Politique Horodatage

Infrastructure de confiance

PL

Politique

Référentiel :	Sous-Référentiel :	Référence :	Statut :
Sécurité	PKI	PKA026 1.3.6.1.4.1.48620.20.1	Validé
Approuvé par :	**Fonction :**	**Date :**	**Signature :**
Sébastien Passelergue	Autorité de Certification	10/01/2023	SEBASTIEN PASSELERGUE Signature numérique de SEBASTIEN PASSELERGUE Date : 2023.01.10 15:25:25 +01'00'
Validé par :	Fonction :	**Date• :**	**Signature :**
Pascal d'Aversa	Directeur de Sécurité	10/01/2023	PASCAL DAVERSA Signature numérique de PASCAL DAVERSA Date : 2023.01.10 15:18:43 +01'00'
Diffusion auprès de :			
En accès pour :	Public.		
Localisation :			

Sommaire

1. INTRODUCTION .....
2. DISPOSITIONS GENERALES.....
3. EXIGENCES OPERATIONNELLES .....
4. EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES, PROCEDURALES ET ORGANISATIONNELLES .....
5. EXIGENCES DE SECURITE TECHNIQUES .....
6. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS .....
7. ANNEXE 1 : DOCUMENTS CITES EN REFERENCE .....

Date de péremption		Responsable de l'actualisation	

Version	Date	Modifications	Auteur
V1.8	18/04/2018	Modifications pour conformité RGPD	MMI
V1.9	23/07/2018	Modifications suite a audit	OLE
V2.0	08/08/2019	Modifications suite a audit	MMI
V2.1	28/05/2021	Modifications suite a audit	MMI
V2.2	10/01/2023	Modification taille clef RSA 2048 à 3072 bits	PDA

• Date d'entrée en vigueur

Documents de référence

Référence	Version	Titre du document

Sommaire détaillé

1. INTRODUCTION 4
1.1 Présentation générale 4
1.2 Identification 4
1.2.1. Identification du document PH 4
1.2.2. Identification de l'OID politique d'horodatage 5
1.3 Publication 5
1.3.1. Circonstances rendant une mise à jour nécessaire 5
1.4 Entité déterminant la conformité des pratiques avec la PH 5
1.5 Procédures d'approbation de la conformité de la DPH 5
1.6 Point de contact 6
1.7 Généralités 6
1.7.1. Définitions 6
1.7.2. Abréviations 7
2. DISPOSITIONS GENERALES 9
2.1 Obligations de l'Autorité d'horodatage 9
2.2 Obligations du Client 9
2.3 Obligations de l'abonné 9
2.4 Obligations de l'utilisateur de contremarques de temps 9
2.5 Obligations pour les AC fournissant les certificats des UHs 9
2.6 Déclarations des pratiques d'horodatage 10
2.7 Conditions Générales d'Utilisation 10
2.8 Conformité avec les exigences légales 10
2.8.1. Droit applicable 10
2.8.2. Règlement des différends 10
2.8.3. Propriété intellectuelle 11
2.8.4. Données nominatives 11
3. EXIGENCES OPERATIONNELLES 12
3.1 Gestion des requêtes de contremarques de temps 12
3.2 Fichiers d'audit 12
3.3 Gestion de la durée de vie de la clé privée 12
3.4 Synchronisation de l'horloge 12
3.5 Exigences du contenu d'une contremarque de temps 13
3.6 Compromission de l'AH 13
3.7 Fin d'activité 14
4. EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES, PROCEDURALES ET ORGANISATIONNELLES 15

4.1 Exigences physiques et environnementales 15
4.1.1. Situation géographique et construction des sites 15
4.1.2. Accès physique 15
4.1.3. Alimentation électrique et climatisation 15
4.1.4. Exposition aux dégâts des eaux 15
4.1.5. Prévention et protection incendie 16
4.1.6. Conservation des supports de données 16
4.1.7. Mise hors service des supports 16
4.1.8. Sauvegarde hors site 16
4.2 Exigences procédurales 16
4.2.1. Analyse des risques 16
4.2.2. Gestion des supports 16
4.2.3. Planification de systèmes 17
4.2.4. Gestion des incidents 17
4.2.5. Manipulation et sécurité des systèmes 17
4.2.6. Procédures de fonctionnement et responsabilités 17
4.2.7. Amélioration continue des systèmes d'information 17
4.2.8. Gestion d'accès au système 18
4.2.9. MESURES DE SECURITE RESEAU 18
4.3 Exigences organisationnelles 19
4.3.1. Rôles de confiance 19
4.3.2. Identification et authentification pour chaque rôle 19
4.3.3. Mesures de sécurité vis à vis du personnel 20
5. EXIGENCES DE SECURITE TECHNIQUES 22
5.1 Exactitude temps 22
5.2 Génération de clé 22
5.3 Certification des clés de l'unité d'horodatage 22
5.4 Protection des clés privées des unités d'horodatage 23
5.5 Exigences de sauvegarde des clés des unités d'horodatage 23
5.6 Destruction des clés des unités d'horodatage 23
5.7 Algorithmes obligatoires 23
5.8 Vérification des contremarques de temps 23
5.9 Durée de validité des certificats de clé publique des unités d'horodatage 23
5.10 Durée d'utilisation des clés privées des UH 24
5.11 profil certificat et contremarque de temps 25
5.11.1. Format du certificat d'horodatage 25
5.12 format de la contremarque temps 28
6. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS 29
6.1 Fréquences et / ou circonstances des évaluations 29
6.2 Identités / qualifications des évaluateurs 29
6.3 AUTRES ELEMENTS DE CONFORMITE 29
7. ANNEXE 1 : DOCUMENTS CITES EN REFERENCE 30
7.1 Réglementation 30
7.2 Documents techniques 30

