Code de pratique et procédures

de l'Autorité d'horodatage 2

CERTSIGN

Version 2.9

Date : 31 janvier 2022

Niveau de sécurité

Document public

Remarque importante

Adresse. 29A Boulevard Tudor Vladimirescu,

AFI Tech Park 1, Bucarest, Roumanie

Téléphone : 0 805 98 80 04

Web : www.certsign.fr

Historique des documents

Version	Date	Motiv	La personne qui a effectué le changement
1.0	Janvier 2017	Publication de la première version	Responsable des services électroniques
2.0	Mars 2017	Deuxième version après l'audit à mi-parcours	Responsable de la sécurité de l'information
2.1	Avril 2017	Mise à jour mineure pour clarification	Responsable de la sécurité de l'information
2.2	Février 2018	Examen annuel	Responsable de la sécurité de l'information
2.3	Novembre 2018	Mise à jour en raison d'un changement de lieu	Responsable des politiques de l'ICP
2.4	Janvier 2019	Examen annuel	Responsable des politiques de l'ICP
2.5	Mars 2019	Mise à jour mineure pour clarification	Responsable des politiques de l'ICP
2.6	Avril 2019	Mise à jour mineure pour clarification	Responsable des politiques de l'ICP
2.7	Janvier 2020	Examen annuel	Responsable des politiques de l'ICP
2.8	Janvier 2021	Examen annuel	Responsable des politiques de l'ICP
2.9	Janvier 2022	Examen annuel	Responsable des politiques de l'ICP

Ce document a été créé par et est la propriété de :

Propriétaire	Auteur	Date de création
Responsable de la sécurité de l'information	Responsable de la sécurité de l'information	Décembre 2016

Liste de distribution

Destination	Date de la distribution
Internet public	Janvier 2017
Internet public	Mars 2017
Internet public	Avril 2017
Internet public	Février 2018
Internet public	Novembre 2018
Internet public	Janvier 2019
Internet public	Mars 2019
Internet public	Avril 2019
Internet public	Janvier 2020
Internet public	Janvier 2021
Internet public	Janvier 2022

Ce document a été approuvé par :

Version	Nom	Date
1.0	Comité de gestion des politiques et procédures	Janvier 2017
2.0	Comité de gestion des politiques et procédures	Mars 2017
2.1	Comité de gestion des politiques et procédures	Avril 2017
2.2	Comité de gestion des politiques et procédures	Février 2018
2.3	Comité de gestion des politiques et procédures	Novembre 2018
2.4	Comité de gestion des politiques et procédures	Janvier 2019
2.5	Comité de gestion des politiques et procédures	Mars 2019

2.6	Comité de gestion des politiques et procédures	Avril 2019
2.7	Comité de gestion des politiques et procédures	Janvier 2020
2.8	Comité de gestion des politiques et procédures	Janvier 2021
2.9	Comité de gestion des politiques et procédures	Janvier 2022

Contenu

1 Objectif

Ce document constitue la politique d'horodatage CERTSIGN et le code de pratique et de procédures de l'Autorité d'Horodatage CERTSIGN (TSPS). Vous devez lire le TSPS sur http://www.certsign.fr/ressources avant de demander le service d'horodatage CERTSIGN 2. L'objet de ce document est de spécifier la politique et les exigences de sécurité relatives aux pratiques d'exploitation et de gestion de CERTSIGN en tant qu'Autorité d'Horodatage conformément à la norme ETSI EN 319 421 « Policy and security requirements for trusted service providers issuing time stamps » (ci-après dénommée CERTSIGN Time Stamping Authority 2 ou CERTSIGN TSA) pour l'émission d'horodatages qualifiés. Ils peuvent être utilisés à l'appui des signatures électroniques ou pour toute application nécessitant la preuve de l'existence d'un horodatage antérieur à une certaine période.
Cette version de la PHS a été approuvée pour utilisation par le Comité de Gestion des Politiques et Procédures de CERTSIGN et peut être modifiée conformément aux politiques et directives adoptées de temps à autre par le Comité de Gestion des Politiques et Procédures de CERTSIGN, Section 6.2.9. La date à laquelle cette version de la PHS entre en vigueur est indiquée dans ce document.

