PUBLIC

POLITIQUE D'HORODATAGE - DECLARATION DES PRATIQUES D'HORODATAGE

AUTEUR(S)	:	F. Da Silva
N° DE DOCUMENT	:	WLM-TSA-F081
VERSION	:	1.2
STATUT	:	Final
SOURCE	:	Worldline
DATE DU DOCUMENT	:	23 avril 2019
NOMBRE DE PAGES	:	25

PROPRIETAIRE	:	Comité MediaCert

Rôle	Nom	Signature	Date
Relecteur 1 – Resp. adjoint TSP	Fanny Lesecq	Fanny Lesecq	23/04/2019
Relecteur 2 – RSSI	Nicolas Abrioux	Nicolas Abrioux	23/04/2019
Fonction d'assurance qualité	Franck Da Silva	Franck Da Silva	23/04/2019
Propriétaire du document	Comité MediaCert	Guillaume Bailleul	23/04/2019
Approbateur - Resp. TSP	Guillaume Bailleul	Guillaume Bailleul	23/04/2019

TSP MediaCert

Digitally signed by TSP MediaCert
DN: CN=TSP MediaCert, O=Worldline, E=dl-mediacert-tsp@worldline.com, C=FR
Reason: I am approving this document
Location:
Date: 2019-04-23 17:34:25

Table des Matières

Liste des modifications

Version	Date	Description	Auteur(s)
0.1	19/10/2017	Version initiale	F. Da Silva
1.0	30/03/2018	Validation du document en Comité Sécurité	Comité Sécurité
1.1	05/07/2018	Ajout de l'OID de l'ETSI 319 421 Ajout de l'exigence de liée au délais de publication des documentations du TSP MediaCert Réordonnancement des étapes à effectuer lors de la cessation d'activité Suppression du champ TSA dans le profil des CT	F. Da Silva
1.2	23/042019	Révision annuelle : pas de modification hormis l'évolution des versions des normes du référentiel	F. Da Silva

1 Introduction

1.1 Présentation générale

Ce document décrit la Politique d'Horodatage du *Trust Service Provider* MediaCert établie par Worldline pour régir le Service d'Horodatage qui peut être utilisé par ses clients de deux manières possibles :

- soit directement en tant que service à part entière ;
- soit indirectement à travers le service de signature électronique, proposé par ce même *Trust Service Provider* MediaCert.

Ce document présente dans ce cadre :

- les exigences auxquelles se conforme le *Trust Service Provider* Mediacert en tant qu'Autorité d'Horodatage ;
- la génération et la gestion des Contremarques de temps ;
- les obligations et exigences portant sur les différents acteurs.

En plus de décrire la Politique d'Horodatage, ce document inclut la partie publique de la Déclaration des Pratiques d'Horodatage. Il s'agit là de l'énoncé des mécanismes et procédures auxquelles l'Autorité d'Horodatage a recours dans la gestion des Contremarques de temps qu'elle génère. Les éléments confidentiels de la Déclaration des Pratiques d'Horodatage sont consignés dans une Documentation Technique des Pratiques d'Horodatage (DTPH).

Cette Politique d'Horodatage – Déclaration des Pratiques d'Horodatage n'impose pas d'exigence 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.

La structure du présent document est basée sur les documents issus de :

- [ETSI 319 421] ;
- [RGS A5].

Le service d'horodatage, décrit par la présente PH, étant un service de confiance de MediaCert, l'ensemble des exigences de [PG] sont, sauf mention contraire, applicables au périmètre du présent service.

Le service d'horodatage vise à émettre des Contremarques de temps qualifiées au sens du Règlement Européen [eIDAS]. Pour ce faire, l'AH est opérée en conformité avec les exigences des normes suivantes :

- [ETSI 319 421] ;
- [QUALIF AH] ;
- [QUALIF PSC].

1.2 Identification du document

Eléments	Valeur
Titre	Politique d'Horodatage - Déclaration des Pratiques d'Horodatage
Référence document	WLM-TSA-F081
OID	1.2.250.1.111.20.2.1
Version	1.2
Auteur	F. Da Silva

La définition de l'OID du présent document est présentée dans la [PG].

Ce présent document sera appelé « PH-DPH » tout le long du document.

1.3 Gestion de la PH

1.3.1 Entité gérant la PH

Le présent document ne rajoute pas d'information par rapport à la [PG].

1.3.2 Entité déterminant la cohérence d'une DPH avec cette PH

Le présent document ne rajoute pas d'information par rapport à la [PG].

