Plate-forme SUNNYSTAMP

POLITIQUE D'HORODATAGE

OID n°1.3.6.1.4.1.22542.3.2.0

Version 1.1
du 1er janvier 2014

Historique des versions

Date	Evolution	Version
1 novembre 2012	Version définitive	v1.0
1 janvier 2014	Nouveau logo	v1.1

SOMMAIRE

1. Préambule 4
2. Présentation générale de la PC 5
2.1 Liste des Acronymes 5
2.2 Définitions des termes utilisés dans la PC 5
2.3 Type d'applications concernés par la PH 7
2.4 Type de contremarques de temps définis par la PH 7
2.5 Modification de la PH 7
3. Dispositions de portée générale 8
3.1 Obligations de l'Autorité d'horodatage 8
3.2 Obligations du Client du service 8
3.3 Obligations de l'Utilisateur destinataire 8
3.4 Obligations spécifiques de l'AC fournissant les certificats 8
3.5 Déclaration des pratiques d'horodatage 8
3.6 Conditions générales d'utilisation 8
3.7 Conformité avec les exigences légales 9
4. Exigences opérationnels 10
4.1 Gestion des requêtes de contremarques de temps 10
4.2 Fichiers d'audit 10
4.2.1. Organisation et contenu des fichiers 10
4.2.2 Gestion des clés 10
4.2.3 Synchronisation de l'horloge 10
4.3 Gestion de la durée de vie de la clé privée 10
4.4 Synchronisation de l'horloge 11
4.5 Exigences du contenu d'une contremarque de temps 11
4.6 Compromission de l'AH 11
4.7 Fin d'activité 12
5. contrôle de securite physique, contrôle des procédures, contrôle du personnel 13
5.1 Contrôles physiques 13
5.1.1 Situation géographique et construction de sites. 13
5.1.2 Accès physique 13
5.1.3 Energie et air conditionné 13
5.1.4 Exposition aux liquides 13
5.1.5 Sécurité incendie 13
5.1.6 Site de secours 13
5.1.7 Conservation des médias 13
5.1.8 Destruction des supports 13
5.1.9 Sauvegarde hors site 14
5.2 Contrôles des procédures 14
5.2.1 Rôles de confiance 14
5.2.2 Nombre de personnes nécessaires à l'exécution de tâches sensibles 14
5.2.3 Identification et authentification des rôles 14
6.3 Contrôle du personnel 14
5.3.7 Contrôle des personnels contractants et sous-traitants 14
5.3.8 Documentation fournie au personnel 14
6. Controles techniques de sécurité 15
6.1 Exactitude de temps 15
6.2 Génération des clés 15
6.3 Certification des clés de l'unité d'horodatage 15

6.4 Protection des clés privées des unités d'horodatage 15
6.5 Exigences de sauvegarde des clés 15
6.6 Destruction des clés des unités d'horodatage 15
6.7 Algorithmes obligatoires 15
6.8 Vérification des contremarques de temps 15
6.9 Durée de validité des certificats de clé publique de l'unité d'horodatage 16
6.10 Durée d'utilisation des clés privées de l'unité d'horodatage 16
7. Profils de certificats et de LCR 17
7.1 Contremarques de temps 17
7.2 Certificats et LCR 17
7.3 Algorithmes cryptographiques 17
8. ANNEXE - Documents techniques 18

1. PREAMBULE

La société LEX PERSONA (http://www.lex-persona.com/) a développé et opère un service d'horodatage sur la plate-forme Sunnystamp. La plate-forme supporte le Service qui réunit un ensemble de composants centralisés :

- Une IGC (Infrastructure de Gestion de Clés) permettant de délivrer des certificats électroniques aux utilisateurs en mode centralisé, ainsi que des fonctions complémentaires, notamment un service d'horodatage.
- Des fonctionnalités de signature électronique de fichiers (en mode centralisé ou décentralisé) et de vérification de fichiers signés électroniquement ;
- Un portail Web (https://www.sunnystamp.com) et diverses interfaces de type Web Services permettant aux Clients qui le désirent d'intégrer à leur système d'information les fonctions de signature électronique de fichiers et de vérification de fichiers signés électroniquement.