2 Références

2.1 Références normatives

1. Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur et abrogeant la directive 1999/93/CE.
2. IETF RFC 3161 « Protocole d'infrastructure à clé publique X.509 de l'Internet pour les horodatages ».
3. ETSI EN 319 401 : « Signatures électroniques et infrastructures (ESI) ; exigences de politique générale pour les prestataires de services de confiance ».
4. ETSI EN 319 421 : « Signatures électroniques et infrastructures (ESI) ; Politique et sécurité. Exigences pour les prestataires de services de confiance émettant des horodatages ».
5. ETSI EN 319 422 : « Signatures et infrastructures électroniques (ESI) ; Profils de protocole temporel et de jeton temporel ».

2.2 Références informatives

1. recommandations UIT-R TF. 460-6 (2002) : « Émissions de fréquences et de temps standard ».
2. IETF RFC 5905 : « Network Time Protocol Version 4 : Protocol Specifications and Algorithms ».
3. Conditions générales pour les clients de timestamp sur www.anf.es
4. ISO/IEC 19790:2012 : « Technologies de l'information - Techniques de sécurité - Exigences de sécurité pour les modules cryptographiques ».
5. ISO/IEC 15408 (parties 1 à 3) : « Technologies de l'information - Techniques de sécurité - Critères d'évaluation de la sécurité des TI ».
6. FIPS PUB 140-2 (2001) : « Security Requirements for Cryptographic Modules ».

3 Définitions et abréviations

3.1 Définitions

- **Temps universel coordonné (UTC)** : échelle de temps basée sur la seconde telle que définie dans la recommandation UIT-R TF.460-6. À toutes fins utiles, l'UTC est équivalent au temps solaire moyen au méridien d'origine (0°). Plus précisément, l'UTC est un compromis entre le temps atomique extrêmement stable (Temps Atomique International - TAI) et le temps solaire dérivé de la rotation irrégulière de la Terre. L'UTC est la principale norme de temps par laquelle le monde entier règle les horloges et l'heure.
- **NTP** : « Network Time Protocol (NTP) est un protocole réseau permettant de synchroniser les horloges des systèmes informatiques en acheminant des paquets réseau avec une latence variable. La norme de référence est l'IETF RFC 1305 (Network Time Protocol (NTP v3)).
- **Ministère des communications et de la société de l'information** : à des fins juridiques, déclaré comme la norme nationale de cette unité, ainsi que la maintenance et la diffusion officielles de l'échelle du « Temps universel coordonné ».
- **Entité partenaire** : Le destinataire d'un horodatage qui s'appuie sur cet horodatage.
- **Autorité d'horodatage (TSA)** : est le TSP qui fournit des services d'horodatage en utilisant une ou plusieurs unités d'horodatage.
- **Bénéficiaire** : la personne morale ou physique pour laquelle un horodateur est émis.

- **Horodatage** : Données sous forme électronique qui relient d'autres données électroniques à un moment donné, fournissant la preuve que ces données existaient à un moment donné.
- **Politique d'horodatage** : Un ensemble de règles indiquant l'applicabilité d'un horodatage à une communauté et/ou une classe d'applications d'exigences de sécurité communes. Il s'agit d'un type spécifique de politique de services de confiance tel que défini dans la norme ETSI EN 319 421.
- **Service d'horodatage :** service fiable d'émission d'horodatages.
- **Unité d'horodatage (TSU)** : Ensemble de matériels et de logiciels géré comme une unité et possédant une seule clé de signature d'horodatage active.
- **Prestataire de services de confiance (TSP)** : Entité offrant un ou plusieurs services de confiance.
- **Déclaration de divulgation du TSA** : ensemble de déclarations concernant les politiques et les pratiques d'une AST qui doivent spécifiquement mettre l'accent sur la divulgation aux bénéficiaires et aux entités partenaires, par exemple, pour répondre aux exigences réglementaires.
- **Code de pratique de la TSA** : Déclaration des pratiques utilisées par la TSA pour émettre des horodateurs.
- **Système TSA** : ensemble de produits et de composants informatiques utilisés pour soutenir la prestation de services d'horodatage.
- **UTC (k)** : échelle de temps donnée par le laboratoire « k » et qui a une relation étroite avec l'UTC, visant à atteindre ± 100 ns.
- **CERTSIGN TSA :** Représente la « CERTSIGN Time Stamp Authority 2 », qui est l'autorité d'horodatage CERTSIGN fonctionnant conformément à la norme ETSI EN 319 421 « Policy and security requirements for trusted service providers issuing time stamps ».