1.3.3 Procédure d'approbation

Le présent document ne rajoute pas d'information par rapport à la [PG].

1.3.4 Point de contact

Le présent document ne rajoute pas d'information par rapport à la [PG].

1.4 Définitions et acronymes

1.4.1 Définitions

Une liste des principales définitions des termes techniques employés dans cette PH-DPH est présentée ci-dessous.

Abonné : entité ayant besoin de faire horodater des données par une Autorité d'Horodatage et qui a accepté les conditions d'utilisation de ses services.

Autorité de Certification : entité qui produit et délivre des Certificats. Cette entité a en charge le cycle de vie complet de ces Certificats (création, publication, révocation, …).

Autorité d'Horodatage : entité en charge de l'émission et de la gestion de Contremarques de temps conformément à la présente PH-DPH.

Bi-clé : couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptographie basée sur des algorithmes asymétriques (RSA par exemple).

Certificat : élément de données normalisé X509 permettant d'associer une clé publique à son détenteur. Un Certificat contient des données comme l'identité du détenteur, sa clé publique, l'identité de l'organisme ayant émis le Certificat, la période de validité, un numéro de série, une empreinte (*thumbprint*) ou bien encore les critères d'utilisation. Le tout est signé par la clé privée de l'Autorité de Certification ayant émis le Certificat.

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

Horodatage : mécanisme qui consiste à associer une date et une heure à un événement, une information ou une donnée informatique dans le but d'enregistrer l'instant auquel une opération a été effectuée.

Jeton d'horodatage : cf. Contremarque de temps.

Service d'Horodatage : ensemble des prestations nécessaires à la génération et à la gestion des Contremarques de temps.

Système d'horodatage : ensemble des Unités d'Horodatage et des composants d'administration et de supervision utilisés pour fournir le Service d'Horodatage.

Unité d'Horodatage : 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 Autorité de Certification et par une clé unique de signature de Contremarques de temps.

***Universal Time Coordinated* :** est une échelle de temps adoptée comme base du temps civil international par la majorité des pays du globe.

UTC(k) : temps de référence réalisé par le laboratoire « k » (ex : Observatoire de Paris) 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.

Utilisateur : entité (personne ou système) qui fait confiance à une Contremarque de temps émise sous la PH-DPH.

1.4.2 Acronymes

Les acronymes utilisés dans la présente PH-DPH sont les suivants :

- **AC :** Autorité de Certification ;
- **AH :** Autorité d'Horodatage ;
- **CGU :** Conditions Générales d'Utilisation ;
- **CT :** Contremarque de temps ;
- **DTPH :** Documentation Technique des Pratiques d'Horodatage ;
- **ETSI :** *European Telecommunication Standards Institute* ;
- **LCR :** Liste des Certificats Révoqués ;
- **OID :** *Object Identifier* ;
- **PH-DPH :** Politique d'Horodatage – Déclaration des Pratiques d'Horodatage ;
- **SH :** Service d'Horodatage ;
- **UH :** Unité d'Horodatage ;
- **UTC :** Temps Universel Coordonné (*Universal Time Coordinated*).

2 Responsabilités concernant la mise à disposition des informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

Le présent document ne rajoute pas d'information par rapport à la [PG].

2.2 Informations devant être publiées

Les informations publiées par le Comité Mediacert sur son site web concernant les Services d'Horodatage sont les suivants :

- la présente PH-DPH écrite en français et en anglais ;
- les anciennes versions de PH-DPH écrites en français et en anglais ;
- les conditions générales d'utilisation en cours de validité ;
- le certificat de chacune des Unités d'Horodatages régies par le présent document ;

La [PG] apporte des informations quant au lieu de mise à disposition des informations susvisées.

2.3 Délais et fréquences de publication

Le présent document ne rajoute pas d'information par rapport à la [PG].

2.4 Contrôles d'accès aux informations publiées

Le présent document ne rajoute pas d'information par rapport à la [PG].

3 Dispositions générales

3.1 Obligations de l'Autorité d'Horodatage

Un certain nombre d'obligations s'imposent à l'AH. En effet, l'AH doit :

- fournir un Service d'Horodatage (SH) conformément aux exigences et aux procédures prescrites dans la présente PH-DPH. En particulier, l'AH vise une disponibilité de son SH de 7j/7 24h/24 ;
- remplir tous ses engagements tels que stipulés dans les CGU ;
- garantir la conformité des exigences et procédures définies dans la DTPH avec la présente PH-DPH ;
- garantir l'adhésion aux obligations complémentaires imposées par l'Autorité de Certification ayant émis les Certificats des Unités d'Horodatage. En particulier, les certificats des Unités d'Horodatage sont dédiés à la génération de CT et ne sont pas utilisés pour aucun autre usage ;
- informer les parties prenantes en cas de compromission d'une UH de son Système d'horodatage, comme rappelé dans la [PG].

