PROVINCE NORD

Plate-forme de dématérialisation des Marchés Publics

Province Nord – Nouvelle Calédonie

Politique d'Horodatage

OID n°1.3.6.1.4.1.44394.2.1.1.1

Table des mises à jour du document :

Date	Evolution	Version
18 juillet 2014	Rédaction initiale	v 1.0
25 août 2014	Corrections diverses – remplacement des certificats	v 1.1
26 novembre 2014	Finalisation du document	v 2.0

SOMMAIRE

1 Présentation générale du service d'horodatage

La Province Nord de Nouvelle Calédonie met en œuvre un service d'horodatage au sein de son infrastructure informatique pour ses projets de dématérialisation internes et externes.

Le service d'horodatage est mis en œuvre par une Unité d'Horodatage (UH) qui génère des contremarques de temps relatives à des empreintes de signatures ou de contenus.

L'UH est placée sous la responsabilité d'une Autorité d'Horodatage (AH). En l'état actuel du présent document, l'AH est la Province Nord de Nouvelle Calédonie, qui délivre ainsi des contremarques de temps dans le cadre de ses projets de dématérialisation.

Le service d'horodatage constitue une prestation technique qui a pour vocation :

- d'être mise à la disposition des besoins internes à la Province Nord de Nouvelle Calédonie ;
- d'être mise à la disposition d'acteurs économiques ou d'autres administrations externes à la Province Nord de Nouvelle Calédonie.

Une contremarque de temps permet de garantir l'antériorité, par rapport à la date indiquée dans la contremarque de temps, d'une empreinte numérique qui a été envoyée au service d'horodatage. La contremarque de temps est signée par l'AH à l'aide de l'UH. A aucun moment ni l'AH ni l'UH ne connaissent le contenu correspondant à l'empreinte numérique envoyée au service d'horodatage.

Le présent document, identifié par un Object Identifier (OID) spécifique, constitue la Politique d'Horodatage (PH) de l'AH. Il définit les exigences auxquelles l'AH se conforme dans la mise en place et la fourniture des contremarques de temps et indique l'applicabilité d'une contremarque de temps à une classe d'application avec des exigences de sécurité communes.

Le présent document pourra, de manière optionnelle, être ultérieurement 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 décrit les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la PH, en particulier les processus qu'une UH emploie pour la génération des contremarques de temps et le maintien de l'exactitude de ses horloges. L'AH peut mettre en œuvre plusieurs UH pour supporter son service d'horodatage.

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

L'OID de la présente politique d'horodatage est 1.3.6.1.4.1.44394.2.1.1.1.

2 Liste des acronymes utilisés dans le document

La liste des acronymes utilisés dans ce document est la suivante :

- AC Autorité de Certification
- AE Autorité d'Enregistrement
- AH Autorité d'Horodatage
- ANSSI Agence Nationale de la Sécurité des Systèmes d'Information
- CGU Conditions Générales d'Utilisation
- DPC Déclaration des Pratiques de Certification
- DPH Déclaration des Pratiques d'Horodatage
- HSM Hardware Security Module
- IGC Infrastructure de Gestion de Clés
- OID Object Identifier
- LCR Liste de Certificats Révoqués
- PC Politique de Certification
- PEM Privacy-Enhanced Electronic Mail
- PH Politique d'Horodatage
- RFC Request For Comments
- UH Unité d'Horodatage
- URL Uniform Resource Locator
- UTC Coordinated Universal Time

3 Définitions des termes utilisés dans ce document

- **Autorité de Certification (AC)** : entité qui délivre les certificats utilisés par l'AH pour signer les contremarques de temps. Dans la présente politique, ces certificats sont délivrés par l'AC « Sunnystamp Timestamping CA 2 ».
- **Autorité d'Enregistrement (AE)** : entité qui vérifie que les demandeurs ou les porteurs de certificat sont identifiés et que les contraintes liées à l'usage d'un certificat sont remplies, tout cela conformément à la politique de certification. Dans la présente politique, l'autorité d'enregistrement est la société « Lex Persona ».
- **Autorité d'Horodatage (AH)** : entité organisationnelle responsable de la délivrance de contremarques de temps.
- **Certificat (d'horodatage) :** fichier électronique attestant qu'une clé publique est associée au processus d'horodatage mis en œuvre par l'UH qui accède à la clé privée correspondant à la clé publique. Il est délivré par une AC. En signant le certificat, l'AC valide le lien entre le processus d'horodatage et la clé publique. Le certificat a une période de validité limitée. Dans la présente politique le processus d'horodatage est dénommé « Province Nord Nouvelle Calédonie Timestamping » et donc le nom commun figurant sur le certificat d'horodatage est « Province Nord Nouvelle Calédonie Timestamping Unit 1 » pour identifier l'UH utilisée.
- **Certificat parent** : certificat d'identité numérique de l'entité qui a délivré le certificat dont il est le parent.
- **Certificat racine** : certificat d'identité numérique pris comme racine de la chaine de certification d'un certificat. Un certificat racine est généralement auto-signé (c'est-à-dire délivré par l'entité qu'il représente) mais pas obligatoirement. Un mécanisme de vérification ne vérifie pas le statut de révocation d'un certificat racine (mais uniquement ses attributs, sa validité et son intégrité).
- **Client du service** : utilisateur du service d'horodatage qui sollicite le service en lui envoyant une empreinte de signature ou de contenu à horodater.
- **Conditions Générales d'Utilisation** : termes décrivant les règles d'utilisation d'un service (application, site Web, fichier informatique, etc.) permettant à son utilisateur d'en connaître l'objet, ses délivrables et ses contraintes.
- **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)** : échelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 [TF.460-5].
- **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 son service d'horodatage et en conformité avec la politique d'horodatage qu'elle s'est engagée à respecter.
- **Format PEM** : format de représentation textuelle (en base 64) d'un certificat et/ou des clés qui le composent.
- **Hardware Security Module** : composant matériel spécialisé permettant d'effectuer des calculs cryptographiques de manière protégée et en minimisant au maximum le risque de compromission des clés de signature ou de chiffrement / déchiffrement.

