs et groupes électrogènes,
- défaillance de climatisation : redondance climatiseurs, alarmes de dysfonctionnement.

4.1.4. Exposition aux dégâts des eaux

Les moyens de protection mis en place par AH permettent de protéger son infrastructure contre les dégâts des eaux.

4.1.5. Prévention et protection incendie

Les zones sécurisées sont soumises à des mesures de prévention et de protection incendie appropriées.

4.1.6. Conservation des supports de données

Les documents « projet » afférents au service d'horodatage sont stockés sur un Intranet et bénéficient d'une sauvegarde quotidienne.

4.1.7. Mise hors service des supports

En fin de vie, les supports seront, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.
Les procédures et moyens de destruction et de réinitialisation sont conformes à la Politique de Sécurité de mise en œuvre par l'AH.

4.1.8. Sauvegarde hors site

En complément de sauvegardes sur sites, l'AH met en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes sont organisées de façon à assurer une reprise des services après incident la plus rapide possible.

4.2 EXIGENCES PROCEDURALES

4.2.1. Analyse des risques

Le service d'horodatage fait partie du périmètre de l'étude de risques menée par almerys.

4.2.2. Gestion des supports

Les supports employés dans les systèmes d'horodatage sont manipulés de manière sécurisée afin de les protéger des dégâts, du vol, de l'accès non autorisé et de l'obsolescence.
Les supports contenant des données sensibles sont retirés de manière sécuritaire quand ils ne sont plus utiles (gestion du recyclage ou de la destruction)

4.2.3. Planification de systèmes

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

4.2.4. Gestion des incidents

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

4.2.5. Manipulation et sécurité des systèmes

L'AH met en œuvre une politique de classification sur l'ensemble des éléments du service d'horodatage.

4.2.6. Procédures de fonctionnement et responsabilités

Les opérations de sécurité sur les composantes du service d'horodatage sont réalisées par du personnel de confiance qui est explicitement mis au courant de ses responsabilités. Les opérations de sécurité incluent notamment :

- 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.

4.2.7. Amélioration continue des systèmes d'information

Almerys met en œuvre un processus d'amélioration continue dans le cadre de son service d'horodatage.

4.2.8. Gestion d'accès au système

L'accès aux systèmes du service d'horodatage est réservé aux seules personnes formellement habilitées. Les administrateurs sont munis d'un certificat personnel permettant de tracer nominativement l'ensemble des accès aux systèmes d'horodatage.
Des équipements de filtrage sont positionnés en amont des serveurs d'horodatage pour garantir que seuls les flux nécessaires et suffisants sont autorisés à accéder à ces serveurs. Les équipements d'infrastructure sont positionnés dans une zone sécurisée.
Toutes les traces liées à l'administration des systèmes sont conservées conformément aux exigences exposées dans le paragraphe 3.2.
Les incidents sur les serveurs d'horodatage font l'objet de remontées d'alertes vers une équipe en charge de les analyser et de les traiter.

4.3 EXIGENCES ORGANISATIONNELLES

4.3.1. Rôles de confiance

Les rôles de confiance définis et le nombre de personnes disposant de ce rôle de confiance pour le service d'horodatage sont au moins :

- Officier de sécurité horodatage : gestion de la sécurité, la configuration et du paramétrage des unités d'horodatage ;
- Administrateur système de l'AH : il installe, configure et maintient à jour l'ensemble de la plateforme technique du SH ;
- Opérateur de l'AH : il a la responsabilité du fonctionnement quotidien des UHs ;
- Contrôleur (auditeur) de l'AH : il est en charge de l'analyse récurrente des événements intervenant sur les composantes de l'AH.

L'AH a également défini des porteurs de secrets pour l'accès aux opérations sensibles sur le boîtier cryptographique stockant les clés privées des unités d'horodatage. Le regroupement d'un sous-ensemble de ces porteurs est nécessaire pour la réalisation de ces opérations.
Pour pouvoir réaliser les opérations d'exploitation et de supervision de l'infrastructure réseau et system, almerys appuie sur ses équipes internes.

4.3.2. Identification et authentification pour chaque rôle

Des mesures d'identification et d'authentification sont mises en place afin de supporter la mise en oeuvre de la politique de contrôle d'accès et la traçabilité des opérations ; la politique de contrôle d'accès limite l'accès aux seules personnes autorisées conformément à leur besoin d'en connaître.

Les rôles attribués concernant les services d'horodatage sont notifiés aux personnes concernées par l'autorité de gouvernance.