3.2 Obligations de l'Abonné

L'Abonné se doit d'accepter et se conformer aux CGU de l'AH s'il souhaite bénéficier du SH.

L'Abonné est responsable du calcul correct de l'empreinte d'une donnée et du lien entre les données horodatées et la CT produite.

L'Abonné s'engage à vérifier la validité des CT dès leur réception et à s'assurer que l'empreinte contenue est identique à celle soumise dans la requête.
De plus, il est recommandé que l'Abonné vérifie le statut du Certificat de l'UH délivrant la CT au moment de la demande d'horodatage.

L'Abonné est responsable de la conservation des CT pour répondre à ses besoins propres.

L'Abonné doit utiliser le service en prenant en compte les limitations du SH, en particulier :

- le service ne doit pas être utilisé pour des usages nécessitant une exactitude supérieure à celle indiquée dans la CT ;
- de la durée limitée de validité des Certificats des Unités d'Horodatage ;
- de la non-conservation potentielle des CT par l'AH.

L'ensemble de ces obligations sont reprises dans les [CGU] du service.

3.3 Obligations de l'Utilisateur

L'Utilisateur doit :

- vérifier que la CT a été correctement signée et que le Certificat de l'UH ayant délivré la CT est valide à l'instant de la vérification de la CT ;
- tenir compte des limitations d'usage de la CT indiquées dans le présent document et dans les [CGU], en particulier en tenant compte de la durée de validité du Certificat de l'Unité d'Horodatage.

La validation d'une Contremarque de temps consiste à :

- comparer le haché contenu dans la CT au haché du document horodaté ;
- valider la chaîne de certification du Certificat de l'UH jusqu'à la racine de confiance ;
- s'assurer qu'aucun Certificat de la chaîne de confiance n'a été révoqué avant l'établissement de la CT. Cela peut être aisément réalisé à l'aide des LCR publiées par les AC émettrices desdits Certificats (voir [PC-DPC]).

Au-delà de la période de validité du Certificat de l'UH, les éléments complémentaires suivants doivent faire l'objet d'une vérification :

- s'assurer que la clé privée de l'UH n'a pas fait l'objet d'une compromission ;
- que l'algorithme de hachage possède toujours la robustesse nécessaire et qu'il n'a pas été mis en évidence l'existence de collisions ;
- que l'algorithme de signature et la taille de clé utilisé dans la signature de la CT est toujours robuste cryptographiquement au moment de la vérification.

Alternativement, le stockage sécurisé ou le renouvellement de la CT sont des méthodes pouvant être mises en œuvre et permettent de démontrer la validité de la CT au-delà de la période de validité du Certificat d'UH.

3.4 Déclaration des Pratiques d'Horodatage

L'AH garantit qu'elle possède la fiabilité nécessaire pour fournir le SH et en décrit la mise en œuvre au sein du présent document. En particulier :

- l'AH effectue de manière régulière une analyse des risques afin d'identifier les risques SSI et les mesures SSI alors mises en œuvre pour traiter ces risques ;
- l'AH possède une DTPH utilisée pour adresser toutes les exigences techniques identifiées dans la présente PH-DPH ;
- l'AH met à disposition des Abonnés et des Utilisateurs les éléments publics de sa DPH au sein du présent document pour qu'ils puissent en évaluer la conformité ;
- l'AH dispose d'une organisation adéquate pour l'approbation de la présente PH-DPH et la vérification de la concordance entre la DTPH et la PH-DPH (cf. chapitre 1.3.3) ;
- le responsable de l'AH garantit que les pratiques sont correctement mises en œuvre ;
- l'AH procède régulièrement à des audits de manière à s'assurer de la conformité des pratiques, y compris les responsabilités, à la DTPH (cf. chapitre 8) ;
- si l'AH a été certifié conforme avec la présente PH-DPH et si une modification envisagée à son initiative peut entraîner une non-conformité avec ladite PH-DPH ou avec la DTPH,

alors l'AH soumettra cette modification à l'organisme de certification indépendant pour avis.

3.5 Conditions Générales d'Utilisation

Les [CGU] du SH reprennent les grands principes décrits dans le présent document. Elles sont basées sur le modèle définit dans l'annexe B de [ETSI 319 421].