- **Identificateur d'objet (OID)** : identificateur alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.
- **Infrastructure de gestion de clés (IGC)** : ensemble de composants, fonctions et procédures dédiés à la gestion de clés cryptographiques asymétriques et des certificats associés. Une IGC peut être composée d'un service de génération de certificats, d'un service d'enregistrement, d'un service de publication, etc.
- **Jeton d'horodatage** : voir « contremarque de temps ».
- **Liste de Certificats Révoqués (LCR)** : liste de certificats ayant fait l'objet d'une révocation.
- **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. Dans la présente politique, le module d'horodatage désigne le produit LP7Timestamp de la société Lex Persona.
- **Politique de Certification** : ensemble de règles définissant les exigences auxquelles l'AC, ainsi que tous les autres intervenants aux services de certification, se conforment dans la mise en place des prestations de certification. Dans le présent ce terme n'est utilisé que pour définir la politique de certification de l'AC ayant délivrée le ou les certificat(s) d'horodatage utilisé(s). L'OID de cette politique est 1.3.6.1.4.1.44394.2.1.1.1.
- **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'applications avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les clients émetteurs de contremarques de temps et les utilisateurs de contremarques de temps. Dans la présente politique l'OID vaut 1.3.6.1.4.1.44394.2.1.1.1.
- **Request For Comments** : demande de commentaires, sous la forme d'un document officiel numéroté décrivant les aspects techniques d'Internet, ou de différents matériels informatiques. Certaines RFC, comme la RFC3161 citée dans ce document deviennent des standards et sont référencées comme telles.
- **Révocation (d'un certificat)** : opération demandée par le porteur, par son AC, ou son AE et dont le résultat est la suppression de la caution de l'AC sur un certificat donné, avant la fin de sa période de validité.
- **Service d'horodatage** : ensemble des prestations nécessaires à la génération et à la gestion de contremarques de temps.
- **Unité d'Horodatage (UH)** : ensemble matériel et logiciel en charge de la création de 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]).
- **Utilisateur (destinataire) de contremarque de temps** : entité destinatrice (personne ou système) qui fait confiance à une contremarque de temps émise sous une PH donnée par une AH donnée.
- **Validation (de certificat)** : opération de contrôle de l'intégrité, de la validité et du statut de révocation d'un certificat.

4 Type d'applications concernés par la PH

Les applications concernées par cette PH sont dans un premier temps celles relatives au domaine des procédures de dématérialisation des réponses aux marchés publics de la Province Nord de Nouvelle Calédonie.

Le service d'horodatage constitue une prestation technique qui a pour vocation :

- d'être mise à la disposition des besoins internes à la Province Nord de Nouvelle Calédonie ;
- d'être mise à la disposition d'acteurs économiques ou d'autres administrations externes à la Province Nord de la Nouvelle Calédonie.

En l'état, le service d'horodatage de la Province Nord de Nouvelle Calédonie sera principalement utilisé par les applications informatiques de la Province Nord, et mis à disposition auprès des utilisateurs internes et externes pour leur permettre d'horodater des signatures et / ou des contenus de manière fiable.

5 Structure des contremarques de temps définis par la PH

La contremarque de temps est un fichier signé qui contient en particulier :

- la valeur de l’empreinte objet de la contremarque de temps et l'algorithme d’empreinte qui a été utilisé ;
- l'identifiant de la PH sous laquelle la contremarque de temps a été générée ;
- la date et le temps UTC de la signature de la contremarque de temps ;
- le certificat de l’UH qui a généré la contremarque de temps.

6 Modification de la PH

La présente PH est la propriété exclusive de la Province Nord de Nouvelle Calédonie. Elle pourra être revue à l'occasion de l'évolution du service et/ou chaque fois qu'il sera nécessaire d'assurer sa conformité à l'état de l'art, et si besoin est, aux évolutions de la réglementation.