Le service d'horodatage est mis en œuvre par une Unité d'horodatage (UH) placée sous la responsabilité d'une Autorité d'Horodatage (AH). En l'état actuel du présent document, l'Autorité d'Horodatage se fond dans l'Autorité de Certification racine Sunnystamp, sans faire appel à un quelconque prestataire externe.

Le service d'horodatage ne constitue pas une prestation technique commercialisée au public. Il s'agit d'un service à usage interne à la disposition de chaque entité de certification composant l'IGC. A cet égard, l'IGC présente d'ailleurs une organisation des Autorités de Certification (AC) hiérarchisée dans le schéma suivant :

- une AC "racine",
- des AC filles pour divers prestataires désirant distribuer des certificats,
- des AC Users pour les clients des prestataires, se référant à l'AC fille du prestataire.

Pour ses besoins propres, Lex Persona dispose également d'une AC fille.

Le présent document, identifié par OID spécifique, constitue la Politique d'Horodatage (PH) de l'Autorité d'horodatage (AH) Lex Persona. Il définit les exigences auxquelles l'AH Lex Persona se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une classe d'application avec des exigences de sécurité communes.

2. PRESENTATION GENERALE DE LA PC

2.1 Liste des Acronymes

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

AC Autorité de Certification
AH Autorité d'Horodatage
ANSSI Agence Nationale de la Sécurité des Systèmes d'Information
DPH Déclaration relative aux procédures d'horodatage
IGC Infrastructure de Gestion de Clés
OID Object Identifier
LCR Liste de Révocation de Certificats
PH Politique d'Horodatage
PS Politique de Service Sunnystamp
UH Unité d'Horodatage
UTC Coordinated Universal Time

2.2 Définitions des termes utilisés dans la PC

Autorité de Certification (AC) : terme employé ici pour nommer l'entité interlocutrice de l'autorité d'enregistrement (AE), et responsable de la délivrance de certificats qu'elle signe. L'AC Lex Persona Interne est le maître d'ouvrage de l'IGC.

Certificat : fichier électronique attestant qu'une clé publique appartient à l'entité qu'il identifie (personne physique ou morale ou entité matérielle). Il est délivré par une AC. En signant le certificat, l'AC valide le lien entre l'entité et la biclé. Le certificat a une période de validité limitée. La présente s'intéresse au cycle de vie de la famille de certificats « Lex Persona Time Stamping Certificate".

Client du service : utilisateur de la plate-forme qui prend en charge le coût d'un des services proposés : signer un fichier, faire signer un fichier, vérifier un fichier signé, etc.

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 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.

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

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.

Génération (d'un certificat) : action réalisée par l'AC « Lex Persona AC Interne » et qui consiste à signer un certificat sur la base d'informations fournies par la composante de l'IGC ayant enregistré une demande d'un client de création de certificat.

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.

Politique de Service (PS) : document, identifiée par un OID, qui décrit les modes de formation d'une signature électronique de fichier générée par un utilisateur, préalablement authentifié, des modes de vérifications de fichiers signés électroniquement ainsi que des services associés optionnels ou complémentaires apportés par la plate-forme.

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 clients émetteurs de contremarques de temps et les utilisateurs de contremarques de temps.

Révocation (d'un certificat) : opération demandée par le porteur, par l'AC, ou l'AE et dont le résultat est la suppression de la caution de l'AC Lex Persona 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 de matériel et de 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 politique d'horodatage donnée par une autorité d'horodatage donnée.

Validation (de certificat) : opération de contrôle du statut d'un certificat.