1. INTRODUCTION

1.1 PRESENTATION GENERALE

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

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

Cette Politique d'horodatage est conforme à la norme

- ETSI EN 319401
- ETSI EN 319 421
- ETSI EN 319 422

À travers cette conformité, be-invest souhaite proposer un service d'horodatage qualifié au sens du Règlement eIDAS.
La présente PH est également conforme aux exigences exprimées dans la PC de l'AC ayant émis les certificats de scellement des différentes UH opérées par l'AH

L'objectif de ce document est de définir les engagements be-invest, en tant qu'AH, respecte dans la délivrance et la gestion de contremarques de temps, ainsi que les obligations des autres participants.

Le présent document est complété, dans sa partie mise en œuvre, par une Déclaration des Pratiques d'Horodatage (DPH) et des Conditions Générales d'utilisation du service d'horodatage (CGU).
Une DPH expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la PH, en particulier les processus qu'une UH emploiera pour la création des contremarques de temps et le maintien de l'exactitude de ses horloges. L'AH be-invest met en œuvre plusieurs UH pour supporter son service d'horodatage.

Cette PH n'impose pas d'exigences sur le lien entre l'empreinte numérique à horodater et le contenu de la donnée électronique qui en est à l'origine. Cette vérification est à la charge de l'utilisateur du service d'horodatage.

1.2 IDENTIFICATION

1.2.1. Identification du document PH

La présente Politique d'Horodatage (PH) be-invest peut être identifiée par son numéro d'identifiant d'objet (OID - cf. page de garde et en-tête de chaque page).

Le numéro d'OID du présent document est : 1.3.6.1.4.1.48620.20.1
La référence du document au sein Be-invest est la suivante : PKA026.

1.2.2. Identification de l'OID politique d'horodatage

L'OID Contremarques de temps émise par l'AH be-invest avec cette politique est :
1.3.6.1.4.1.48620.20.1.1 conforme à ETSI EN 319 421 itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)

En cas de changement de politique l'OID des Contremarques de temps, le nouvel OID sera :
1.3.6.1.4.1.48620.20.1.2 ETSI EN 319 421

1.3 PUBLICATION

La présente Politique d'Horodatage est publiée sur l'URL :

- https://pki.almerys.com/horodatage.html,
- https://pki.be-ys.com/horodatage.html,

L'AH publie également :

- Les certificats de ses unités d'horodatage,
- Les CGU d'horodatage,
- Le présent document.

1.3.1. Circonstances rendant une mise à jour nécessaire

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

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

Toutes les remarques, ou souhaits d'évolution, sur la présente politique sont à adresser par courriel à l'adresse indiqué dans le paragraphe 1.6.
L'AH notifiera, par une publication d'un bandeau sur le site de publication, de la mise-à-jour d'une nouvelle version de la présente PH.

1.4 ENTITE DETERMINANT LA CONFORMITE DES PRATIQUES AVEC LA PH

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

1.5 PROCEDURES D'APPROBATION DE LA CONFORMITE DE LA DPH

L'approbation de conformité de la DPH par rapport à cette PH est à la charge de l'AG, et du responsable de sécurité des services de confiance.

Le responsable de sécurité des services de confiance est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPH doit suivre le processus d'approbation mis en place.

1.6 POINT DE CONTACT

Le représentant habilité à contacter pour toutes questions concernant la présente Politique d'horodatage est :
Autorité de Gouvernance IGC be-ys
Email :gouvernance.igc@be-ys.com

be-invest
– 17 rue Léon Laval –
L-3372 LEUDELANGE – LUXEMBOURG

1.7 GENERALITES

1.7.1. Définitions

Abonné – Entité ayant besoin de faire horodater des données par une Autorité d'Horodatage et qui a accepté les conditions d'utilisation de ses services. Cette notion est valable pour les hypothèses où la Contremarque de temps est demandée directement à l'AH.

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

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

Client - Entité cliente qui met à la disposition de ses Utilisateurs le service de signature électronique be-invest.