Les coordonnées des entités responsables de la présente PC sont les suivantes :

- Organisme responsable

  Province Nord, Koné, Nouvelle Calédonie.

- Personne physique responsable

  Monsieur Bernard Sautet, Direction des Systèmes d'Information, Province Nord, Koné, Nouvelle Calédonie.

7 Dispositions de portée générale

7.1 Obligations de l’AH

L'AH s’assure de la conformité des exigences et des procédures prescrites dans cette politique.

L'AH garantit l'adhésion aux obligations complémentaires indiquées dans la contremarque de temps ou bien directement ou bien incorporées par référence.

L'AH s’engage à remplir tous les engagements stipulés dans ses CGU (voir paragraphe **Erreur ! Source du renvoi introuvable.**).

7.2 Obligations du Client du service

Le Client du service émetteur de contremarques de temps peut accéder à ce service directement par le biais de requêtes HTTP conformes au protocole [RFC3161].

7.3 Obligations de l'Utilisateur destinataire

L’utilisateur destinataire d’une contremarque de temps, en cas de vérification, doit :

- Vérifier que la contremarque de temps a été correctement signée, et que le certificat de l’UH était valide et non révoqué à l'instant de la vérification.
- Tenir compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la présente PH.

7.4 Obligations spécifiques de l'AC fournissant les certificats

Le certificat de clé publique délivré à l'UH est confectionné par une AC qui respecte les exigences du niveau de sécurité une étoile (*) de la PC Type "Cachet Serveur" du RGS, à l’exception du « Hardware Security Module » (HSM) utilisé qui est uniquement de type logiciel.

7.5 DPH

Au niveau des exigences présentées par cette PH, il n'est pas fait pour l’instant de référence à une DPH.

8 CGU

L'AH impose aux utilisateurs émetteurs et destinataires de contremarques de temps des CGU qui comportent les éléments suivants :

- Une information sur un point de contact pour l'AH (voir paragraphe 6) ;
- Une référence (URL) de la PH : https://www.marchespublics.province-nord.nc;
- Au moins un algorithme d'empreinte qui peut être utilisé pour représenter la donnée à horodater : SHA256 ;
- La période de temps minimum, hors cas de révocation, durant laquelle les contremarques de temps seront vérifiables : 2 ans ;
- L'exactitude du temps dans les contremarques de temps par rapport au temps UTC : 1 seconde ;
- Les limitations sur l'utilisation du service d'horodatage (voir paragraphes □, 7.2 et 7.3).
- Des obligations supplémentaires éventuelles qui pour des raisons contractuelles en termes de fourniture de service ne font partie de la PH ;
- L'information sur la manière de vérifier les contremarques de temps de telle façon que l'utilisateur de contremarques de temps puisse "raisonnablement avoir confiance" dans les contremarques de temps ainsi que les restrictions possibles sur leur période de validité : cette information est constituée du ou des certificats d'horodatage et de leur chaine complète de certification ; ces informations sont fournies au format PEM en fin de paragraphe ;
- La période de temps pendant laquelle les fichiers d'audit de l'AH sont conservés : 5 ans.