Ces [CGU] sont mises à disposition des Abonnés et des Utilisateurs sur le site de publication (cf. chapitre 2.2).

3.6 Conformité avec les exigences légales

3.6.1 Confidentialité des données professionnelles

Le présent document ne rajoute pas d'information par rapport à la [PG].

3.6.2 Données personnelles

Dans le cadre des services fournis par l'Autorité d'Horodatage régie par la présente PH-DPH, il n'y a pas de manipulation de données personnelles nécessitant une déclaration CNIL. L'ensemble des exigences de [PG] concernant les données personnelles est, de ce fait, non-applicable au périmètre du SH.

3.6.3 Dispositions concernant la résolution de conflits

Le contact habilité pour toute remarque, demande d'informations complémentaires, réclamation ou remise de dossier de litige concernant la présente PH-DPH est défini au chapitre 1.3.4.

En cas de litige relatif à l'interprétation, l'application et/ou l'exécution du présent document et faute de parvenir à un accord amiable, tout différend sera porté devant les tribunaux compétents de Paris.

3.6.4 Indemnités

Sans objet.

4 Exigences opérationnelles

4.1 Gestion des requêtes de Contremarques de temps

L'Abonné envoi sa requête de CT au SH du TSP MediaCert de Worldline. Cette requête doit respecter la norme [RFC 3161] en prenant en compte les restrictions de la norme [ETSI 319 422] et doit contenir une empreinte calculée par un algorithme conforme à l'état de l'art et autorisé par la PH-DPH (cf. chapitre 6.7).

L'AH fournit une CT en réponse à une demande contenant l'empreinte de la donnée à horodater. La fourniture de la CT n'excède pas quelques secondes [1], ceci afin de ne pas nuire ni dégrader l'ergonomie de l'application appelante.

La CT générée en réponse par le SH contient alors l'empreinte en question, une heure fiable et est signée par l'UH émettrice.

4.2 Fichiers d'audit

4.2.1 Type de données constituant les fichiers d'audit

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

L'AH conserve les informations pertinentes concernant les données délivrées et reçues, notamment afin de pouvoir fournir des preuves en justice. Parmi ces informations, on trouve les éléments relatifs :

- à l'administration du SH ;
- au fonctionnement du SH ;
- au cycle de vie des Bi-clés des UH ;
- au cycle de vie des Certificats d'UH ;
- aux évènements touchant à une synchronisation d'horloge des UH, y compris les évènements touchant à la détection de perte de synchronisation et à la re-calibration de l'horloge des UH.

L'AH régie par la présente PH-DPH se réserve le droit de conserver les CT générés par ses UH.

4.2.2 Période de conservation des fichiers d'audit

Sauf indication contraire, les fichiers d'audits sont conservés pendant une durée de dix (10) ans, soit sept (7) ans après l'expiration de la CT.

4.2.3 Protection des fichiers d'audit

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

[1] Ce temps de réponse correspond au temps écoulé entre la réception de la requête et la signature de la CT résultante.

4.3 Gestion de la durée de vie de la clé privée

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. Pour cela, des procédures opérationnelles et techniques sont mises en place et sont définies au sein de la DTPH.

La durée de vie des clés privées d'UH est définie au chapitre 6.10 du présent document.

4.4 Synchronisation de l'horloge

L'AH garantie que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée de une seconde.

Plus spécifiquement :

- La garantie de synchronisation avec UTC est réalisée à travers une synchronisation de l'horloge de l'UH avec les serveurs d'un laboratoire reconnu UTC(k) (cf. chapitre 0) ;
- 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 ;
- les horloges des UH sont protégées contre les menaces relatives à leur environnement qui pourraient aboutir à une désynchronisation avec le temps UTC en dehors de l'exactitude déclarée ;
- l'AH garantie que tout non-respect de l'exactitude annoncée par l'horloge interne d'une de ses UH sera détecté ;
- si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude déclarée, ou que les serveurs de temps ne sont plus disponibles, alors les CT ne seront plus générées tant que l'horloge de l'UH n'est pas resynchronisée ;
- l'AH garantit que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé comme notifié par l'organisme approprié. Le changement pour tenir compte du saut de seconde est effectué durant la dernière minute du jour où le saut de seconde est programmé.

4.5 Exigences du contenu d'une Contremarque de temps

Les CT émises par les UH de l'AH régie par cette PH-DPH sont générées dans les locaux sécurisés de Worldline et incluent un temps établit en conformité aux exigences de la section 4.4. Ces CT sont conformes à la norme [ETSI 319 422] et donc au standard [RFC 3161].