2.3 Type d'applications concernés par la PH

Les applications concernées par cette PH sont toutes les applications qui mettent en œuvre les progiciels et librairies Lex Persona pour lesquels l'utilisateur de ces applications dispose d'une licence d'utilisation du service, qu'elle soit implicitement ou explicitement décrite. A contrario, il est rigoureusement interdit d'utiliser le service d'horodatage Sunnystamp et de générer des contremarques de temps sans licence d'utilisation adéquate.
En l'état, le service d'horodatage est principalement utilisé par le service de signature électronique à des fins techniques, comme pour l'horodatage des cachets serveurs ou l'horodatage des comptes-rendus de vérification de signature ou pour tout autre traitement précisé par la Politique de Services (PS) de Sunnystamp.

2.4 Type de contremarques de temps définis par la PH

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

- l'identifiant de la politique d'horodatage sous laquelle la contremarque de temps a été générée ;
- la valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
- la date et le temps UTC ;
- l'identifiant du certificat de l'Unité d'horodatage (UH) qui a généré la contremarque de temps (qui contient aussi le nom de l'Autorité d'horodatage).

Les certificats peuvent encore contenir des informations supplémentaires.

2.5 Modification de la PH

La présente PH est la propriété exclusive de la société Lex Persona. Elle sera revue à l'occasion de l'évolution du service au sein de l'IG 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
Société Lex Persona, BP 601, 10901 TROYES CEDEX 9.

Personne physique responsable
François DEVORET, gérant, Lex Persona.

3. DISPOSITIONS DE PORTEE GENERALE

3.1 Obligations de l'Autorité d'horodatage

L'Autorité d'horodatage s’assure de la conformité des exigences et des procédures prescrites dans cette politique.
L'Autorité d'horodatage garantit l'adhésion aux obligations complémentaires indiquées dans la contremarque de temps ou bien directement ou bien incorporées par référence.
L'Autorité d'horodatage s’engage à remplir tous les engagements stipulés dans ses conditions générales d'utilisation.

3.2 Obligations du Client du service

Le Client du service émetteur de contremarque de temps ne peut accéder à ce sous-ensemble de fonctionnalités de la plate-forme que par l'intermédiaire de la plate-forme.

3.3 Obligations de l'Utilisateur destinataire

Les utilisateurs destinataires de contremarques de temps en cas de vérification doivent :
a) vérifier que la contremarque de temps a été correctement signée, et que le certificat de l’unité d’horodatage est valide à l'instant de la vérification.
b) tenir compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la présente PH et la Politique de Service.

3.4 Obligations spécifiques de l'AC fournissant les certificats

Le certificat de clé publique délivré à l'unité d'horodatage est confectionné par une AC respectant les exigences du niveau de sécurité une étoile (*) de la Politique de Certification Type "cachet serveur" du RGS.

3.5 Déclaration des pratiques d'horodatage

Au niveau d'exigences présentées par cette PH, il n'y a pas de Déclaration des Pratiques d'Horodatage.

3.6 Conditions générales d'utilisation

L'Autorité d'horodatage met à disposition des utilisateurs destinataires de contremarques de temps :

- Une information sur un point de contact pour l'Autorité d'horodatage.
- Une description ou une référence de la politique d'horodatage appliquée.
- Au moins un algorithme de hachage qui peut être utilisé pour représenter la donnée à horodater.
- La période de temps minimum, hors cas de révocation, durant laquelle les contremarques de temps seront vérifiables.
- L'exactitude du temps dans les contremarques de temps par rapport au temps UTC.
- N'importe quelles limitations sur l'utilisation du service d'horodatage.
- Les obligations des utilisateurs de contremarques de temps, si elles ne font partie ni du contrat de service général
- 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 sa période de validité.
- La période de temps pendant laquelle les fichiers d'audit de l'Autorité d'horodatage sont conservés.
- Les éléments permettant de valider la chaîne de certificats

3.7 Conformité avec les exigences légales

L'Autorité d'horodatage 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'Autorité d'horodatage, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.

4. EXIGENCES OPERATIONNELS

4.1 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'AH de la requête et la signature de la contremarque de temps résultante.

4.2 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 30 ans en particulier dans le but de fournir une preuve en cas d'enquêtes judiciaires ou administratives.