3.2 Abréviations

Aux fins du présent document, les abréviations sont les suivantes :

BIPM Bureau International des Poids et Mesures
AC Autorité de certification
FR Technologies de l'information
PPMB Comité de gestion des politiques et procédures
TAI Temps atomique international
TSA Horodatage
TSP Un prestataire de services de confiance
TST Jeton d'horodatage
TSU Unité d'horodatage
UTC Temps universel coordonné

4 Concepts généraux

4.1 Concepts et conditions générales

TSPS Il s'agit d'une description détaillée des conditions de prestation de services, des pratiques de gestion et d'exploitation que CERTSIGN Time Stamping Authority 2 applique dans le cadre de la prestation de services d'horodatage.

4.2 Services d'horodatage

La prestation de services d'horodatage est décomposée, dans le présent document, en services composants suivants aux fins de la classification des exigences :

- **Prestation d'horodatages** : ce composant de service génère des TST.
- **Gestion de l'horodatage** : le composant de service qui surveille et contrôle le fonctionnement des services d'horodatage afin de s'assurer que le service fourni est conforme aux spécifications de la CPS et de la TSA CPS.

CERTSIGN TSA adhère aux normes et règlements énoncés dans la section 2 du présent document afin de maintenir la fiabilité des services d'horodatage pour les bénéficiaires et les entités partenaires.

4.3 Parties des services d'horodatage

4.3.1 Autorité d'horodatage (TSA)

Un prestataire de services de confiance (TSP) qui fournit des services d'horodatage au public est appelé Autorité d'horodatage (TSA). L'AH a la responsabilité globale de fournir les services d'horodatage identifiés dans la clause 4.2. L'AH est responsable de l'exploitation d'une ou plusieurs TSU qui créent et signent pour le compte de l'AH. Le TSA responsable de l'émission des horodateurs est identifiable.

TSA CERTSIGN confirme que TSA est audité au moins une fois tous les 24 mois par un organisme d'évaluation de la conformité. Le rapport d'évaluation est envoyé à l'organisme national de surveillance.
Si l'organisme de contrôle demande à la TSA de remédier à une quelconque non-conformité, certSIGN as TSA agira de manière appropriée et en temps voulu.

L'organe de surveillance sera informé de tout changement dans la prestation de l'AST.

TSA CERTSIGN peut faire appel à d'autres parties pour fournir certaines parties des services d'horodatage. Cependant, l'AST assume toujours la responsabilité globale (conformément à la clause 6.5) et s'assure que les exigences de la politique identifiées dans ce document sont respectées.

TSA CERTSIGN peut gérer plusieurs unités d'horodatage identifiables.

TSA CERTSIGN est un prestataire de services de confiance qualifié, tel que décrit dans eIDAS, qui émet des horodateurs.

L'AH CERTSIGN est identifiée dans le certificat du TSU utilisé pour signer la CT.

Coordonnées :
CERTSIGN SA

Adresse. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, Bucarest, Roumanie
Téléphone : 0 805 98 80 04
Web : www.certsign.fr

4.3.2 Bénéficiaire

Si le bénéficiaire est un utilisateur final, ce dernier sera directement responsable s'il ne remplit pas correctement ses obligations.
Si le bénéficiaire est une organisation, elle comprend plusieurs utilisateurs finaux ou un utilisateur final individuel, et certaines des obligations qui s'appliquent à l'organisation doivent également s'appliquer aux utilisateurs finaux. Dans tous les cas, l'organisation sera responsable si les utilisateurs finaux ne remplissent pas correctement leurs obligations ; par conséquent, une telle organisation doit informer ses utilisateurs finaux de manière adéquate.

4.3.3 Entité partenaire TSA

Une entité partenaire est un individu ou une entité agissant en invoquant une TST générée selon la politique CERTSIGN TSA [ETSI EN 319 421]. Une entité partenaire peut ou non être également bénéficiaire.

5 Politiques d'horodatage

5.1 Généralités

TSA CERTSIGN génère des TST conformément à la norme ETSI EN 319 421 et à la politique d'horodatage. Les TST sont émises avec une précision d'une seconde par rapport à l'UTC ou mieux.

5.2 Identification

L'identifiant de la politique d'horodatage spécifié dans ce document est OID :

1.3.6.1.4.1.25017.2.2.1

{iso(1) organisme identifié(3) dod(6) internet (1) privé(4) entreprise(1) CERTSIGN (25017) TSA(2) CPS-PC-EU Règlement 910/2014(2)}

- 1 est le numéro de l'unité TS

En incluant cet identifiant d'objet dans les horodatages générés, TSA CERTSIGN affirme sa conformité avec cette politique d'horodatage.

L'horodatage comprend également l'OID **0.4.0.2023.1.1,** si cela est spécifié dans le contenu de la demande d'horodatage.