4.3.3. Mesures de sécurité vis à vis du personnel

4.3.3.1. Qualifications, compétences, et habilitations requises

Tout intervenant amené à occuper un rôle identifié comme sensible est soumis à une clause de confidentialité.
L'AH s'assure que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles.
Le personnel d'encadrement de l'AH possède l'expertise appropriée, et est familier des procédures de sécurité.
Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités (description de poste) et des procédures liées à la sécurité du système et au contrôle du personnel.

4.3.3.2. Procédures de vérification des antécédents

Almerys procède avant le recrutement d'une personne à la vérification des antécédents de cette dernière, de manière à valider sa correspondance vis-à-vis du poste à pourvoir.

4.3.3.3. Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement. Cela concerne essentiellement le personnel opérant sur les composantes du service d'horodatage.
Les personnels participant au service d'horodatage ont notamment des connaissances sur les thèmes suivants :
Technologie et fonctionnement de l'horodatage ;
Technologie et principe de la signature électronique ;
Connaissance des principes de calibration et de synchronisation des horloges de temps ;
Connaissance et respect des règles de sécurité pour les personnels techniques.

4.3.3.4. Exigences en matière de formation continue et fréquences des formations

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants.
Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.

4.3.3.5. Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans le règlement intérieur.

4.3.3.6. Exigences vis à vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées. Il s'agit essentiellement du personnel de surveillance du site de Clermont et des équipes de l'éditeur du serveur d'horodatage qui a en charge le maintien opérationnel du système.

4.3.3.7. Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de la prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans le service d'horodatage disposent des procédures correspondantes.

5. EXIGENCES DE SECURITE TECHNIQUES

5.1 EXACTITUDE TEMPS

L'AH garantit que son horloge est synchronisée sur des serveurs Ntp avec le temps UTC selon l'exactitude déclarée de une seconde.
Les serveurs ntp sont autonomes et bénéficient d'une procédure de synchronisation avec des sources GPS, DCF77, et références UTC(k).

5.2 GENERATION DE CLE

L'AH garantit que les clés cryptographiques des UH sont produites dans des circonstances et un environnement contrôlés. La protection de ces clés s'appuie sur des HSM Cryptographiques.
Lors de cette génération, les clés privées d'UH ne sont pas exportable de ces ressources.
La génération des clés privées des unités d'horodatage est réalisée durant une cérémonie des clés qui fait l'objet d'un procès-verbal.
Les modules des clés privées d'UH ont une longueur de 2048 bits pour l'algorithme RSA.

5.3 CERTIFICATION DES CLES DE L'UNITE D'HORODATAGE

L'AH s'assure que la valeur de la clé publique et l'identifiant de l'algorithme de signature contenus dans la demande de certificat de l'UH sont égaux à ceux générés par l'UH.

C'est l'AC « ALMERYS CUSTOMER SERVICES CA NB » de l'IGC Almerys qui est chargée de la génération des certificats des UH.
La demande de certificat envoyée auprès de l'AC contient, en plus des informations exigées dans la PC de l'AC « ALMERYS CUSTOMER SERVICES CA NB» pour la partie enregistrement, au moins les informations suivantes :

- le nom (DN) de l'UH pour laquelle la demande de certificat est faite, l'AG s'assure que le nom de l'UH est unique lors de la demande de génération ;
- la valeur de la clé publique (et l'identifiant de l'algorithme) ;

La longueur des clés de l'AH est de 2048 bits.

La vérification de ces informations lors de l'import du certificat est faite par l'unité d'horodatage en contrôlant ces informations par rapport à celle fournies dans la demande de certificat.
L'import du certificat permet de valider et d'initialiser le contexte d'horodatage et ainsi permettre le démarrage de l'unité d'horodatage.

5.4 PROTECTION DES CLES PRIVEES DES UNITES D'HORODATAGE

Les clés privées des UH sont stockées dans un HSM certifié FIPS 140-2 niveau 3.

5.5 EXIGENCES DE SAUVEGARDE DES CLES DES UNITES D'HORODATAGE

Une sauvegarde la partition HSM contenant les clés de chaque UH est effectuée lors de la KC.

5.6 DESTRUCTION DES CLES DES UNITES D'HORODATAGE

Les clés de signature des UH sont détruites à la fin de leur cycle de vie.

5.7 ALGORITHMES OBLIGATOIRES

Par défaut, l'AH est configurée pour accepter les algorithmes souhaités par les Abonnés, si ceux-ci sont compatibles avec les meilleures pratiques et les recommandations de l'ANSSI et de l'ETSI.

Les contremarques de temps sont signées selon les algorithmes et les longueurs de clé conformes aux exigences des autorités compétentes en la matière. La bi-clé de l'UH est une bi-clé RSA de 2048 bits. L'algorithme de signature utilise une fonction de hachage SHA-256.