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

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

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

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

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

Jeton d'horodatage – Voir Contremarque de temps.

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

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

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

Système d'horodatage – Ensemble des Unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir des Services d'horodatage.

Unité d'Horodatage (UH) – Ensemble de matériel et de logiciel en charge de la création de Contremarques de temps caractérisé par un identifiant de l'Unité d'Horodatage accordé par une AC, et une clé unique de signature de contremarques de temps.

UTC(k) – Temps de référence réalisé par le laboratoire "k" et synchronisé avec précision avec le temps UTC, dans le but d'atteindre une précision de ±100 ns, selon la recommandation S5 (1993) du Comité Consultatif pour la définition de la Seconde. (Rec. ITU-R TF.536-1 [TF.536-1]).

Nota – Une liste des laboratoires UTC(k) est indiquée dans la section 1 de la Circulaire T publiée par le BIPM et est disponible sur le site web du BIPM (www.bipm.org).

Utilisateur de contremarque de temps – Entité (personne ou système) qui fait confiance à une Contremarque de temps émise sous une Politique d'horodatage donnée par une Autorité d'horodatage donnée.

Utilisateur final - Abonné Utilisateur de Contremarques de temps.

1.7.2. Abréviations

Pour le présent document, les abréviations suivantes s'appliquent :

AC	Autorité de Certification
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CG	Conditions Générales d'utilisation du service d'horodatage
Delta-LCR	Liste de Certificats Révoqués partielle
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion de Clés
LCR	Liste des Certificats Révoqués
OID	Object Identifier
PH	Politique d'Horodatage
PSHE	Prestataire de Services d'Horodatage

UH	Unité d'Horodatage
UTC	Coordinated Universal Time

2. DISPOSITIONS GENERALES

2.1 OBLIGATIONS DE L'AUTORITE D'HORODATAGE

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

2.2 OBLIGATIONS DU CLIENT

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

2.3 OBLIGATIONS DE L'ABONNE

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

2.4 OBLIGATIONS DE L'UTILISATEUR DE CONTREMARQUES DE TEMPS

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

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

2.5 OBLIGATIONS POUR LES AC FOURNISSANT LES CERTIFICATS DES UHS

Les certificats d'horodatage peuvent être délivrés par l'une des AC suivantes :

- BE-YS SIGNATURE AND AUTHENTICATION CA NC faisant l'objet d'une qualification ETSI EN 319411-2 QCP-l
- BE-YS CUSTOMER SERVICES CA NB faisant l'objet d'une certification, et ETSI EN 319411 LCP.

Le certificat de l'UH utilisé pour signer les demandes de Contremarques de temps devra contenir l'OID correspondant de l'AC.

2.6 DECLARATIONS DES PRATIQUES D'HORODATAGE

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

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

2.7 CONDITIONS GENERALES D'UTILISATION

L'AH définit des CGU qui reprennent les grands principes décrits dans la présente PH. Ces CGU sont basées sur le modèle défini dans l'annexe B de l'ETSI 319421.

2.8 CONFORMITE AVEC LES EXIGENCES LEGALES

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

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

2.8.1. Droit applicable

Le présent document est régi par la loi luxembourgeoise.

2.8.2. Règlement des différends

Pour toute demande d'information ou réclamation relative au service de génération et de gestion de contremarques de temps, il convient de contacter le service Autorité d'horodatage par mail à l'adresse suivante : gouvernance.igc@be-ys.com.

Les parties s'efforceront de régler à l'amiable tout litige concernant l'interprétation ou l'exécution du contrat dans les meilleurs délais. En l'absence de conciliation tout litige relatif à la validité, l'interprétation ou l'exécution des CGU sera soumis aux tribunaux compétents du Luxembourg.

2.8.3. Propriété intellectuelle

Sur le plan de la propriété intellectuelle, les produits mis en œuvre dans le service d'horodatage appartiennent aux éditeurs de ces produits.
Les utilisateurs de ces services ne disposent d'aucun droit de propriété intellectuelle sur ces différents éléments. Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent, par quelque procédé que ce soit, est strictement interdite et constitue une contrefaçon sanctionnée par le Code de la propriété intellectuelle, sauf accord préalable et écrit par be-invest.

2.8.4. Données nominatives

Toute collecte et tout traitement de données à caractère personnel par l'AH Be-invest sont réalisés dans le strict respect de la réglementation en vigueur, et en particulier le règlement européen n° 2016/679 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, et abrogeant la directive 95/46/CE dit « Règlement Général sur la Protection des Données (RGPD).

Les informations considérées comme personnelles sont au moins les informations d'enregistrement du Client
Elles ont traitées dans le strict respect de la réglementation en vigueur relative au [RGPD].

Le traitement des données à caractère personnel est sous la responsabilité de la direction. Pour la conformité [RGPD], be-invest a mis en place une organisation centrée sur le Délégué à la Protection des Données DPO.