5.3 Communauté d'utilisateurs et applicabilité

Cette politique est destinée à satisfaire les exigences de marquage temporel pour la validité à long terme (par exemple, comme défini dans la norme ETSI EN 319 122), mais elle est généralement applicable à toute utilisation qui a une exigence de qualité équivalente. Cette politique peut être utilisée pour les services d'horodatage publics ou pour les services d'horodatage utilisés dans une communauté fermée.

6 Politiques et pratiques

6.1 Évaluation des risques

CERTSIGN TSA effectue régulièrement des évaluations des risques afin de garantir la qualité et la fiabilité des services d'horodatage. Les contrôles de sécurité définis dans un cadre de sécurité pour les services d'horodatage sont vérifiés tous les six mois pour s'assurer de leur efficacité.

Le processus de gestion des risques de CERTSIGN couvre ce sujet en détail.

6.2 Code de pratique et procédures pour les services de confiance

L'assurance de la qualité est l'une des qualités les plus importantes de TSA CERTSIGN. Par conséquent, divers contrôles de sécurité ont été mis en place pour garantir la qualité, les performances et le fonctionnement du service d'horodatage.

Les contrôles de sécurité sont documentés et sont régulièrement vérifiés par une entité indépendante et de confiance capable de vérifier la conformité aux contrôles de sécurité.

En outre, pour la conformité avec la norme ETSI EN 319 421, les mesures suivantes ont été appliquées respectivement aux services suivants :

6.2.1 Format des horodateurs

Le jeton d'horodatage émis par TSA CERTSIGN est conforme à la norme d'horodatage RFC 3161. Le service émet des horodatages avec un algorithme RSA et une longueur de clé de 2048 bits, supportant l'algorithme de hachage SHA256.

6.2.2 Précision du temps

Les TST sont émises avec une précision de 1 seconde de l'UTC ou mieux.

6.2.3 Limites de service

Le service d'horodatage de TSA CERTSIGN peut être utilisé pour toute transaction légale sans limitations. Dans la mesure permise par la loi, certSIGN ne sera en aucun cas responsable (sauf en cas de fraude ou de faute intentionnelle) pour :

- Toute perte de profit ;
- Toute perte de données ;
- Tout dommage indirect, consécutif ou punitif découlant de l'utilisation, de la livraison, de l'octroi de licences et de l'exécution ou de la non-exécution des certificats ou des signatures numériques, ou en rapport avec ceux-ci ;
- Tout autre dommage.

certSIGN n'assume aucune responsabilité financière pour les horodateurs mal utilisés.

certSIGN couvrira les dommages qu'elle pourrait causer du fait de la prestation de services d'horodatage à des personnes qui ont bâti leur conduite morale sur les effets juridiques de certificats qualifiés jusqu'à l'équivalent en lei de la somme de 10 000 euros pour chaque risque assuré.

certSIGN couvrira les dommages qu'elle pourrait causer du fait de la prestation de services d'horodatage à des personnes qui ont bâti leur conduite morale sur les effets juridiques de certificats qualifiés jusqu'à l'équivalent en lei de la somme de 10 000 euros pour chaque risque assuré. Le risque assuré représente chaque dommage causé, même s'il y en a plusieurs, à la

suite d'un manquement du prestataire aux obligations prévues par la loi.

6.2.4 Obligations des bénéficiaires

Pour des informations détaillées, voir « Termes et conditions des services d'horodatage ».

6.2.5 Obligations des entités partenaires

Pour des informations détaillées, voir « Termes et conditions des services d'horodatage ».

6.2.6 Vérification de l'horodatage

La vérification de l'horodatage comprend les éléments suivants :

Vérification de l'émetteur de l'horodateur

L'émetteur est une autorité d'horodatage qui utilise des certificats numériques appropriés pour émettre l'horodatage. Les clés publiques des certificats utilisés sont incluses dans les certificats du TSU et de l'AC et sont publiées pour vérifier que l'horodatage a été signé par l'AH.

Vérification de l'état de révocation de l'horodateur

La vérification de la révocation d'un certificat d'UH est effectuée à l'aide du service OCSP disponible à l'adresse http://ocsp.certsign.ro ou de la LCR disponible à l'adresse http://crl.certsign.ro/certsign-qualifiedca.crl.

Vérification de l'intégrité de l'horodateur

L'intégrité cryptographique de l'horodatage, par exemple la structure ASN.1 est correcte, et un ensemble de données (les données ont été horodatées) appartient à l'application. Cela peut être vérifié par le biais du service web TSA CERTSIGN, qui est proposé gratuitement.