Certificat d'horodatage :

```
-----BEGIN CERTIFICATE-----

MIIEiDCCA3CgAwIBAgIIN9WmhDgH0ZkwDQYJKoZIhvcNAQELBQAwYzELMAkGA1UE
BhMCRlIxFDASBgNVBAoMC0xFWCBQRVJTT05BMRcwFQYDVQQLDA4wMDAyIDQ4MDYy
MjI1NzElMCMGA1UEAwwcU3VubnlzdGFtcCBUaW1lc3RhbXBpbmcgQ0EgMjAeFw0x
NDA4MjUxNDE3MDJaFw0xOTA4MjUxNDE3MDJaMIGKMQswCQYDVQQGEwJGUjENMAsG
A1UEBwwES29uZTEWMBQGA1UECgwNUHJvdmluY2UgTm9yZDEUMBIGA1UECwwLMDE0
NDQwMi4wMDExPjA8BgNVBAMMNVByb3ZpbmNlIE5vcmQgTm91dmVsbGUgQ2Fsw6lk
b25pZSBUaW1lc3RhbXBpbmcgVW5pdCAxMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA7LbK4YQSqu9RZJnEtzFlsgviTa5tDwNAyAugGMEeO/fHBAWyNGS/
pTo6Yb/M3vKpLGSNWzWUHLF5xB1BeIlKEOe3vBtj6STl/NWb1HQloJftn7qZnFFK
htko7auSLhMctKHkTgjDWA2/4UJnlPNiBGGv6Lnxp15qPsJouskPbNjyP5Xv3Xz4
VtTHpjl6pcdH4PB8cEk9Vvue1xYAHAheT7yB6z0qejKf38hH9A8o817HojICTZPK
/YRyw7KiCeVRnLVMJdy37erUjcMKEjfXMktPxhOlvK6YPAfzhROYryMaMN+VfaEw
cWyUsPJfLXMk3pHTMPU+ZDnM2uLanV8dGQIDAQABo4IBFjCCARIwHQYDVR0OBBYE
FPlWQ54pFMz6Yvg6XI19vXajPK6MMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgwFoAU
Gc8DFE/FMbvXc1a7cuL0FkbGb18wSAYDVR0gBEEwPzA9Bg0rBgEEAYGwDgYAFQIB
MCwwKgYIKwYBBQUHAgEWHmh0dHBzOi8vcGtpLnN1bm55c3RhbXAuY29tL2NwczBQ
BgNVHR8ESTBHMEWgQ6BBhj9odHRwOi8vcGtpLnN1bm55c3RhbXAuY29tL2NybHMv
c3VubnlzdGFtcC10aW1lc3RhbXBpbmctY2EtMi5jcmwwDgYDVR0PAQH/BAQDAgeA
MBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMA0GCSqGSIb3DQEBCwUAA4IBAQCcPeM0
165rKJTXJ5cgi4Jdct22ihwMG7D0iOkZUezwen/ULRZpQjzT5vHzqwdUEHZEWXWH
ftfeF1PoINBaWisFNxSA7exTEJ88iwXW2RY+j/x2QaK+btKRNRQBrNTmnlvoHLo7
4AYahkf/ZCw9ksY7uaYKHrbTjRvVu/HQmc2lyJwe8r5GoHxEJnJjy5pcTClZg7iP
FkV4I9MgzPT+oiBRoaov/16yhOvQBabdsfecev+MDrEK0uLbkgvOz6hol4BXk6uq
ojV8berG+jf3JGdxT0M039e+lwnKpqfylItjRbX92H0+mBucxZVp2kJx64B1lntk
X2FXe3hoLq9N4Edf
-----END CERTIFICATE-----
```

Certificat parent :

```
-----BEGIN CERTIFICATE-----
MIIEtDCCApygAwIBAgIINXNe7TGn1WQwDQYJKoZIhvcNAQELBQAwWTELMAkGA1UE
BhMCRlIxFDASBgNVBAoMC0xleCBQZXJzb25hMRcwFQYDVQQLDA4wMDAyIDQ4MDYy
MjI1NzEbMBkGA1UEAwwSU3VubnlzdGFtcCBSb290IENBMB4XDTE0MDgyNTEzNDQx
MVoXDTI0MDgyNTEzNDQxMVowYzELMAkGA1UEBhMCRlIxFDASBgNVBAoMC0xFWCBQ
RVJTT05BMRcwFQYDVQQLDA4wMDAyIDQ4MDYyMjI1NzElMCMGA1UEAwwcU3Vubnlz
dGFtcCBUaW1lc3RhbXBpbmcgQ0EgMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAK7Yg5wFG7ajEnLvQWDvwHix8u2RGOP01y/W9IG74Ho1t+xC4odSzyfm
4UX0zfy77Ak5lbexNkAs36xOJ7Q/2oPdJxMZOnpZXzPtwja3RARMKVz9oAylVu0X
uvYBkvg5NaoOMH6uvc5iRp+CZIkf/+u32EKB3cFB9AxMkp5JzCXhW2bWyZ9iXxid
Likd7Y+sgXNxJXPClSCjX55I2EP1jkUF1+UKJJHxIOPXw06j6z8+jctV5ONfiD+U
+m32wmhez9vm0Ncsw33i3z44Pb77KMBBHj5IfvIND4kz3324vfQnPzSf38OkXh0F
rTgboYdTwtXZd5YRnIQC8WvQjBy/y0sCAwEAAaN2MHQwHQYDVR0OBBYEFBnPAxRP
xTG713NWu3Li9BZGxm9fMA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgwFoAUATpj
f2+z6nSCYY884hDjNAJJ/ogwEQYDVR0gBAowCDAGBgRVHSAAMA4GA1UdDwEB/wQE
AwIBBjANBgkqhkiG9w0BAQsFAAOCAgEAdQFX1PoLQUgcUzvn11lQLagtVERi+LVe
J88OY0ub9I5eDY4FACmshSIBRNBHb5OW4hWyvbtW13OUwC98rpHGzQeXuflh6i/7
V5FLS5P9vMAmOzU98UnqYHdsrcwP1NjrdHRgrASzhu3oPA1bd9EqlHPocXmLqud+
6PX3QqdaJA5F9OCRCXKBL4khfGmAormQPM3rx+zPdJCyunXzNW/BDoyZkGfGDxt5
6jumcskiVRm+24lPlF6uoiQwfuJuwImhMcz4L1rchfV3jM1FqiHwtcUCJZ7VJv+S
Knd3ZoEZLY3kNBqcavHne0KgzLgDc7F+ALmoErPBWU142aTOjfDMMGstZ+WF728z
+Qi2SS+p4PocZ3TLJPOsgciqYk2JCaoqBCCEq5J48BaRLXA1w4GJmxQHTduH2dGJ
YhMQUAgDPDz2TDQUWA2Z9zslc6rMgkQzao+e8YHyeQF75zf66M0s0l3X2trosUxW
kH39Pj2TEOL4iu9ZFoDQXv3VHDiavo8ziz8RELYYuxZM1fgG2UrmUh87z5Xr0clk
nABNXC1Wspk2zj4CFMly+l60VUXnrfelNZnTYgRkzs4tTjCd25QnV02owApjY6oY
0J/7j1ooFUAz9BU9kP2xSgjtBNq5i0q+nUGiV8gtMphRQ1lkbbFTjOlqtCdHsgWn
D4nMNYLwvrA=
-----END CERTIFICATE-----
```

