CERTINOMIS
UNE MARQUE DE DOCAPOSTE

CGU Service d'Horodatage

Conditions générales d'utilisation

Résumé

Le présent document constitue les conditions générales d'utilisation du service d'horodatage de Certinomis. Ces conditions sont complétées par une politique d'horodatage, qui décrit de façon plus détaillée l'organisation et la mise en œuvre de ce service.

Version

Statut	Validé
Version	V. 1.1
Date d'enregistrement	26/09/2024
Responsable du document	Direction Générale Certinomis
Approbateur (s)	Autorité de Gestion des Politiques (AGP)
Nom fonctionnel	CGU Service d'Horodatage Certinomis

Diffusion : Publique

Table des matières

1. Définitions et abréviations

1.1. Définitions

Autorité de Certification (AC) - Entité émettant des Certificats après vérification de l'identité de la personne ou du représentant du système applicatif, ou de la procédure ayant mené à son identification. L'AC est responsable de l'ensemble des composantes matérielles, humaines et organisationnelles utilisées dans le processus de création et de gestion des Certificats.

Autorité d'Horodatage (AH) - Autorité responsable de la gestion de l'environnement d'horodatage et de la production des jetons d'horodatage de Certinomis sur les données qui lui sont présentées afin d'attester de l'existence de ces données à la date de la marque de temps. Il s'agit de Certinomis dans le cadre de la présente PH.

Commission d'Approbation des Politiques et Homologation (CAPH) - La CAPH de Certinomis est constituée de représentants désignés par Certinomis pour créer, contrôler le respect et faire évoluer la documentation des politiques régissant l'infrastructure des Services Électroniques de Confiance.

Contremarque de temps - Donnée 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) - Échelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 [TF.460-5].

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

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

Jeton d'horodatage - Voir contremarque de temps.

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

Opérateur de Service d'Horodatage (OSH) - Opérateur assurant les prestations techniques nécessaires au processus d'horodatage. Il est en charge du bon fonctionnement et de la sécurité des moyens informatiques et techniques. Il est en charge de la sécurité des personnels, des locaux et, plus généralement, du bon respect des procédures, toutes choses indispensables pour garantir un niveau de fiabilité.

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

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

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

Service demandeur - Entité demandant à l'AH la fourniture de service d'horodatage et ayant explicitement ou implicitement accepté les termes et conditions de cette fourniture.

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 final - Personne physique ou morale identifiée ou non qui reçoit par l'intermédiaire du service demandeur un jeton d'horodatage correspondant à la fourniture d'un service d'horodatage par l'AH.

1.2. Abréviations

AC	Autorité de Certification
AGP	Autorité de Gestion des Politiques
AH	Autorité d'Horodatage
CGU	Conditions Générales d'utilisation du service d'horodatage
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunications Standards Institute
LCR	Liste des Certificats Révoqués
IGC	Infrastructure de Gestion de Clés
OID	Object Identifier
OSH	Opérateur de Services d'Horodatage
PH	Politique d'Horodatage
PSHE	Prestataire de service d'horodatage
UH	Unité d'Horodatage
UTC	Coordinated Universal Time

2. Cadre d'application

L'horodatage électronique est un service de sécurité qui permet d'attester que des données sous forme électronique existaient bien à un instant donné. Ce service contribue à d'autres services à valeur ajoutée (lettre recommandée électronique, validation de dépôt d'une offre dans le cadre d'un appel d'offre, etc.).

L'horodatage électronique est réalisé sous le contrôle et sous la responsabilité d'une Autorité d'Horodatage (AH). Le service d'horodatage électronique est sollicité par des « services demandeurs », qui ont en charge la fourniture, à leurs « utilisateurs finaux », des services à valeur ajoutée qui intègrent le service d'horodatage électronique. Ainsi, l'AH est en relation directe avec les services demandeurs, et indirectement avec les utilisateurs finaux.

Un service d'horodatage est un service électronique de confiance. Il est nécessaire que les services demandeurs et, indirectement, les utilisateurs finaux puissent avoir confiance dans l'AH pour la fourniture de services d'horodatage fiables. Cette fiabilité nécessite la mise en œuvre de moyens techniques, humains et organisationnels adéquats.

L'AH s'engage et est responsable vis-à-vis des services demandeurs sur la mise en œuvre de ces moyens.

L'objet des présentes conditions d'utilisation est résumé, de façon claire et accessible aux services demandeurs et aux utilisateurs finaux, les engagements pris par l'AH dans sa *Politique d'Horodatage*.

L'Autorité d'horodatage est établie en France.