6.2.7 Droit applicable

Pour des informations détaillées, voir « Termes et conditions des services d'horodatage ».

6.2.8 Disponibilité du service

TSA CERTSIGN a mis en place les mesures suivantes pour assurer la disponibilité du service :

- Configuration redondante des systèmes informatiques pour éviter un point de défaillance unique.
- Des connexions Internet haut débit redondantes pour éviter les pertes de service,
- Utilisation d'alimentations sans coupure et d'un générateur électrique.

Bien que ces mesures assurent la disponibilité du service TSA CERTSIGN, une disponibilité annuelle de 100% ne peut être garantie. TSA CERTSIGN a pour objectif de fournir une disponibilité de service de 99% par an.

6.2.9 Procédures d'approbation des PPP

CERTSIGN est responsable, par le biais du Comité de Gestion des Politiques et Procédures, de l'approbation et de la modification des TSPS. Le TSPS est révisé au moins une fois par an.

Les seules modifications que le PPMB peut apporter aux spécifications des SPT sans notification sont des modifications mineures qui n'affectent pas le niveau d'assurance des SPT, par exemple des corrections éditoriales ou typographiques ou des changements de coordonnées.

Les erreurs, les mises à jour ou les suggestions de modification de ce document sont communiquées, y compris une description de la modification, une justification de la modification et les coordonnées de la personne qui demande la modification.

Le PPMB accepte, modifie ou rejette la modification proposée après l'achèvement d'une phase d'examen.

Toute modification du CPP est approuvée par le PPMB et est notifiée aux clients CERTSIGN. Les sujets/bénéficiaires doivent uniquement se conformer aux exigences du CPP actuellement applicables.

Les bénéficiaires doivent uniquement se conformer au document actuellement applicable. Les bénéficiaires qui n'acceptent pas les nouveaux termes et règlements modifiés du TSPS doivent faire une déclaration appropriée dans les 15 jours suivant la date de la nouvelle version de l'approbation du TSPS. Cela entraînera la résiliation du contrat pour les services d'horodatage fournis.

6.3 Modalités et conditions

Le document publié « Conditions d'utilisation des services d'horodatage » contient des informations sur, par exemple, les limites du service, les obligations du bénéficiaire, les informations destinées aux entités partenaires ou les limitations de responsabilité. En outre, les informations suivantes s'appliquent :

6.3.1 Mise en œuvre de la politique de service de confiance

Ce document informe sur la politique applicable au service de confiance. Pour plus de détails, voir le chapitre 5.

6.3.2 Période de conservation des journaux

Les journaux d'événements TSP sont stockés dans des fichiers sur le disque système jusqu'à ce qu'ils atteignent la limite maximale autorisée. Une fois l'espace alloué dépassé, les journaux sont stockés dans des archives et ne sont disponibles que hors ligne. Les journaux archivés sont conservés pendant au moins 10 ans.

6.4 Politique de sécurité de l'information

TSA CERTSIGN a mis en place une politique de sécurité de l'information à l'échelle de l'entreprise. Tous les employés doivent se conformer aux règlements énoncés dans cette politique et aux concepts de sécurité dérivés. La politique de cybersécurité est revue régulièrement, en particulier lorsque des changements importants interviennent. Le Conseil d'administration de CERTSIGN approuve les modifications de la politique de cybersécurité.

6.5 Obligations de la TSA

6.5.1 Obligations de la TSA envers les bénéficiaires

Le respect des procédures énoncées dans ce document est assuré par TSA CERTSIGN. Un organe de contrôle indépendant vérifie régulièrement l'efficacité des procédures.

Ce document n'impose aucune obligation particulière au bénéficiaire au-delà des autres exigences spécifiques de TSA mentionnées dans la clause 11 des Conditions Générales d'Utilisation du Service d'horodatage offert par **CERTSIGN Time Stamping Authority 2.**

6.6 Informations pour les entités partenaires

- Les entités partenaires vérifient que la TST a été signée correctement avec la clé de certificat d'UH appropriée et s'assurent que la clé privée utilisée pour signer la TST n'a pas été révoquée.

- Les entités partenaires sont tenues de prendre toutes les mesures nécessaires pour assurer la validité de la TST au-delà de la durée de vie des certificats CERTSIGN TSA.
- Vous devez tenir compte de toute limitation de l'utilisation de l'horodatage indiquée par la politique d'horodatage.
- Vous devez tenir compte de toutes les autres précautions énoncées dans les accords ou ailleurs.

7 Gestion de la TSA et opérations

7.1 Introduction

TSA CERTSIGN a mis en place un système de gestion de la sécurité de l'information pour maintenir la sécurité du service.