Certificat racine :

```
-----BEGIN CERTIFICATE-----
MIIFlzCCA3+gAwIBAgIIMwWVcAp9M4swDQYJKoZIhvcNAQELBQAwWTELMAkGA1UE
BhMCRlIxFDASBgNVBAoMC0xleCBQZXJzb25hMRcwFQYDVQQLDA4wMDAyIDQ4MDYy
MjI1NzEbMBkGA1UEAwwSU3VubnlzdGFtcCBSb290IENBMB4XDTExMTAyNjEzMjYy
NVoXDTMxMTAyNjEzMjYyNVowWTELMAkGA1UEBhMCRlIxFDASBgNVBAoMC0xleCBQ
ZXJzb25hMRcwFQYDVQQLDA4wMDAyIDQ4MDYyMjI1NzEbMBkGA1UEAwwSU3Vubnlz
dGFtcCBSb290IENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAoKyO
Ex+rvhXgXfhviW+MAi022izm5mlmiUTeE4ykhpasrjxnkvXRoAoB8L+enSfip9BM
AKRrVBm7mk+JcPJhf53bRlIbolT50tt9SysuNYo8rCrLS6G3Aof3KFNuU1Ke/OED
vu8m7wOuREdfORTrvJ1hMckYgWC3HNRov/9J8iesA3b95mYbus0FDxJgplS90HlF
e8bN9lI1pZEtR2m6590+30Hy1eWDLUigX6uYcj8M59xS7YIaslZAvehA6rV4D3Ae
DpQjNrw0QlxFEczS/ATx4dKr+8Rkr2/DY7Tk1jnhrEM3E0hX9a2e2m2/PCfKslYQ
mtDISAR1+7jEa6DOoVua19HkFgCt8YdHy9tt9o/l/Th7TWXtptWpc2a2VHfNluRU
igAPryLfmbggBIfsFz8Iz4OHE5EAMpoYwyvnL0poy9XQ2XfsVxbq0njQqJSyQ6Tu
L0+GY9noH94KZsmzBpwV+cCaKdTsBW807TZXFwm2YioTT5mOkJB99vranmJR8Kui
XB/ARJeS+FMLGMe1HhEwebSxNeWyJvFAMTgNwbyyBuaKXIiF3BBRDPOg2T8sw9VM
Mg2sFEsq9cavxMJhHAGM0UGXDO8kDIvLrmBSeKuAcrEuip6Om4qeC30YEZ24+uI2
hgFYvRTnfon6fCHDE6xFR/RcfE6dsv3Y1JiUjA0CAwEAAaNjMGEwHQYDVR0OBBYE
FAE6Y39vs+p0gmGPPOIQ4zQCSf6IMA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgw
FoAUATpjf2+z6nSCYY884hDjNAJJ/ogwDgYDVR0PAQH/BAQDAgEGMA0GCSqGSIb3
DQEBCwUAA4ICAQAaf98ZDsdi1CrH/iFrv1yZo4rHgaJXlK6voGxeRszfd7aSs3ra
HadMubT6buu6Cd765PQpi9O5ZXPKhxywlI3AMx2DdZsfFlV05dfPHQD+EEIawBiU
G0bHq8CeRtNDk9xJfZMiMkFDN/hol3NC3+Ci1caUjyheql2UVnfzcF7E5gVAb12u
OxHSIKZU8Hp0Lm7UZroPWvFRSoasQ9Gbiiisnb1dXMk06sEJoG1k08bLxkLvn+Kk
5WZHv0EjkOTPpljKnux8uNIhf+kq4CpP+AvdXsjancGeBYYruTZT8ruoCfQ8q6nQ
4fFfXmUmDlENkcStmotiwOnO3LVEbQufE2FzdGed8R1Wgsvs7RjSUifEJEjSCwfj
tRNZ4C/Wi2Q9JvUoMY1nHh8ow979Xw7mpj6DKBpYo43iwOlN1Z5W3giokgDfg/wl
bfMqvtEHYeF/S6+Ze8hbqdVnJMNbwkIsOYDZL2y9EnKAlYejBE/3veqJKniiQFqU
O7zUPjz8ZcV6Efm/SN9QpQfMIvashk+yR66WG+WK1u2yxY6aLu2rGNjcbZ2vKf+u
EpKL5MEj9YUMPGYw7nY2pYwKomj0W8jHMpIL+KyxBhfhMl/IU8FIH6X3W7mqO4If
lGCEe74ORTxm84UPNZwXP3dBb15jnqkU8QFCJoYZTN0w0NyfCPxLJ8qksQ==
-----END CERTIFICATE-----
```