Chaque CT est signée par la clé privée, réservée à cet effet, de l'UH émettrice (cf. chapitre 6.3).

Ces CT sont constituées de la manière décrite au chapitre 7.2 du présent document.

4.6 Compromission de l'Autorité d'Horodatage

Dans le cas d'évènements qui affectent la sécurité du SH ou les CT émises ou dans le cas d'évènements qui sont susceptibles de le faire, l'AH garantit qu'une information appropriée est mise à la disposition des Abonnés et des Utilisateurs.

Parmi ces évènements, figurent notamment :

- la compromission, réelle ou suspectée, de la clé privée d'une UH ayant un Certificat émis par l'AH régie par cette PH-DPH ;
- la perte de connexion prolongée avec les serveurs de temps ;
- la perte détectée de calibrage de l'horloge d'une UH ayant un Certificat émis par l'AH régie par cette PH-DPH.

La [PG] définit les procédures et politiques à appliquer en cas d'incident.

En cas de compromission, de suspections de compromission, ou d'émission de CT erronés suite à une perte de calibration, l'AH notifiera les Abonnés et Utilisateurs impactés, ainsi que l'ANSSI. L'UH à l'origine de la compromission sera désactivée jusqu'à correction effective ou levée de la suspicion.

4.7 Fin d'activités

Comme défini dans la [PG], un plan de cessation d'activités est défini et maintenu pour l'AH. Il sera appliqué lorsque Worldline devra interrompre le SH régi par le présent document. Ce plan permet à l'AH de garantir que les dérangements potentiels aux Abonnés et aux Utilisateurs de CT seront réduits au minimum suite à la cessation d'activité du SH et assure en particulier la maintenance continue des informations nécessaires pour vérifier la justesse de CT.

Ce plan comprend entre autres les points suivants :

- avant de mettre fin à son SH, les procédures suivantes seront exécutées :
  - l'AH rendra disponible à tous ses Abonnés et Utilisateurs l'information concernant sa fin d'activité ;
  - l'AH prévient directement et sans délai le point de contact de l'organe de contrôle national (ANSSI) de la cessation d'activité ;
- lors de l'arrêt de son SH, les procédures suivantes seront exécutées :
  - l'AH formalise la fin de la contractualisation avec les Abonnés ;
  - l'AH demandera la révocation de l'ensemble de ses Certificats ;
  - les clés privées des UH seront détruites de telle façon que celles-ci ne puissent pas être recouvrées (cf. chapitre 6.6) ;
  - l'AH abrogera les autorisations données aux éventuels sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de génération des CT ;
  - l'AH transférera à Worldline ses obligations de maintien des fichiers d'audit et des archives nécessaires pour démontrer son fonctionnement correct durant une période de 10 ans minimum à compter de la fin effective d'activité ;
  - l'AH transférera à un Worldline ses obligations de rendre disponibles ses clés publiques ainsi que ces Certificats aux Utilisateurs pendant une période de 10 ans minimum à compter de la fin effective d'activité.

- l'AH prend les mesures nécessaires pour couvrir les dépenses pour accomplir les exigences susvisées dans le cas où l'AH tomberait en faillite ou pour d'autres raisons serait incapable de couvrir les dépenses par elle-même.

4.8 Révocation d'un Certificat d'Unité d'Horodatage

4.8.1 Raison de révocation

L'AH peut procéder à une demande de révocation d'un Certificat d'UH entre autres pour les raisons suivantes :

- fin de vie anticipée de l'AH ou de l'UH ;
- compromission ou suspicion de compromission de la clé privée de l'UH.

L'ensemble des raisons d'une demande de révocation d'un Certificat d'UH est décrit dans la [PC-DPC] de l'AC Horodatage émettrice du Certificat concerné.

4.8.2 Procédure de révocation

La procédure de révocation d'un Certificat d'Unité d'Horodatage du TSP MediaCert est interne et est spécifiée dans la DTPH. Celle-ci est conforme aux exigences décrites dans [PC-DPC] de l'AC Horodatage émettrice du Certificat concerné.

5 Exigences physiques et environnementales, procédurales et organisationnelles

5.1 Exigences physiques et environnementales

5.1.1 Situation géographique et construction des sites

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.1.2 Accès physique

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

Notamment, les systèmes critiques du service d'horodatage, en particulier les UH, sont opérés dans une zone sécurisée (cf. [PG]) utilisés par l'ensemble des Services de Confiance du TSP MediaCert.