La prestation d'un TST en réponse à une demande est à la discrétion de TSA CERTSIGN, sous réserve de l'accord du bénéficiaire.

7.2 Organisation interne

La structure organisationnelle, les politiques, les procédures et les contrôles de CERTSIGN s'appliquent également à TSA CERTSIGN.

Les procédures organisationnelles suivent les règles et règlements définis dans la section 2.1 de ce document.

a) Entité juridique

L'autorité d'horodatage est fournie par CERTSIGN SA.
CERTSIGN SA est une entreprise technologique spécialisée dans le développement et la production de produits, solutions et services de sécurité de l'information :

CERTSIGN SA
Adresse. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, Bucarest, Roumanie
Téléphone : 004-021-31.19.901
Fax : 004-021-31.19.905

Web : www.certsign.fr

b) La gestion de la sécurité informatique et la gestion de la qualité des services sont effectuées dans le cadre du concept de sécurité des services.

7.3 Un personnel fiable

certSIGN garantit que la personne exerce ses responsabilités professionnelles conformément au rôle qui lui est attribué au sein de l'Autorité d'horodatage :

- Au moins un diplôme d'études secondaires,
- Il est citoyen roumain,
- Il a signé un contrat décrivant son rôle et ses responsabilités au sein du dispositif,
- Il a suivi un programme de formation en adéquation avec ses fonctions et les tâches liées à son poste,
- A été formé à la protection des données personnelles et des informations confidentielles ou privées,
- Signature d'un contrat contenant des clauses sur la protection des informations sensibles (en termes de sécurité certSIGN) et des données privées et confidentielles des Bénéficiaires,
- N'exerce pas d'activités pouvant donner lieu à des conflits d'intérêts.

Les employés certSIGN ayant un rôle de confiance doivent obtenir l'avis de l'administrateur de la sécurité.
Dans certSIGN, les rôles de confiance suivants sont définis, qui peuvent être attribués à une ou plusieurs personnes :

- **Administrateur de la sécurité** - Responsabilité globale de la mise en œuvre des politiques et procédures de sécurité.

- Initie l'installation, la configuration et la gestion des applications logicielles et matérielles de certSIGN (y compris les ressources réseau) ; initie et suspend les services fournis par certSIGN ; coordonne les administrateurs, initie et supervise la génération de clés et de secrets partagés ; approuve les droits de sécurité et les privilèges d'accès des utilisateurs ; vérifie les journaux d'événements ; supervise les audits internes et externes ; reçoit et répond aux rapports d'audit ; supervise la suppression des résultats d'audit.
- Supervise les opérateurs ;
- Vérifie la conformité avec la politique d'horodatage et le code de pratique et de procédures ;
- **Administrateur de système** - Autorisé à installer, configurer et gérer les systèmes et applications de Time Stamp Authority.
- **Opérateur de système** - Responsable du fonctionnement quotidien des systèmes et applications TSA. Autorisé à effectuer les opérations de sauvegarde et de redémarrage du système ; transfère les copies de sauvegarde des archives et des données actuelles hors site à certSIGN.
- **Administrateur HSM** - Gère le module de sécurité et crée des cartes d'opérateur.
- **Operateur HSM** - Démarre l'application d'horodatage.
- **Administrateur du registre électronique** - veille à ce que tous les documents soient établis et conservés conformément à la politique d'horodatage.
- **Auditeur de système** - autorisé à accéder aux archives, aux journaux d'audit des systèmes de confiance de l'autorité de certification. Responsable de la conduite des audits internes de conformité avec le Code de pratiques et de procédures de l'Autorité de certification ; cette responsabilité s'étend également à l'Autorité d'enregistrement opérant au sein de certSIGN.

Nombre de personnes nécessaires pour effectuer une tâche

Le processus de génération de clés - pour la signature des horodateurs - est l'une des opérations qui requiert une attention particulière. Elle nécessite la présence d'au moins deux personnes : un administrateur de sécurité et un administrateur système. Les détenteurs de secrets partagés - qui conservent leur partie de la clé dans un endroit sûr - participent également au processus de génération de clé d'une UH.

La présence de l'administrateur de sécurité et d'un nombre approprié de détenteurs de secrets partagés est également requise lors du chargement de la clé cryptographique dans le module matériel de sécurité.

L'activation de la clé privée requiert le quorum selon le schéma de seuil ; cela signifie que la présence des détenteurs du secret partagé est également requise chaque fois que le service est redémarré.