9 Conformité avec les exigences légales

L'AH garantit la conformité avec les exigences légales, notamment :

- en matière de traitement non autorisé ou illégal des données personnelles contre la perte accidentelle, la destruction de données personnelles ou les dégâts commis aux données personnelles ;
- en matière de non divulgation d'informations fournies par les Clients à l'AH, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.

10 Exigences opérationnelles de l’AH

10.1 Gestion des requêtes de contremarques de temps

La fourniture d'une contremarque de temps en réponse à une demande n’excède pas quelques secondes entre le délai écoulé entre la réception par l'UH de la requête et la signature de la contremarque de temps résultante.

10.2 Fichiers d'audit

L'AH garantit que toutes les informations appropriées concernant le fonctionnement du service d'horodatage sont enregistrées pendant une période de temps de 5 ans en particulier dans le but de fournir une preuve en cas d'enquêtes judiciaires ou administratives.

10.2.1 Organisation et contenu des fichiers

Les événements spécifiques et les données enregistrées sont documentés par l'AH.

La confidentialité et l'intégrité des enregistrements d'audit courants et archivés relatifs au fonctionnement des services d'horodatage sont assurées.

Les enregistrements relatifs à l’administration du service d'horodatage sont intégralement archivés et de manière adaptée à la sensibilité des informations.

Les enregistrements relatifs au fonctionnement du service d'horodatage sont disponibles s'ils sont exigés dans le but de fournir une preuve d'un fonctionnement correct des services d'horodatage en cas d'enquêtes judiciaires ou administratives.

L'instant précis d'évènements significatifs concernant l'environnement de l'AH, la gestion des clés, et la synchronisation de l'horloge est enregistré.

Les enregistrements relatifs à l’administration du service d'horodatage sont gardés, après la date d'expiration de la validité de la clé de signature de l'UH durant une période de temps appropriée pour fournir des éléments de preuves nécessaires tel qu'indiqué dans les CGU de l’AH.

10.2.2 Gestion des clés

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

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

10.2.3 Synchronisation de l'horloge

Les enregistrements concernant tous les événements touchant à une synchronisation de l'horloge des UH sont effectués, ce qui inclut l'information concernant des recalibrages ou des synchronisations normales.

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

Gestion de la durée de vie de la clé privée

L'AH garantit que la clé privée de signature de l'UH n'est pas employée au-delà de la fin de leur cycle de vie.

En particulier :

- Des procédures opérationnelles et techniques sont mises en place afin d'assurer 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.
- Le système d'horodatage détruira la clé privée si la fin de la période d'utilisation de cette clé privée a été atteinte.

10.3 Synchronisation de l'horloge

L'AH garantit que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée d'une seconde. En particulier :

- Le calibrage de chaque horloge d'UH est maintenu de telle manière que l'horloge ne puisse pas normalement dériver à l'extérieur de l'exactitude déclarée ;
- Les horloges de l'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 garantit qu'elle peut détecter sans délai si son horloge interne ne respecte plus l'exactitude déclarée et à défaut d'y remédier dans les meilleurs délais, ne plus générer des contremarques de temps ;
- L'AH garantit que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde[1] est programmé comme notifié par l'organisme approprié.

10.4 Exigences du contenu d'une contremarque de temps

L'AH garantit que les contremarques de temps sont générées en toute sécurité et incluent le temps correct. En particulier :

- La contremarque de temps inclut un identifiant du certificat de l'unité d'horodatage ainsi que le certificat d'horodatage lui-même. Le certificat, quant à lui, inclut :

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

- un identifiant du pays dans lequel l'AH est établie ;
- un identifiant de l'AH ;
- une identification de l'UH qui génère les contremarques de temps ;

- La contremarque de temps inclus l'OID de la PH ;
- Chaque contremarque de temps comporte un identifiant unique ;
- Les informations de temps portées dans les contremarques de temps peuvent être reliées à au moins un temps fourni par un laboratoire UTC (k) ;
- Le temps inclus dans une contremarque de temps est synchronisé avec le temps UTC suivant l'exactitude déclarée ;
- La contremarque de temps inclut une représentation de la donnée à horodater telle que fournie par le demandeur ;
- La contremarque de temps est signée par une clé produite exclusivement à cette fin.

10.5 Compromission de l'AH

La compromission de l'AH peut être due aux évènements suivants :

- Vol des serveurs des UH ;
- Vol des clés privées des UH ;
- La compromission de la clé privée de l'AC ayant servi à générer les certificats des UH.