4.2.1. Organisation et contenu des fichiers

- Les événements spécifiques et les données enregistrées sont documentés par l'Autorité d'horodatage.
- 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 des services d'horodatage sont intégralement archivés et de manière adaptée à la sensibilité des informations.
- Les enregistrements relatifs au fonctionnement des services 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'Autorité d'horodatage, 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'unité d'horodatage durant une période de temps appropriée pour fournir des éléments de preuves nécessaires tel qu'indiqué dans les conditions générales d'utilisation de l'Autorité d'horodatage.

4.2.2 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 unités d'horodatage sont effectués.

4.2.3 Synchronisation de l'horloge

- Les enregistrements concernant tous les événements touchant à une synchronisation de l'horloge des unités d'horodatage 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.

4.3 Gestion de la durée de vie de la clé privée

L'Autorité d'horodatage garantit que la clé privée de signature de l'unité d'horodatage 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'unité d'horodatage 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.

4.4 Synchronisation de l'horloge

L'Autorité d'horodatage 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'unité d'horodatage 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.

4.5 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 l'identifiant du certificat de l'unité d'horodatage. Le certificat inclus :
    - un identifiant du pays dans lequel l'Autorité d'horodatage est établie,
    - un identifiant de l'Autorité d'horodatage,
    - une identification de l'unité d'horodatage qui génère les contremarques de temps.
- La contremarque de temps inclus l'OID de la politique d'horodatage.
- 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.
- La contremarque de temps respecte les exigences du chapitre 7 ci-dessous.

4.6 Compromission de l'AH

Dans le cas d'événements qui affectent la sécurité des services d'horodatage, incluant la compromission de la clé privée de signature d'une unité d'horodatage 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 :

[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.

- 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 unité d'horodatage, qui pourrait affecter des contremarques de temps émises, de la manière suivante : la plateforme 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 avec un certificat d'horodatage de secours prend le relais sur basculement manuel.
- Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, 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'unité d'horodatage, 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.

4.7 Fin d'activité

La fin de l'activité de l'AH, pour toutes causes que ce soit, peut se produire dans les deux contextes suivants :

- Si la plate-forme d'horodatage Lex Persona poursuit son activité, l'AH déléguera à un opérateur de service d'horodatage du marché la confection de ses contremarques de temps ;
- Si la plate-forme d'horodatage Lex Persona est en fin d'activité, la Politique de Service Lex Persona en indique les modalités.

5. CONTROLE DE SECURITE PHYSIQUE, CONTROLE DES PROCEDURES, CONTROLE DU PERSONNEL

NOTE : EN L'ETAT ACTUEL DE L'IGC, L'AH NE SE DISTINGUE PAS DE L'AC. EN CONSEQUENCE, L'ORGANISATION DES CONTROLES VISEE DANS CE CHAPITRE EST CELLE DE LA POLITIQUE DE CERTIFICATION.

5.1 Contrôles physiques

5.1.1 Situation géographique et construction de sites.
Aucune exigence n'est stipulée. Les précisions pourront être fournies dans la DPC.

5.1.2 Accès physique
Afin de limiter l'accès aux applications et aux informations de l'IGC, les accès aux bâtiments des composants de l'AC et de l'AE 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'AC, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physiques aux machines.

5.1.3 Energie et air conditionné
Afin d'assurer la disponibilité des systèmes informatiques de l'AC, des systèmes de génération ou de protection des installations électroniques sont mis en place par l'intermédiaire d'alimentation de secours.
Des précisions quant aux moyens mis en œuvre à cette fin pourront être fournies dans la DPC.

5.1.4 Exposition aux liquides
Les précisions pourront être éventuellement fournies dans la DPC.

5.1.5 Sécurité incendie
Afin d'assurer la protection des systèmes informatiques de l'AC, 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 du système permettant la publication de la LCR en cours de validité ainsi que son accès logique par les applications utilisatrices des certificats sont assurés.

5.1.6 Site de secours
Afin d'assurer la disponibilité du système et des services, l'AC dispose des moyens nécessaires à assurer la reprise de l'activité dans les délais impartis à la fonction. Des précisions quant aux moyens mis en œuvre à cette fin pourront être fournies dans la DPC.