Conformément à la législation et réglementation en vigueur, les informations à caractère personnel remises par les Clients à l'AH ne sont ni divulguées ni transférées à un tiers, sauf dans les cas suivants : consentement préalable de la personne concernée, décision judiciaire ou autre autorisation légale.

3. EXIGENCES OPERATIONNELLES

3.1 GESTION DES REQUETES DE CONTREMARQUES DE TEMPS

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

3.2 FICHIERS D'AUDIT

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

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

La confidentialité des enregistrements d'audit est assurée par une gestion d'accès physique, système et réseau appropriée. L'intégrité est assurée par un scellement cryptographique.
Les journaux du service d'horodatage sont conservés pendant 5 ans.

3.3 GESTION DE LA DUREE DE VIE DE LA CLE PRIVEE

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

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

3.4 SYNCHRONISATION DE L'HORLOGE

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

- Signal GPS ;
- Signal DCF77 ;
- NTP internet pour la récupération de source de temps UTC,

En particulier :

a) Le calibrage de chaque horloge d'UH est maintenu de telle manière que les horloges ne puissent pas normalement dériver en dehors de l'exactitude déclarée.
b) L'AH s'assure que tout non-respect de l'exactitude déclarée par son horloge interne sera détecté.

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

c) Si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude annoncée, ou que les serveurs de temps ne sont plus disponibles, alors les Contremarques de temps ne seront plus générées par cette UH.

La perte de calibration d'une ou de l'ensemble des unités d'horodatage est prise en compte dans le plan de secours. Le plan de secours contient également un plan de communication envers les abonnés et les utilisateurs en cas de perte de calibration.

3.5 EXIGENCES DU CONTENU D'UNE CONTREMARQUE DE TEMPS

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

Champ	***Description***	***Valeur***
version		1
Policy	OID de la PH	1.3.6.1.4.1.48620.20.1.1 ETSI EN 319 421
messageDigest	OID de l'algorithme de hash, et empreinte (hash) des données à horodater (inclue dans la requête d'horodatage)	
serialNumber	Identifiant unique de la contremarque de temps	
GenTime	Heure de génération de la contremarque de temps calculée par rapport à une source UTC(k)	
accuracy	Précision déclaré	1 seconde
Ordering		False
nonce	Identique à celui présenté lors de la demande de génération si celui-ci est présent dans cette dernière	
TSA	champ "subject" du certificat d'horodatage	
Extension	Pas d'extension supplémentaire	

3.6 COMPROMISSION DE L'AH

L'AH garantit, dans le cas d'événements qui affectent la sécurité des Services d'horodatage – incluant la compromission de la clé privée de signature d'une UH ou la perte détectée de calibrage qui pourrait affecter des Contremarques de temps émises –, qu'une information appropriée est mise à la disposition des Abonnés, des Clients et des Utilisateurs de contremarques de temps.

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

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

Le plan de secours contient également un plan de communication envers les abonnés et les utilisateurs en cas de compromission de l'AH.

3.7 FIN D'ACTIVITE

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

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

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

4. EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES, PROCEDURALES ET ORGANISATIONNELLES

4.1 EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES

4.1.1. Situation géographique et construction des sites

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

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

4.1.2. Accès physique

La protection physique des systèmes de l'UH repose sur la définition de périmètres de sécurité physiques avec des accès restreints aux seuls personnels autorisés. Des systèmes de contrôles d'accès sont en place pour répondre à cette exigence.
L'AH garantit que l'accès physique aux services critiques est contrôlé et que les risques physiques d'atteinte à ses actifs sont réduits au minimum. En particulier, pour la fourniture du service d'horodatage :

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

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

Les entrées dans les zones sécurisées font l'objet d'une surveillance indépendante et les personnels non autorisés sont obligatoirement accompagnés d'une personne de confiance autorisée dans les zones sécurisée.

4.1.3. Alimentation électrique et climatisation

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

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

4.1.4. Exposition aux dégâts des eaux

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

4.1.5. Prévention et protection incendie

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

4.1.6. Conservation des supports de données

Les documents « projet » afférents au service d'horodatage sont stockés sur un Intranet et bénéficient d'une sauvegarde quotidienne.
En particulier, les supports font l'objet de mesures contre les dommages, le vol, les accès non autorisés et l'obsolescence. Ces mesures s'appliquent durant toute la période de rétention du contenu de ces supports.
En particulier, les systèmes ne peuvent être sortis des sites sans autorisation préalable.

4.1.7. Mise hors service des supports

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

4.1.8. Sauvegarde hors site

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

4.2 EXIGENCES PROCEDURALES

4.2.1. Analyse des risques

Le service d'horodatage fait partie du périmètre de l'étude de risques menée par be-invest.
be-invest a réalisé une analyse de risque pour identifier, analyser et évaluer les risques pesant sur l'IGC en prenant en compte les risques techniques et métier. Suite à cette analyse de risque, be-invest a sélectionné et mis en œuvre des mesures de traitement du risque et les procédures opérationnelles associées, de telle façon que le niveau de sécurité soit approprié vis-à-vis du degré de risque.