5.8 VERIFICATION DES CONTREMARQUES DE TEMPS

L'AH garantit 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 UH sont disponibles, joints à la Contremarque de temps.
b) La chaîne de certification Almerys complète est disponible comprenant le certificat de l'AH, le certificat de l'AC intermédiaire « ALMERYS CUSTOMER SERVICES CA NB», ainsi que le certificat de l'AC racine « almerys Root CA ».
   Ces certificats sont disponibles sous http://pki.almerys.com/
c) Les LCR des AC suscités sont disponibles en activant les URL disponibles dans les certificats dans l'attribut cRLDistributionPoint.
   Ces LCR sont également publiées sous http://pki.almerys.com/

5.9 DUREE DE VALIDITE DES CERTIFICATS DE CLE PUBLIQUE DES UNITES D'HORODATAGE

La durée de validité des certificats des UH n'est pas plus longue que la fin de validité du certificat d'AC « almerys customer services ca nb» qui l'a émis.
Par défaut, cette durée est de 3 ans minimum.

5.10 DUREE D'UTILISATION DES CLES PRIVEES DES UH

La durée de vie minimale des clés privées des UH est de 2 ans, et au maximum 2 ans et 3 mois.
Le renouvèlement de certificat d'une UH s'effectue dans les trois (3) mois, au-delà des deux (2) ans de durée de vie du certificat de l'UH.

5.11 PROFIL CERTIFICAT ET CONTREMARQUE DE TEMPS

5.11.1.Format du certificat d'horodatage

tbsCertList		Valeur
version		2 (c'est-à-dire version3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
▶ algorithm		Sha2withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN = ALMERYS CUSTOMER SERVICES CA NB OU = ADVANCED SERVICES OU = 0002 432701639 O = ALMERYS C = FR
validity		
▶ notBefore		Date de création
▶ notAfter		notBefore + 3 ans
subject CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN= ALMERYS TIMESTAMP SERVER Y OU = TIMESTAMP SERVICES OU=0002 432701639 O=ALMERYS C=FR
subjectPublicKeyInfo		
▶ algorithm ➥ algorithm ➥ parameters		rsaEncryption RSAParams : NULL
▶ subjectPublicKey		RSAPublicKey (2048 bits)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
▶ authorityKeyIdentifier	Non	Hash de la clé publique de l'issuer
▶ subjectKeyIdentifier	Non	Hash de la clé publique de l'issuer
▶ keyUsage	Oui	digitalSignature (0)
▶ privateKeyUsagePeriod		Extension non utilisée
▶ certificatePolicies	Non	Stratégie du certificat : Identificateur de stratégie = 1.2.250.1.16.12.5.41.1.5.2.1.2
▶ basicContraints ➥ cA ➥ pathLenConstraint	Non	false None

▶ extKeyUsage	oui	id-kp-timestamping
▶ cRLDistributionPoints	Non	Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/almeryscustomerservicescanb.crl
Private extensions		
▶ authorityInfoAccess	Non	[1] : accessMethod : id-ad-calssuers accessLocation : http://pki.almerys.com/almeryscustomerservicescanb.cer
▶ subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha2withRSAEncryption
parameters		NULL

5.12 FORMAT DE LA CONTREMARQUE TEMPS

Champ	***Description***	***Valeur***
version		1
Policy	OID de la PH	
messageDigest	OID de l'algorithme de hash, et empreinte (hash) des données à horodater (inclue dans la requête d'horodatage)	
serialNumber	Identifiant unique de la contremarque de temps	
GenTime	Heure de génération de la contremarque de temps calculée par rapport à une source UTC(k)	
accuracy	Précision déclaré	1 seconde
Ordering		False
nonce	Identique à celui présenté lors de la demande de génération si celui-ci est présent dans cette dernière	
TSA	champ "subject" du certificat d'horodatage	
Extension	Pas d'extension supplémentaire	

6. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

6.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Un contrôle de conformité à la PH en vigueur lors de la mise en œuvre opérationnelle du système, et lors de toute modification significative est effectué.
almerys bénéficie de plusieurs types d'audit :
– un audit interne réalisé par des prestataires externes spécialistes du domaine du SH ;
– un audit de certification réalisé par un organisme accrédité au moins une fois par an.

6.2 8.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

L'évaluateur se doit d'être rigoureux pour s'assurer que les politiques, déclarations et services sont correctement mis en œuvre et détecter les cas de non conformités qui pourraient compromettre la sécurité du service offert.
L'AH s'engage à mandater des évaluateurs qui sont compétents en sécurité des systèmes d'information, en particulier dans le domaine d'activité de la composante contrôlée.

7. ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

7.1 REGLEMENTATION

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
[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".