En cas de compromission de la clé privée de l'AC, la procédure mise en place est détaillée dans la PC/DPC en vigueur pour cette AC.

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, l'AH garantit qu'une information appropriée est mise à la disposition des utilisateurs de contremarques de temps. En particulier :

- Le plan de secours de l'AH traite le cas de la compromission réelle ou suspectée de la clé privée de signature de l'unité d'horodatage ou la perte de calibrage de l'horloge d'une UH, qui pourrait affecter des contremarques de temps émises, de la manière suivante : la plate-forme d'horodatage est hébergée sur une infrastructure haute disponibilité ; en cas de problème avec l'infrastructure ou les certificats, un serveur d'horodatage de secours sera mis en place pour un basculement manuel.
- Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une UH, qui pourrait affecter des contremarques de temps émises, l'AH mettra à la disposition de tous les utilisateurs de contremarques de temps une description de la compromission qui est survenue.
- Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage de l'UH, qui pourrait affecter des contremarques de temps émises, l'AH prendra les mesures nécessaires pour que les contremarques de temps de cette unité ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.
- En cas d'un évènement majeur dans le fonctionnement de l'AH ou d'une 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 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 sécurité des services d'horodatage.

10.6 Fin d'activité

En cas de fin d'activité du service d'horodatage, la Province Nord de Nouvelle Calédonie :

- Rendra disponible aux émetteurs et utilisateurs des contremarques de temps l'information de la cessation d'activité (via un site web) ;
- Abrogera l'ensemble des contrats établis avec les tiers dans le cadre du service d'horodatage ;
- Transfèrera à un organisme fiable les fichiers d'audit ;
- Fournira à un organisme fiable les informations nécessaires à la vérification des contremarques de temps ;
- Détruira les clés privées de toutes les unités d'horodatage de son service d'horodatage.
- Le choix de l'organisme qui récupèrera les données d'audit sera défini dans le cadre du plan de fin d'activité mis en œuvre par l'AH.

11 Contrôle de sécurité physique, contrôle des procédures, contrôle du personnel

11.1 Contrôles physiques

11.1.1 Situation géographique et construction de sites.

Le service d'horodatage est hébergé dans le Data Center de la Province Nord.

11.1.2 Accès physique

Afin de limiter l'accès aux applications et aux informations du service d'horodatage, les accès aux bâtiments des composants de l'AH et de l'UH sont limités aux seules personnes autorisées à pénétrer dans les locaux. De plus, la traçabilité des accès est assurée.

Afin d'assurer la disponibilité du système de l'UH, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physiques aux machines.

11.1.3 Energie et air conditionné

Afin d'assurer la disponibilité des systèmes informatiques de l'AH, des systèmes de génération ou de protection des installations électroniques sont mis en place par l'intermédiaire d'alimentation de secours.

11.1.4 Exposition aux liquides

Aucune exigence autre que celles prises en compte lors de la construction du Data Center.

11.1.5 Sécurité incendie

Afin d'assurer la protection des systèmes informatiques de l'AH, la zone sécurisée abritant les machines de dispositifs préventifs et de systèmes est équipée d'un système anti-incendie et de système d'extinction du feu par la diffusion d'un gaz inerte.

L'intégrité physique de l'UH permettant la génération des contremarques de temps ainsi que son accès logique par les applications utilisatrices des contremarques de temps sont assurés.

11.1.6 Destruction des supports

La destruction des supports sera assurée avec un niveau de sécurité équivalent aux conditions dans lesquelles les informations qu'ils contiennent ont été créées.

11.1.7 Sauvegardes

Les sauvegardes des applications et des informations de l'AH sont organisées de façon à assurer une reprise des services après incident la plus rapide possible.

Les médias devront être conservés avec un niveau de sécurité équivalent aux conditions dans lesquelles les informations qu'ils contiennent ont été créées.

11.2 Contrôles des procédures

11.2.1 Rôles de confiance

Afin de veiller à la séparation des opérations et tâches critiques, on distingue plusieurs rôles au sein des composantes de l'AH.

11.2.2 Nombre de personnes nécessaires à l'exécution de tâches sensibles

Ce nombre est égal à 1. Pour des tâches considérées comme critiques l'agent effectuant la tâche engage sa pleine responsabilité.

11.2.3 Identification et authentification des rôles

Chaque composante de l'AH vérifie l'identité et les autorisations de tout membre de son personnel et :

- Ajoute son nom aux listes de contrôle d'accès aux locaux à l'emplacement de l'AH.
- Ajoute son nom à la liste des personnes autorisées à accéder physiquement au système de l'AH.

11.3 Contrôle du personnel

Les tâches sensibles sont effectués par du personnel ayant :

- Les connaissances nécessaires aux techniques de l'horodatage,
- Les connaissances nécessaires aux certificats et à la gestion des listes de révocations,
- Les connaissances et l'expérience en sécurité des systèmes d'informations.