Toute autre opération ou rôle décrit dans le présent code de pratique peut être effectué par une seule personne spécifiquement désignée à cet effet.

Identification et authentification pour chaque rôle

Le personnel de certSIGN est soumis à une identification et une authentification chaque fois qu'il accède à un système informatique équipé de systèmes de contrôle d'accès. L'identification et l'authentification se font par une ou une combinaison des méthodes suivantes :

- Nom et mot de passe
- Clé privée et code PIN stockés électroniquement

- Clé privée stockée sur un composant matériel (sur un dispositif cryptographique) et PIN
- Carte d'accès avec photo du titulaire
- Chaque compte alloué :
- Il doit être unique et attribué à une personne spécifique,
- Il ne peut être partagé avec aucune autre personne,
- Elle est restreinte, en fonction du poste (découlant du rôle exercé par la personne) sur la base des contrôles du logiciel système, du système d'exploitation et des applications de certSIGN.

Chaque dispositif cryptographique ou carte d'accès utilisateur est remis par l'administrateur de sécurité sur la base d'une déclaration.

Exigences en matière de formation du personnel

Le personnel qui assume des rôles et des activités dans le cadre de l'Autorité d'horodatage doit être formé sur les points suivants :

- Les règlementations du Code de pratique et procédures,
- Politiques d'horodatage,
- Mesures de sécurité actives,
- Applications du logiciel l'Autorité de gestion des horodateurs,
- Responsabilités découlant des rôles et activités entrepris dans le cadre du systeme.

Sanctions pour les actions non autorisées

Si un accès non autorisé est découvert ou suspecté, l'administrateur de la sécurité enquêtera sur l'incident et pourra refuser à une personne l'accès au système certSIGN. Les mesures disciplinaires pour de tels incidents sont décrites dans les politiques et procédures appropriées et sont conformes aux exigences légales.

Personnel contractuel

Le personnel contractuel (services externes, développeurs de sous-systèmes ou d'applications, etc.) respecte les mêmes mesures de sécurité que les employés permanents.
En outre, pendant la période où ils travaillent sur le site certSIGN, les agents contractuels doivent être accompagnés à tout moment par un employé de certSIGN, à l'exception de ceux qui ont été habilités par l'Administrateur de sécurité et qui peuvent accéder à des informations classifiées en interne ou conformément aux règles en vigueur.

7.4 Contrôle de gestion

Toutes les ressources de l'Autorité de gestion des horodateurs (informations, systèmes et applications) sont régulièrement inventoriées et classées en termes de sécurité et d'importance commerciale. Des processus ont été mis en place pour que la gestion de ces ressources (entrée, sortie, stockage, transfert, utilisation) soit strictement contrôlée par des mesures directement proportionnelles à leur importance et à leur classification.

certSIGN utilise un processus de gestion des changements contrôlés. Avant que certSIGN ne soit utilisé en production, chaque application est installée de manière à permettre le contrôle de la version actuelle et à empêcher l'installation non autorisée de logiciels ou l'altération de logiciels existants. Le développement, les essais et la production sont des domaines distincts et le transfert

d'informations et d'applications d'un domaine à l'autre est contrôlé.

Des règles similaires s'appliquent lors du remplacement de composants matériels, tels que :

- Les dispositifs physiques doivent être fournis de manière à permettre le contrôle et l'évaluation du parcours de chaque dispositif sur le site d'installation,
- La livraison d'un dispositif de remplacement physique est similaire à la livraison du dispositif d'origine ; le remplacement est effectué par un personnel qualifié et fiable.

7.5 Contrôle d'accès

L'accès à une ressource est obtenu par un processus contrôlé qui implique les gestionnaires, les administrateurs de système et l'administrateur de sécurité. Le principe du besoin d'en connaître et le principe de la séparation des tâches sont respectés. Les droits d'accès existants sont vérifiés périodiquement pour déterminer s'ils sont adéquats.

Différents niveaux de sécurité en matière d'accès physique et logique assurent le fonctionnement sécurisé du service de marquage temporaire. Par exemple :

- Environnement physique sécurisé
- Séparation des segments de réseau
- Séparation des tâches
- Pare-feu
- Surveillance des réseaux et des services
- Renforcement des systèmes informatiques

Si une personne effectuant des opérations pour les services d'horodatage reçoit un autre rôle ou quitte l'organisation, tous ses jetons de sécurité sont retirés.

Relations avec les tiers

Le processus concerne principalement les relations avec les prestataires de services et son contrôle consiste à assurer la sécurité des informations auxquelles ces prestataires de services ont accès.