L'analyse de risque est approuvée par le Responsable de l'IGC qui accepte, par cette approbation, le risque résiduel identifié.

Les mesures de traitement du risque sont décrites dans la DPH ainsi que dans sa PSSI.

Cette analyse de risque est revue régulièrement, a minima annuellement et lors de toute évolution significative d'un système ou d'une composante de l'IGC be-ys.

4.2.2. Gestion des supports

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

4.2.3. Planification de systèmes

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

4.2.4. Gestion des incidents

Les systèmes de l'AH font l'objet d'une surveillance. Cette surveillance inclut une revue des traces d'audit afin d'identifier la présence d'activités anormales et d'alerter les personnels d'un potentiel incident de sécurité

Un rapport d'incident et des procédures de réponse aux incidents sont employés d'une telle façon que les dégâts liés aux incidents de sécurité et aux défaillances sont réduits au minimum.
En cas d'incident, d'AH agit sans délai et de façon coordonnée afin de répondre rapidement à l'incident et de limiter l'impact en cas de faille de sécurité.
Les incidents ayant un impact potentiellement critique sur la sécurité sont suivis par des personnels en rôle de confiance. Ces personnels s'assurent que les procédures de remontés et de traitement des incidents sont correctement appliqués.

En cas d'incident majeur de sécurité ou de perte d'intégrité ayant un impact important sur ses opérations de service de confiance ou sur les données personnelles, be-invest notifiera les parties concernées, en particulier l'organe de contrôle et l'organe en charge de la protection des données personnelles, dans les 24 heures après l'identification de l'incident, conformément aux exigences du Règlement eIDAS et, le cas échéant, les clients impactés.

4.2.5. Manipulation et sécurité des systèmes

L'AH met en œuvre une politique de classification sur l'ensemble des éléments du service d'horodatage. Tout changement qui impacterait le niveau de sécurité doit être approuvé au préalable par l'AG. La configuration des différents systèmes est vérifiée périodiquement de façon sécurisée afin de s'assurer qu'elle ne viole pas la politique de sécurité.
Les HSM utilisés par les UH font l'objet de mesures de sécurité tout au long de leur cycle de vie, afin de s'assurer qu'ils n'ont pas fait l'objet d'altération, en particulier durant leur transport ou durant leur stockage.

4.2.6. Procédures de fonctionnement et responsabilités

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

- les procédures opérationnelles et les responsabilités ;
    - la planification et la qualification des systèmes sécurisés ;
    - la protection vis-à-vis du logiciel malveillant ;
    - la maintenance ;
    - la gestion du réseau ;
    - le contrôle actif des journaux d'audit, l'analyse des événements et les suites à donner ;
    - le traitement et la sécurité des médias ;
    - l'échange des données et du logiciel.

4.2.7. Amélioration continue des systèmes d'information

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

4.2.8. Gestion d'accès au système

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

4.2.9. MESURES DE SECURITE RESEAU

4.2.9.1. Segmentation en zone

Fondé sur les résultats de l'analyse de risque, be-invest a segmenté son réseau en zones séparées (fonctionnellement, logiquement ou physiquement). Des mesures de contrôle similaire sont mis-en place pour l'ensemble des éléments d'une même zone. Chaque système de l'IGC est exploité dans une zone réseau sécurisée et est installé suivant des procédures et une configuration assurant une exploitation sécurisée.
Les systèmes les plus critiques, tels que les AC Racines, sont opérés dans les zones les plus sécurisées.

be-invest a également mis en place une séparation stricte entre les systèmes de production et les autres systèmes (test, qualification,…)

4.2.9.2. Interconnexion

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

L'AH garantit que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement et logiquement sécurisé.

Les accès et les communications en les zones sont restreints. Les connexions et services non nécessaires sont désactivés ou interdits. L'ensemble des règles sont revues régulièrement.

De plus, les échanges entre composantes au sein de l'IGC be-ys font l'objet de la mise en place de canaux sécurisés logiquement distincts et permettant d'assurer l'authentification de la destination des données et d'assurer l'intégrité et la confidentialité des données échangées. De plus, les échanges entre composantes au sein de l'IGC be-invest font l'objet de la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés notamment).

4.2.9.3. Connexions

Seuls les personnels en rôle de confiance ont accès aux zones réseaux sécurisées. De plus, les échanges entre composantes au sein de l'IGC be-invest font l'objet de la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés notamment).
Les réseaux permettant d'opérer et d'administré l'IGC sont séparés. Le réseau d'administration est dédié à cet usage.