11.3.1 Contrôle des personnels contractants et sous-traitants

Sans objet.

11.3.2 Documentation fournie au personnel

Une documentation détaillée des tâches à accomplir est fournie au responsable du site. Par ailleurs ces personnels disposent de la documentation nécessaire à leur présence sur le site de production.

Un accord de confidentialité est exigé pour toute personne externe à l'AH et ses composantes.

12 Contrôles techniques de sécurité

12.1 Exactitude de temps

Si une UH fournit une exactitude différente de la seconde, celle-ci est alors désactivée. Pour cette raison l'exactitude n'est pas indiquée dans une contremarque de temps.

12.2 Génération des clés

L'AC garantit que toutes les clés cryptographiques servant à générer les certificats d'horodatage sont produites dans des circonstances contrôlées.

12.3 Certification des clés de l'unité d'horodatage

Dans le cas où l'AH utilise un HSM pour la signature des contremarques de temps de l'UH et ce HSM a été utilisé pour générer la clé privée correspondant à la clé publique du certificat 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 identiques à ceux générés par le HSM.

Dans cette même situation, l'AH vérifie, lors de l'import du certificat qu'il provient bien de l'Autorité de Certification auprès de laquelle la demande de certificat a été effectuée et que sa clé publique et l'identifiant de l'algorithme de signature du certificat correspondent également à ceux fournis dans la demande de certificat.

L'AH ne peut être opérationnelle qu'une fois ces exigences remplies.

12.4 Protection des clés privées des unités d'horodatage

L'Autorité d'horodatage s'assure que la clé privée de l'UH reste confidentielle et conserve son intégrité.

12.5 Exigences de sauvegarde des clés

[Pas d'exigences spécifiques – pris en charge par l'AC]

12.6 Destruction des clés des UH

L'AH garantit que les clés de signature sont détruites à la fin de leur cycle de vie.

12.7 Algorithmes obligatoires

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

- Accepter des valeurs de hachage générées par des clients et employant les algorithmes de hachage conformes aux exigences du [RGS].
- Génère des contremarques de temps signées selon les algorithmes et les longueurs de clé conformes aux exigences du [RGS].

12.8 Vérification 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 :

- Les certificats des unités d'horodatage sont disponibles, et joints à la contremarque de temps.
- Un ou plusieurs certificats utilisables pour valider une chaîne de certificats se terminant par un certificat d'unité d'horodatage sont disponibles.

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

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

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

12.9 Durée de validité des certificats de clé publique de l'UH

La durée de validité des certificats des UH ne peut pas être plus longue que :

- La durée de vie cryptographique de la clé privée associée ;
- La fin de validité du certificat d'AC qui l'a émis.

12.10 Durée d'utilisation des clés privées de l'UH

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

13 Profils de certificats et de LCR

13.1 Contremarques de temps

Les contremarques de temps fournies par l'AH ont une structure TimeStampToken conforme à la [RFC3161]. Le tableau ci-dessous reprend l'ensemble des champs d'un TimeStampToken tels que définis dans la [RFC3161].

La contremarque de temps est conforme au tableau ci-dessous.

Champ	Exigences
messageImprint	Empreinte des données et OID de l'algorithme utilisé (voir ci-dessous)
accuracy	Absent
ordering	false
tsa	Province Nord Nouvelle Calédonie Timestamping Unit 1
extensions	Absent
Policy	1.3.6.1.4.1.44394.2.1.1.1

Les OID des algorithmes d'empreinte sont les suivants :

SHA1	1.3.14.3.2.26
SHA256	2.16.840.1.101.3.4.2.1
SHA384	2.16.840.1.101.3.4.2.2
SHA512	2.16.840.1.101.3.4.2.3

13.2 Certificats et LCR

Les gabarits des certificats d'UH sont conformes aux exigences des certificats de type « cachet » dont la clé privée associée est utilisée pour signer des jetons d'horodatage qui présentent les caractéristiques suivantes :

- L'extension "Extended Key Usage" est présente, marquée critique, et ne contient que l'identifiant id-kp-timeStamping à l'exclusion de toute autre ;
- Le champ "DN Subject" identifie l'AH suivant les mêmes règles que l'identification des AC et l'identifiant propre à l'UH concernée, au sein de l'AH, est porté dans l'attribut commonName du DN de ce champ ;
- La durée de vie maximale est bornée selon le couple {durée de vie cryptographique de la clé ; fin de validité de la durée de vie de l'AC émettrice} ;
- La liste de distribution LCR est définie en extension.

13.3 Algorithmes cryptographiques

Des algorithmes et des longueurs de clés conformes au RGS sont utilisés pour signer les contremarques de temps. Les biclés RSA sont d'une longueur de 2048 bits. La signature des contremarques de temps utilise l'algorithme de hachage SHA256.

14 Annexes - Documents techniques

[RGS]	Référentiel Général de Sécurité – version 1.0
[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".