En effet, des mesures de contrôle d'accès sont mises en place de façon à protéger physiquement les HSM de l'AH de tout accès non-autorisés, en particulier :

- au sein de l'environnement sécurisé où ils sont entreposés ;
- lors de leur éventuel stockage temporaire avant mise en production.

Cet environnement sécurisé protège physiquement et logiquement les systèmes et données du SH contre des accès non-autorisés pouvant entraîner une compromission.
En particulier, les mesures suivantes sont en place :

- chaque entrée et sortie de la zone sécurisée fait l'objet d'une traçabilité ;
- les entrée et sortie de la zone font l'objet d'une supervision indépendante ;
- toute personne ayant un accès non-permanent fait l'objet d'une surveillance par une personne en rôle de confiance dans toutes les zones sécurisées.

Seuls les personnels en rôle de confiance sont autorisés à accéder aux zones sécurisées.

5.1.3 Alimentation électrique et climatisation

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.1.4 Vulnérabilité aux dégâts des eaux

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.1.5 Prévention et protection incendie

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.1.6 Conservation des supports

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.1.7 Mise hors service des supports

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

Notamment, en cas de mise hors service d'un HSM, les clés d'UH sont effacées au préalable en s'appuyant sur les fonctions de « zeroization » du HSM.

Les équipements, données, supports et logiciels opérés dans la zone sécurisée ne peuvent être retirés du site sans autorisation.

5.1.8 Sauvegardes hors site

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.2 Exigences procédurales

5.2.1 Rôles de confiance

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.2.2 Nombre de personnes requises par tâche

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.2.3 Identification et authentification pour chaque rôle

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.2.4 Rôles exigeant une séparation des attributions

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.2.5 Gestion opérationnelle

L'AH s'assure que les composants du Système d'horodatage sont sûrs et correctement opérés, avec un risque minimal d'échec. De plus, l'AH met en place, sur le périmètre du service d'horodatage, un système de management de la qualité et de la sécurité du système d'information.

5.2.5.1 Échange de données et du logiciel

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.2.5.2 Mesures de sécurité techniques spécifiques aux systèmes informatiques

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.2.5.3 Mesures de sécurité réseau

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.2.5.4 Manipulation et sécurité des supports

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

Notamment, concernant la gestion et la conservation des supports, l'AH s'assure du suivi et de la sécurité des HSM protégeant les clés d'UH tout au long de leur cycle de vie en particulier, l'AH, par des mesures de sécurité organisationnelle, s'assure que les HSM n'ont pu être altérés :

- durant leur transport ;
- durant leur stockage temporaire avant leur installation sur le site sécurisé de production.

5.2.5.5 Planification du système

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

Notamment, l'AH assure une surveillance de sa capacité à traiter la volumétrie de demandes et réalise des projections afin d'assurer une montée en charge adéquate du service.

5.2.5.6 Qualification du système

L'Unité d'Horodatage établissant le lien entre la date et l'heure et les données horodatées est composée :

- d'une application d'horodatage ;
- d'un HSM conforme au chapitre 6.2.

L'AH procède à l'homologation de son SH afin d'assurer un niveau de sécurité adéquate.

5.2.5.7 Rapport d'incidents et réponse

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.2.6 Gestion des accès au Système d'horodatage

L'ensemble des exigences de la [PG] s'applique. En particulier, l'AH configure les systèmes opérant les UH de façon à ce que l'ensemble des comptes, applications, services, protocoles et ports non-nécessaires pour les Services d'Horodatages soient effacés ou désactivés.

5.2.7 Déploiement et maintenance

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.3 Exigences organisationnelles

5.3.1 Qualifications, compétences et habilitations requises

L'ensemble des exigences de la [PG] est applicable. En particulier, l'AH emploie un nombre suffisant de personnels pour opérer son service de confiance d'horodatage. Le personnel dispose des compétences techniques, de l'expérience et de la formation nécessaire pour réaliser les tâches nécessaires au fonctionnement de l'AH.

5.3.2 Procédures de vérification des antécédents

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.3.3 Exigences en matière de formation initiale

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.3.4 Exigences et fréquences en matière de formation continue

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.3.6 Sanctions en cas d'actions non autorisées

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Le présent document ne rajoute pas d'information par rapport à la [PG].

5.3.8 Documentation fournie au personnel

Le présent document ne rajoute pas d'information par rapport à la [PG].