3. Coordonnées de l'autorité d'horodatage

3.1. Point de contact

L'adresse de l'Autorité d'horodatage est la suivante :

Docaposte Certinomis - Direction Générale

45-47 Boulevard Paul Vaillant-Couturier

94677 Ivry sur Seine

Les demandes d'informations et réclamations pourront être adressé par e-mail à l'adresse suivante :

- ld-politiquecertification@certinomis.fr

3.2. Identification

L'Autorité d'horodatage est identifiée comme suit dans les certificats des unités d'horodatage (où XXX désigne un numéro de série spécifique à l'unité d'horodatage) :

CN = CERTINOMIS_UNITE_HORODATAGE_ 81610_0050000XXX_XXX

SERIALNUMBER = N° unique

OU = 0002 433998903

2.5.4.97 = NTRFR-433998903

O = DOCAPOSTE CERTINOMIS

L = Ivry sur Seine

S = 94

4. Politique d'horodatage

Les présentes CGU correspondent à la PH identifiée par l'OID suivant :

1.2.250.1.86.5.1.1.1.1

5. Utilisation des jetons d'horodatage

5.1. Algorithmes de production du jeton d'horodatage

Les algorithmes suivants sont acceptés pour l'empreinte numérique des données horodatées (cette empreinte est réalisée par le demandeur et transmise dans la requête) :

- SHA-256 ;
- SHA-384 ;
- SHA-512.

Les contremarques de temps sont signées en utilisant des algorithmes et des longueurs de clés conformes à l'état de l'art et aux exigences du [RGS]. Les bi-clés RSA des unités d'horodatage ont une longueur de 4096 bits (RSA) ou 384 bits (ECC). La signature des contremarques utilise une fonction de hachage de la famille SHA-2.

5.2. Vérification d'un jeton d'horodatage

La vérification d'un jeton d'horodatage est réalisable de façon autonome par le service demandeur pendant la période de publication en ligne des LCR délivrées par l'AC émettant les certificats d'horodatage de l'AH :

- La vérification d'un jeton d'horodatage s'effectue à partir des informations publiées par l'AC émettrice du certificat d'UH qu'il comprend ;
- Le service demandeur doit vérifier la validité de la signature électronique du jeton d'horodatage ainsi que la validité du certificat de signature (non révocation et non expiration à la date de vérification).
- Les LCR de l'AC, qui comportent tous les certificats révoqués depuis le début de l'existence de l'AC, sont accessibles sur son site Internet pendant leur période de publication ;
- La période de vérification autonome d'un jeton d'horodatage par le service demandeur est au minimum d'un an après sa date d'émission.

Au-delà de cette période, le service demandeur peut vérifier un jeton d'horodatage par requête expresse auprès de l'AH. Les conditions financières de traitement de cette requête faisant intervenir un huissier sont détaillées dans le contrat de service liant l'AH et le service demandeur.

6. Limitations

6.1. Précision des jetons d'horodatage

La précision de l'heure contenue dans le jeton d'horodatage vis-à-vis de l'échelle de temps UTC est d'une seconde.

6.2. Enregistrement des informations concernant l'exploitation des services d'horodatage

L'AH s'assure que toute donnée concernant l'exploitation des services d'horodatage est enregistrée pour une période de 10 ans, en particulier pour fournir des preuves légales.

6.3. Autres limitations

Les données transmises dans une requête de jeton d'horodatage restent de la responsabilité des services demandeurs.

7. Obligations

7.1. Obligations des services demandeurs

Le service demandeur s'engage à vérifier la validité d'un jeton d'horodatage dès sa réception selon la procédure de vérification décrite dans la PH. Le service demandeur s'engage également à vérifier que les données sur lesquelles portent le scellement d'horodatage sont bien celles transmises pour horodatage.

L'archivage des jetons d'horodatage émis pour un service demandeur relève de la responsabilité dudit service demandeur. Par défaut, le service d'horodatage ne réalise aucun archivage des jetons d'horodatage produits. À la demande du client, moyennant des accords contractuels adéquats, le service d'horodatage peut fournir un service d'archivage des jetons d'horodatage générés.

7.2. Obligations des utilisateurs finaux

Les utilisateurs finaux n'ont pas d'obligation vis-à-vis de l'AH.

Il leur est cependant recommandé de valider (ou faire valider par les services demandeurs) les jetons d'horodatage. Dans ce cas, ils doivent appliquer les procédures de vérification de la validité des jetons d'horodatage définies dans au chapitre 8 des présentes CGU.

8. Vérification des jetons d'horodatage

La procédure de vérification de la validité d'un jeton d'horodatage doit au minimum permettre de garantir que :

- Le jeton d'horodatage émane bien des services d'horodatage de l'AH concernée par la présente PH en contrôlant :
  - La provenance du certificat d'horodatage (i.e. de l'AC émettrice par rapport à celle attendue) ;
  - La correspondance du champ OID du jeton d'horodatage (Champ *Policy* de *TSTInfo*) avec l'OID de la PH ;
- La signature apposée sur le jeton d'horodatage est correcte (vérification de l'intégrité du jeton d'horodatage) ;
- Les attributs du certificat d'horodatage sont bien spécifiques à l'horodatage ;
- Le certificat d'horodatage est valide en contrôlant :
  - Sa non-révocation auprès de l'AC émettrice (interrogation de CRL) ;
  - La signature apposée sur le certificat par l'AC émettrice (vérification de l'intégrité des données du certificat) ;
  - La période de validité du certificat ;
- Les certificats de l'ensemble de la chaîne de certification sont valides ;
- L'empreinte présente dans le jeton d'horodatage est bien celle des données présentées au Service d'horodatage.