5.1.7 Conservation des médias
Les médias sont conservés avec un niveau de sécurité équivalent aux conditions dans lesquelles les informations qu'ils contiennent ont été créées.

5.1.8 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.
Des précisions quant aux moyens mis en œuvre à cette fin pourront être fournies dans la DPC.

5.1.9 Sauvegarde hors site

Les sauvegardes des applications et des informations de l'AC sont organisées de façon à assurer une reprise des services après incident la plus rapide possible, en particulier pour les applications intervenant dans la publication d'une LCR et dans la révocation des certificats.
Les médias devront être conservés avec un niveau de sécurité équivalent aux conditions dans lesquelles les informations qu'ils contiennent ont été créées.

5.2 Contrôles des procédures

5.2.1 Rôles de confiance

Afin de veiller à la séparation des opérations et tâches critiques, on distingue plusieurs rôles au sein des composantes de l'IGC. Les attributions précises et associées à chaque rôle sont décrites dans la DPC Lex Persona AC Interne.

5.2.2 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.

5.2.3 Identification et authentification des rôles

Chaque composante de l'AC et de l'AE vérifie l'identité et les autorisations de tout membre de son personnel afin de lui faire attribuer un certificat d'authentification et :

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

6.3 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 signature électronique,
- Les connaissances et l'expérience en sécurité des systèmes d'informations.

5.3.7 Contrôle des personnels contractants et sous-traitants

Sans objet.

5.3.8 Documentation fournie au personnel

Une documentation détaillée des tâches à accomplir est fournie au responsable du site. Par ailleurs ces personnels disposent bien entendu de toute documentation nécessaire à leur présence sur le site de production.
Un accord de confidentialité est exigé pour toute personne externe à l'IGC est ses composantes.

6. CONTROLES TECHNIQUES DE SECURITE

6.1 Exactitude de temps

Si une unité d'horodatage 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.

6.2 Génération des clés

L'Autorité d'horodatage garantit que toutes les clés cryptographiques sont produites dans des circonstances contrôlées. En particulier, la génération des clés de signature des unités d'horodatage est effectuée dans un module d'horodatage répondant aux exigences du chapitre 7 ci-dessous.

6.3 Certification des clés de l'unité 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'Unité d'Horodatage sont identiques à ceux générés par l'Unité d'Horodatage.
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.
L'AH ne peut être opérationnelle qu'une fois ces exigences remplies.

6.4 Protection des clés privées des unités d'horodatage

L'Autorité d'horodatage s'assure que sa clé privée reste confidentielle et conserve son intégrité. Elle est confinée et utilisée à l'intérieur d'un module d'horodatage répondant aux exigences du chapitre 7.3 ci-dessous.

6.5 Exigences de sauvegarde des clés

[Pas d'exigences spécifiques]

6.6 Destruction des clés des unités d'horodatage

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

6.7 Algorithmes obligatoires

L'Autorité d'horodatage, 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 chapitre 7 ci-dessous.
- Génère des contremarques de temps signées selon les algorithmes et les longueurs de clé conformes aux exigences du chapitre 7 ci-dessous.

6.8 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.

6.9 Durée de validité des certificats de clé publique de l'unité d'horodatage

La durée de validité des certificats des unités d'horodatage 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.

6.10 Durée d'utilisation des clés privées de l'unité d'horodatage

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).

7. PROFILS DE CERTIFICATS ET DE LCR

7.1 Contremarques de temps

Les contremarques de temps fournies par l'AH est une structure TimeStampToken conforme au [RFC3161]. Le tableau ci-dessous reprend l'ensemble des champs d'un TimeStampToken tels que définis dans le [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	Lex Persona Time Stamping Certificate [A ou B]
extensions	Absent
Policy	1.3.6.1.4.1.22542.3.2.0

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

7.2 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.

7.3 Algorithmes cryptographiques

Des algorithmes et des longueurs de clés conforment au RGS sont utilisés pour les 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.

8. ANNEXE - 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".