Tous les systèmes de l'AH sont configurés de façon à supprimer ou désactiver les comptes, applications, services et ports qui ne sont pas utilisés pour les opérations de l'IGC.

4.2.9.4. Disponibilité

Afin de répondre aux besoins de disponibilité de ses composantes, be-invest a mis en place des mesures de redondances permettant d'offrir une haute disponibilité des services critiques.

4.2.9.5. Scan de vulnérabilité

be-invest réalise régulièrement des scans de vulnérabilité sur ses adresses IP publiques et privées. Chaque scan est réalisé par une personne ou une entité qualifiée et indépendante.
Toute vulnérabilité critique est adressée dans les 48h après sa découverte. Les vulnérabilités font l'objet d'un plan de remédiation. S'il est jugé que des mesures de remédiation ne sont pas justifiées, l'AH consigne cette décision et ses justifications dans un rapport.

4.2.9.6. Test d'intrusion

be-invest réalise des tests d'intrusion lors de la mise en place de nouvelles infrastructures ou lors de modification significatives d'une composante.
Les tests de pénétration sont réalisés par des personnels, internes ou externes ayant la qualification et les qualités nécessaires, en particulier en termes de compétences, de connaissance des outils, d'efficacité, d'éthique et d'indépendance.

4.3 EXIGENCES ORGANISATIONNELLES

4.3.1. Rôles de confiance

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

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

L'AH a également défini des porteurs de secrets pour l'accès aux opérations sensibles sur le boîtier cryptographique stockant les clés privées des unités d'horodatage. Le regroupement d'un sous-ensemble de ces porteurs est nécessaire pour la réalisation de ces opérations.
Pour pouvoir réaliser les opérations d'exploitation et de supervision de l'infrastructure réseau et system, be-invest appuie sur ses équipes internes.
L'attribution des rôles est réalisée sur le principe de la séparation des rôles et du moindre privilège, en prenant en compte la sensitivité des droits et les niveaux d'accès.

4.3.2. Identification et authentification pour chaque rôle

Des mesures d'identification et d'authentification sont mises en place afin de supporter la mise en oeuvre de la politique de contrôle d'accès et la traçabilité des opérations ; la politique de contrôle d'accès limite l'accès aux seules personnes autorisées conformément à leur besoin d'en connaître.
Les rôles attribués concernant les services d'horodatage sont notifiés aux personnes concernées par l'autorité de gouvernance. Les personnels ne se voient pas attribuer leurs accès tant que la nomination n'est pas effective et que les vérifications d'antécédents ne sont pas réalisées.

4.3.3. Mesures de sécurité vis à vis du personnel

4.3.3.1. Qualifications, compétences, et habilitations requises

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

4.3.3.2. Procédures de vérification des antécédents

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

4.3.3.3. Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement. Cela concerne essentiellement le personnel opérant sur les composantes du service d'horodatage.
Les personnels participant au service d'horodatage ont notamment des connaissances sur les thèmes suivants :

- Sécurité de l'information
- Protection des données personnelles
- Technologie et fonctionnement de l'horodatage ;
- Technologie et principe de la signature électronique ;
- Connaissance des principes de calibration et de synchronisation des horloges de temps ;
- Connaissance et respect des règles de sécurité pour les personnels techniques.

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

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants.
Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.
De plus, les personnels en rôle de confiance assistent, au moins annuellement, à une formation sécurité incluant :

- Une présentation des nouvelles menaces ;
- Une présentation des pratiques de sécurité en vigueur.

4.3.3.5. Sanctions en cas d'actions non autorisées

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

4.3.3.6. Exigences vis à vis du personnel des prestataires externes

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

4.3.3.7. Documentation fournie au personnel

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

5. EXIGENCES DE SECURITE TECHNIQUES

5.1 EXACTITUDE TEMPS

L'AH garantit que son horloge est synchronisée sur des serveurs Ntp avec le temps UTC selon l'exactitude déclarée de une seconde.
Les serveurs ntp sont autonomes et bénéficient d'une procédure de synchronisation avec des sources GPS, DCF77, et références UTC(k).
Les serveurs ntp font l'objet de mesures de protection (tel que des mesures de restriction d'accès, de protection électrique, …) afin de les protéger contre des attaques permettant de faire dériver l'horloge hors de son exactitude nominale. De plus, des mesures de détection sont en place sur les unités d'horodatage pour détecter des comportements anormaux (par exemple : retour en arrière de l'horloge).

La précision des horloges est maintenue, même en cas d'occurrence d'une seconde intercalaire. L'AH met en place des procédures de suivi des secondes intercalaires et intervient sur les UH si nécessaire en cas d'occurrence.