Les certificats des UH sont mis à disposition des utilisateurs sur le site *https://www.certinomis.fr/nos-certificats-racines*.

Les certificats de l'AC émettrice des certificats d'UH et l'ensemble de la chaîne de certification sont disponibles sur le site *https://www.certinomis.fr/* et rappelés ci-dessous.

8.1. Certificat racine

Version	3 (0x2)
Serial Number	1 (0x1)
Signature Algorithm	sha256WithRSAEncryption
Issuer	C=FR, O=Certinomis, OU=0002 433998903, CN=Certinomis - Root CA
Not Before	Oct 21 09:17:18 2013 GMT
Not After	Oct 21 09:17:18 2033 GMT
Subject	C=FR, O=Certinomis, OU=0002 433998903, CN=Certinomis - Root CA
Public Key Algorithm	rsaEncryption
Public-Key	(4096 bit)

8.2. Certinomis AC PRIME

Cette AC a signé les certificats des Unités d'horodatage jusqu'au 9 septembre 2020.

Version	3 (0x2)
Serial Number	03:ba:10:ff:1a:1d:bc:0d:05:0d:4b:21:42:46:2f:3c:0b:80:26:b8
Signature Algorithm	sha256WithRSAEncryption
Issuer	C=FR, O=Certinomis, OU=0002 433998903, CN=Certinomis - Root CA
Not Before	Oct 21 10:15:47 2013 GMT
Not After	Oct 21 10:15:47 2023 GMT
Subject	C=FR, O=Certinomis, OU=0002 433998903, CN=Certinomis - Prime CA
Public Key Algorithm	rsaEncryption
Public-Key	(4096 bit)

8.3. Certinomis AC TIMESTAMP

Cette AC signe les certificats des Unités d'horodatage depuis le 9 septembre 2020.

Version	3 (0x2)
Serial Number	f3:18:e8:a4:f6:b7:9c:58:77:75:aa:6c:d5:44:df:42:58:fe:4f:74
Signature Algorithm	sha256WithRSAEncryption
Issuer	C=FR, O=Certinomis, OU=0002 433998903, CN=Certinomis - Root CA
Not Before	Oct 18 09:59:31 2017 GMT
Not After	Oct 18 09:59:31 2033 GMT
Subject	CN=Certinomis - Timestamp CA, OID.2.5.4.97=NTRFR-433998903, O=Certinomis, C=FR
Public Key Algorithm	rsaEncryption
Public-Key	(4096 bit)

9. Politiques et normes

Le service d'horodatage émet ses jetons conformément aux normes suivantes :

- Le standard *ETSI EN 319-421v1.1.1 (2016-03)*;
- La politique nommée « Best Practices Policy for Time-Stamp (BTSP) » décrite dans les spécifications de l'ETSI EN 319 421 et identifiée par l'OID suivant : 0.4.0.2023.1.1
- Le Règlement No 910/2014 du Parlement européen et du conseil du 23 juillet 2014 (règlement eIDAS)
- La *Politique d'horodatage type* du R.G.S., *Référentiel Général de Sécurité – Annexe A5 – PH Type*, version 3.0 du 27 février 2014

9.1. Politique d'horodatage

La PH est disponible sur le site de Certinomis à l'URL suivante :

https://www.certinomis.fr/nos-certificats-racines/nos-politiques-de-certification

9.2. Durée de validité

En cas de changement de la PH ayant un impact sur les utilisateurs et abonnés du service, ceux-ci sont avertis au moins un mois à l'avance de la nature et la portée de ces changements à travers la publication, sur le site ci-dessus, de la future version de la PH.

L'organisme de qualification indépendant retenu pour valider la conformité de la PH avec les exigences du R.G.S. et du règlement eIDAS est la société LSTI (453 867 863 RCS Saint-Malo).

10. Conformité avec les exigences légales

10.1. Droit applicable

Le présent document est régi par la loi française.

10.2. Règlement des différends

Tout litige qui surviendrait concernant l'interprétation et l'exécution de la présente Politique d'Horodatage devra faire l'objet d'une tentative de règlement amiable en contactant l'Autorité d'horodatage par courriel ou en utilisant le formulaire en ligne mis à disposition des utilisateurs du service (voir 3.1 des présentes). À défaut de règlement amiable, le litige sera soumis au droit français, et porté devant le tribunal compétent dans le ressort de la cour d'appel de Paris statuant en droit français.