6 Exigences de sécurité techniques

6.1 Exactitude du temps

L'AH garantit que les CT générées par ses UH ont un écart de temps maximum d'une (1) seconde par rapport au temps fournit par le laboratoire UTC(k)[2]. Cette précision est obtenue par synchronisation et contrôle des horloges des UH en se basant sur deux sources de temps différentes dont au moins une référence UTC(k).

6.2 Génération de clé

Les conditions de la génération des Bi-clés d'UH sont définies dans la [PG]. En particulier, les clés des UH sont générées dans les locaux de MédiaCert par au moins deux (2) personnes autorisées en rôle de confiance. Comme indiqué dans la politique générale, les clés d'UH sont générées dans un HSM. Ce HSM fait l'objet :

- d'une conformité critères communs à un niveau EAL4 ou supérieur ;
- d'une qualification au niveau renforcé par l'ANSSI.

Chaque UH ne possède qu'une clé privée active à la fois. Le renouvellement du Certificat sans renouvellement de la Bi-clé n'est pas autorisé par la présente PH-DPH. Les clés d'UH ne sont utilisées que dans les HSM qui ont été utilisés pour leur génération (cf. chapitre 6.5).

6.3 Certification des clés de l'Unité d'Horodatage

Les Certificats des UH régies par cette PH-DPH sont générés par l'AC Horodatage conformément aux exigences définies dans la [PC-DPC] qui lui est associée. L'AH se conforme par ailleurs aux obligations, définies dans la [PC-DPC] correspondante, qui lui incombe.

Lors de la délivrance d'un Certificat d'UH par l'AC Horodatage, l'AH vérifie l'ensemble de la chaîne du Certificat et en particulier :

- que le Certificat est bien émis par l'AC requise ;
- qu'il est conforme au gabarit attendu.

L'AH s'assure que l'UH ne peut être opérationnelle qu'une fois ces vérifications effectuées avec succès. En aucun cas, une UH de pourra générer des CT avant la vérification, l'installation et la publication de son certificat.

6.4 Protection des clés des Unités d'Horodatage

Le présent document ne rajoute pas d'information par rapport à la [PG].

6.5 Exigences de sauvegarde des clés des Unités d'Horodatage

[2] Pour des écarts de l'ordre de la seconde (généralement de quelques dizaines de nano-secondes au grand maximum), l'écart entre UTC et la source UTC(k) utilisée est jugé négligeable.

La sauvegarde des clés des UH est interdite par la présente PH-DPH.

6.6 Destruction des clés des Unités d'Horodatage

La clé privée de l'UH ne faisant pas l'objet de sauvegarde (cf. chapitre 6.5), la destruction de l'instance de la clé présente dans le HSM, via les fonctionnalités de ce dernier, permet sa destruction de façon définitive.

6.7 Algorithmes obligatoires

L'AH accepte les algorithmes de calcul d'empreintes numériques, par les Abonnés, compatibles avec les meilleures pratiques et recommandations de l'ANSSI et de la norme [ETSI 119 312]. En voici la liste :

- SHA-256 ;
- SHA-512.

La taille des Bi-clés et les algorithmes utilisés par les UH utilisées pour signer les CT sont conformes aux exigences [ETSI 119 312] :

Algorithme	Fonction de hachage	Taille (bits)
RSA	SHA-256	2048

MediaCert s'autorise à faire évoluer ces algorithmes en fonction de l'état de l'art de la cryptanalyse et des recommandations de l'ANSSI.

6.8 Vérification des Contremarques de temps

L'AH garantit que les Utilisateurs ont accès à l'information nécessaire pour vérifier la signature numérique des CT. Les Certificats d'UH sont notamment joints aux CT et disponibles sur le site institutionnel du *Trust Service Provider* MediaCert (conformément à la [PC-DPC]).

6.9 Durée de validité des Certificats de clé publique des Unités d'Horodatage

Les Certificats de clé publique des UH ont une durée de vie de trois (3) ans. L'AH garantit que la durée de vie de ces Certificats est conforme à l'algorithme et à la taille de clés associée utilisés conformément à [ETSI 119 312] et aux recommandations de l'ANSSI.

6.10 Durée d'utilisation des clés privées des Unités d'Horodatage

La durée d'utilisation des clés privées d'UH est inférieure à la durée de vie du Certificat associée (cf. chapitre 6.9).
La durée d'utilisation des clés privées d'UH est limitée en pratique à un (1) an afin de faciliter la vérification des jetons d'horodatage grâce à une période adéquate de validité du Certificat (cf. chapitre 6.9).
Le SH rejette automatiquement toute demande de CT si la limite de validité de la clé privée est dépassée.