5.2 GENERATION DE CLE

L'AH garantit que les clés cryptographiques des UH sont produites dans des circonstances et un environnement contrôlé. La protection de ces clés s'appuie sur des HSM Cryptographiques ayant fait l'objet d'une certification de conformité (voir §5.3).
Lors de cette génération, les clés privées d'UH ne sont pas exportable de ces ressources.
La génération des clés privées des unités d'horodatage est réalisée durant une cérémonie des clés qui fait l'objet d'un procès-verbal. Les clés sont générées par aux moins deux personnels autorisés en rôle de confiance.
Les modules des clés privées d'UH ont une longueur de 3072 bits pour l'algorithme RSA.

5.3 CERTIFICATION DES CLES DE L'UNITE D'HORODATAGE

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

Ce sont les AC « BE-YS CUSTOMER SERVICES CA NB », et « BE-YS SIGNATURE AND AUTHENTICATION CA NC »de l'IGC be-ys qui est chargée de la génération des certificats des UH. Ces ACs émettent des certificats d'horodatage en conformité avec les normes ETSI EN 319411-1 et ETSI EN 319411-2.
La demande de certificat envoyée auprès de l'AC contient, en plus des informations exigées dans la PC de l'AC pour la partie enregistrement, au moins les informations suivantes :

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

La longueur des clés de l'AH est de 3072 bits minimum. L'algorithme de signature mis en œuvre est RSA avec Sha-2 (avec SHA-256 minimum).

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

L'unité d'horodatage n'émet aucun jeton avant l'importation et la vérification effective du certificat. La clé privée de l'unité d'horodatage n'est pas utilisée pour un autre usage que la génération de jetons d'horodatage.

5.4 PROTECTION DES CLES PRIVEES DES UNITES D'HORODATAGE

Les clés privées des UH sont stockées dans un HSM certifié Critères Commun EAL4+ et/ou FIPS 140-2 niveau 3.

5.5 EXIGENCES DE SAUVEGARDE DES CLES DES UNITES D'HORODATAGE

Une sauvegarde la partition HSM contenant les clés de chaque UH est effectuée lors de la KC. Cependant, l'AH assure qu'une seule clé privée est active dans un HSM à un instant donné. La sauvegarde, le stockage et la restauration des copies de sauvegarde des clés d'UH ne peuvent être réalisés que par au moins deux personnels autorisés en rôle de confiance dans un environnement sécurisé. Toute les copies de secours font l'objet de mesures de sécurité permettant d'assurer leur intégrité et leur confidentialité et ne peuvent être exportées du HSM que sous forme chiffrée.

5.6 DESTRUCTION DES CLES DES UNITES D'HORODATAGE

Les clés de signature des UH sont détruites à la fin de leur cycle de vie.
La destruction consiste à détruire les clés dans les HSM ainsi que toutes les copies de secours.
Les clés sont également effacées du HSM si celui-ci fait l'objet d'un dé-commissionnement.

5.7 ALGORITHMES OBLIGATOIRES

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

Les contremarques de temps sont signées selon les algorithmes et les longueurs de clé conformes aux exigences des autorités compétentes en la matière. La bi-clé de l'UH est une bi-clé RSA de 3072 bits Minimum. L'algorithme de signature utilise une fonction de hachage SHA-256 Minimum.

5.8 VERIFICATION DES CONTREMARQUES DE TEMPS

Les jetons d'horodatage peuvent être vérifiés de manière autonome pendant une durée maximale de 3ans.
L'AH garantit que les Utilisateurs de contremarques de temps peuvent avoir accès à l'information utilisable pour vérifier la signature numérique des Contremarques de temps. En particulier :

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

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

La durée de validité des certificats des UH n'est pas plus longue que la fin de validité du certificat de l'ACqui l'a émis.

Par défaut, cette durée est de 3 ans minimum.

5.10 DUREE D'UTILISATION DES CLES PRIVEES DES UH

La durée de vie minimale des clés privées des UH est de 2 ans, et au maximum 2 ans et 3 mois.
Le renouvèlement de certificat d'une UH s'effectue dans les trois (3) mois, au-delà des deux (2) ans de durée de vie du certificat de l'UH.
Une fois la période de validité dépassée, l'unité d'horodatage rejette toutes les demandes de jetons tant que le certificat n'est pas renouvelé.

5.11 PROFIL CERTIFICAT ET CONTREMARQUE DE TEMPS

5.11.1. Format du certificat d'horodatage

5.11.1.1. Profil ETSI 319411-1 LCP

tbsCertList		Valeur
version		2 (c'est-à-dire version3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OI=organization Identifier O=organizationName C=countryName		OI = VATLU-LU29222134 CN = BE-YS CUSTOMER SERVICES CA NB O = BE INVEST International S.A. C = LU
validity		
▶ notBefore		Date de création
▶ notAfter		notBefore + 3 ans
subject CN=commonName OI=organization Identifier OU=organizationalUnitName O=organizationName C=countryName		OI = VATLU-LU29222134 CN = BE INVEST TIMESTAMP UNIT X OU = TIMESTAMPING SERVICES O = BE INVEST International S.A. C = LU
subjectPublicKeyInfo		
▶ algorithm ➥ algorithm ➥ parameters		rsaEncryption RSAParams : NULL
▶ subjectPublicKey		RSAPublicKey (3072 bits)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
▶ authorityKeyIdentifier	Non	hash de la clé publique de l'issuer
▶ subjectKeyIdentifier	Non	hash de la clé publique du sujet
▶ keyUsage	Oui	digitalSignature (0)
▶ privateKeyUsagePeriod		Extension non utilisée
▶ certificatePolicies	Non	Stratégie du certificat : Identificateur de stratégie = 1.3.6.1.4.1.48620.41.1.5.2.1.2.1
▶ basicContraints	Non	false

⮡ cA ⮡ pathLenConstraint		None
▶ extKeyUsage	oui	id-kp-timestamping
▶ cRLDistributionPoints	Non	Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/almeryscustomerservicescanb.crl
Private extensions		
▶ authorityInfoAccess	Non	[1] : accessMethod : id-ad-caIssuers accessLocation : http://pki.almerys.com/almeryscustomerservicescanb.cer [2] accessMethod : id-ad-ocsp accessLocation : http://ocsp.almerys.com
▶ subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

5.11.1.2. Profil ETSI 319411-2

tbsCertList		Valeur
version		2 (c'est-à-dire version 3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OI=organisationIdentifier O=organizationName C=countryName		OI = VATLU-LU29222134 CN = BE-YS SIGNATURE AND AUTHENTICATION CA NC O = BE INVEST International S.A. C = LU
validity		
▶notBefore		Date de création
▶notAfter		notBefore + 3 ans Maximum
subject CN=commonName OU=organizationalUnitName OI= organisationIdentifier O=organizationName C=countryName		 OI = VATLU-LU29222134 CN = BE INVEST TIMESTAMP UNIT X OU = TIMESTAMPING SERVICES O = BE INVEST International S.A. C = LU
subjectPublicKeyInfo		
▶algorithm ⮡algorithm		 rsaEncryption

⮑parameters		RSAParams : NULL
▶subjectPublicKey		DER encoded RSAPublicKey (3072 bits)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
▶authorityKeyIdentifier	Non	**hash de la clé publique de l'issuer**
▶ subjectKeyIdentifier	Non	**hash de la clé publique de l'issuer**
▶keyUsage	Oui	digitalSignature (0)
▶privateKeyUsagePeriod		Extension non utilisée
▶certificatePolicies	Non	Stratégie du certificat : Identificateur de stratégie = 1.3.6.1.4.1.48620.41.1.7.3.1.5.1
▶ Qualified Certificate Statements	Non	- id-etsi-qcs-QcCompliance true
		-id-etsi-qcs-QcSSCD False
		-id-etsi-qcs-QcPDS URL = http://pki.almerys.com/intermediate/almeryssignatureandauthenticationcanc/PDS/almeryssignatureandauthenticationcanc-PDS.pdf
		-id-etsi-qcs-QcType id-etsi-qct-eseal
▶basicContraints ⮑cA ⮑pathLenConstraint	Non	 false None
▶extKeyUsage	oui	Timestamping
▶cRLDistributionPoints	Non	Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/almerysauthenticationandsignaturecanc.crl
Private extensions		
▶authorityInfoAccess	Non	[1] : accessMethod : id-ad-caIssuers accessLocation : URL=http://pki.almerys.com/ almerysauthenticationandsignaturecanc.cer [2] accessMethod : id-ad-ocsp accessLocation : http://ocsp.almerys.com
▶subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

5.12 FORMAT DE LA CONTREMARQUE TEMPS

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

NOTA : le certificat de l'unité d'horodatage est inclus dans le jeton.

6. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

6.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Un contrôle de conformité à la PH en vigueur lors de la mise en œuvre opérationnelle du système, et lors de toute modification significative est effectué.
be-invest bénéficie de plusieurs types d'audit :
– un audit interne/ou audit de surveillance réalisé par des prestataires externes spécialistes du domaine du SH;
– un audit de qualification réalisée par un organisme accrédité au moins une fois tous les deux ans.

6.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

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

6.3 AUTRES ELEMENTS DE CONFORMITE

Les pratiques de l'AH sont non-discriminatoires. Dans la mesure du possible, l'AH mettra en œuvre toutes les dispositions nécessaires pour rendre accessible son service aux personnes en situation de handicap.

7. ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

7.1 REGLEMENTATION

Renvoi	Document
[RGPD]	Réglement européen n° 2016/679 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, et abrogeant la directive 95/46/CE.
[REG_eIDAS]	Règlement eIDAS

7.2 DOCUMENTS TECHNIQUES

Renvoi	Document
[ETSI_319401]	General Policy Requirements forTrust Service Providers
[ETSI EN 319421]	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[ETSI EN 319422]	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol andtime-stamp token profiles
[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".