7 Profil des Certificats et Contremarques de temps

7.1 Certificat d'Unité d'Horodatage

Les informations concernant le profil des Certificats d'UH sont disponibles dans la [PC-DPC].
Ces Certificats sont émis par une AC dédiée opérée par MediaCert en conformité avec la norme [ETSI 319 411-2] au niveau QCP.

7.2 Contremarques de temps

Champ	Description	Valeur
version	Version du format	1
policy	OID de la PH-DPH appliquée	1.2.250.1.111.20.2.1
messageImprint	OID de l'algorithme de hash des données à horodater	Identique aux valeurs inclues dans la demande
serialNumber	Identifiant unique de la CT. Cet identifiant peut être un nombre de 160 bits au plus.	Généré par l'UH
genTime	Temps au moment de la génération de la CT, synchronisé avec le temps UTC	Heure de l'UH au moment de la génération
accuracy	Précision déclarée de la CT conformément à la PH-DPH appliquée	1 seconde
ordering	Information d'ordonnancement	False
nonce	Donnée anti-rejeu	Identique à celui présent dans la demande (si présent)

8 Audit de conformité et autres évaluations

8.1 Fréquences et/ou circonstances des évaluations

Worldline, dans le cadre de la qualification de son SH, procède à un audit externe de Certification à la norme [ETSI 319 421] de l'AH tous les deux (2) ans par un organisme accrédité.

En complément, Worldline effectue un audit de surveillance (interne ou externe) entre deux (2) audits externe de Certification à la norme [ETSI 319 421].

8.2 Identités / qualifications des évaluateurs

8.2.1 Audit de certification

Le présent document ne rajoute pas d'information par rapport à la [PG].

8.2.2 Audit de surveillance

Le présent document ne rajoute pas d'information par rapport à la [PG].

8.3 Relations entre évaluateurs et entités évaluées

8.3.1 Audit de certification

Le présent document ne rajoute pas d'information par rapport à la [PG].

8.3.2 Audit de surveillance

Le présent document ne rajoute pas d'information par rapport à la [PG].

8.4 Sujets couverts par les évaluations

Le présent document ne rajoute pas d'information par rapport à la [PG].

8.5 Actions prises suite aux conclusions des évaluations

Le présent document ne rajoute pas d'information par rapport à la [PG].

8.6 Communication des résultats

Le présent document ne rajoute pas d'information par rapport à la [PG].

9 Annexes

9.1 Réglementations

Référence	Description
[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
[EIDAS]	REGLEMENT (UE) N°910 DU PARLEMENT EUROPEEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

9.2 Références documentaires

9.2.1 Réglementation technique

Référence	Description
[ETSI 119 312]	ETSI TS 119 312 v1.2.2 (2018-09) Electronic Signature and Infrastructures (ESI); Cryptographic Suites
[ETSI 319 401]	ETSI EN 319 401 v2.2.1 (2018-04) Electronic Signature and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI 319 421]	ETSI EN 319 421 v1.1.1 (2016-03) Electronic Signature and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps OID : 0.4.0.2023.1.1
[ETSI 319 422]	ETSI EN 319 422 v1.1.1 (2016-03) Electronic Signature and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[RFC 3161]	Network Working Group – August 2001 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
[RGS A5]	Politique d'Horodatage Type v3.0 Référentiel Général de Sécurité (RGS) version 2.0 – Annexe A5 Référence : RGS_v-2-0_A5
[QUALIF AH]	Services d'horodatage électronique qualifiés - Critères d'évaluation de la conformité au règlement eIDAS Agence nationale de la sécurité des systèmes d'information (ANSSI) Version 1.1 du 3 janvier 2017
[QUALIF PSC]	Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS Agence nationale de la sécurité des systèmes d'information (ANSSI) Version 1.2 du 05 juillet 2017

[ETSI 319 411-2]	ETSI EN 319 411-2 v2.2.2 (2018-04) Electronic Signature and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

9.2.2 Documentation Worldline

Référence	Description
[CGU]	Conditions Générales d'Utilisation Autorité d'Horodatage Référence : WLM-TSA-F089
[PC-DPC]	Politique de Certification – Déclaration des Pratiques de Certification TSP MediaCert Référence : WLM-TSP-F104 OID : 1.2.250.1.111.20.3.1.2
[PG]	Politique Générale du TSP MediaCert TSP MediaCert Référence : WLM-TSP-F094 OID : 1.2.250.1.111.20.1.1