Gestion des capacités

Le processus par lequel certSIGN surveille en permanence le chargement des systèmes qui fournissent des services de confiance afin de garantir la qualification et les performances supposées par les politiques et les contrats.

Surveillance

Les systèmes technologiques, les services et le personnel font l'objet d'un contrôle permanent afin de garantir que la sécurité et la qualité du service satisfont les clients et assurent le respect des dispositions légales, des règlements et de leurs propres normes.

Sécurité physique

L'accès physique à certSIGN est contrôlé à la fois par un système de contrôle d'accès par carte de proximité et par des agents de sécurité présents en permanence. Le même système de cartes d'accès contrôle l'accès aux salles où se trouvent les ressources critiques. Des systèmes de détection d'intrusion sont également installés ainsi qu'un système de vidéosurveillance en circuit fermé.

7.6 Contrôles cryptographiques

7.6.1 Génération des clés TSU

La paire de clés TSU est générée par un double contrôle, dans l'emplacement certSIGN, en présence d'un groupe d'administrateurs (selon la matrice des rôles de l'Autorité d'horodatage certSAFE) dans un module de sécurité matériel (HSM) conforme à la norme FIPS PUB 140-2 [I. 9], niveau 3, ou ISO 15408 Critères communs EAL 4+. La clé privée est stockée en permanence sous forme cryptée sur cet appareil et ne quitte jamais l'appareil sous forme non cryptée.

Les actions effectuées lors de la génération de la bi-clé sont enregistrées, datées et signées par chaque personne présente dans le schéma de génération de la bi-clé. Les enregistrements sont conservés à des fins d'audit ou pour des contrôles réguliers du système.

La clé est générée et existe tout au long de son cycle de vie dans un environnement électronique protégé physiquement et électromagnétiquement.

Après avoir généré la paire de clés pour la signature des horodatages et activé la clé privée dans le module matériel de sécurité, elle peut être utilisée pour des opérations cryptographiques jusqu'à ce que sa validité expire ou qu'elle soit compromise.

TSU utilise une paire de clés RSA d'une longueur de 2048 bits. Cette paire de clés est uniquement utilisée pour la signature des TST.

7.6.2 Protection de la clé privée de la TSU

Le module matériel de sécurité utilisé par les autorités de certification est conforme à la norme FIPS PUB 140-2 [I. 9], niveau 3, ou à la norme ISO 15408 Critères communs EAL 4+. La signature électronique est créée en utilisant l'algorithme RSA en combinaison avec le sommaire cryptographique SHA-256.

Le double contrôle d'accès est réalisé en distribuant des secrets aux opérateurs autorisés. Les secrets sont stockés sur des cartes ou des jetons cryptographiques, protégés par un code PIN et transférés de manière authentifiée à leurs détenteurs.

Pour les opérations telles que l'initiation du module cryptographique matériel et le transfert de la clé privée, un schéma de seuil d'accès (de type k sur n) est mis en œuvre en partageant les secrets.

Le nombre total de secrets partagés est de 3, et le nombre requis de secrets permettant l'accès à la clé privée est de 2.

La procédure de transfert du secret partagé implique la présence du détenteur du secret tout au long du processus de génération de la clé et pendant sa distribution, l'acceptation du secret donné et les responsabilités découlant de sa préservation.

Avant de recevoir sa part du secret, chaque détenteur du secret partagé doit être présent en personne lors du partage du secret pour vérifier l'exactitude du secret créé et de sa distribution. Chaque partie du secret partagé doit être transférée au titulaire sur une carte cryptographique protégée par un code PIN, choisi par le titulaire et connu de lui seul.

La création et la réception du secret partagé sont confirmées par une signature manuscrite sur un formulaire dont une copie est conservée dans les archives de l'Autorité de certification et par le détenteur du secret.

Les détenteurs du secret partagé doivent protéger leur part contre toute divulgation. Le titulaire déclare qu'il :

- ne divulguera pas, ne copiera pas et ne partagera pas le secret avec quiconque et n'utilisera pas sa part du secret d'une manière non autorisée,
- ne révèlera pas (directement ou indirectement) qu'il est le détenteur du secret

Le détenteur du secret partagé doit s'acquitter de ses devoirs et obligations tels que requis par le présent code de pratique et de procédure de manière responsable dans toutes les situations possibles. Le titulaire d'un secret partagé doit informer l'émetteur du secret en cas de vol, de perte, de divulgation non autorisée ou de compromission de la sécurité du secret immédiatement après l'incident. Le propriétaire d'un secret partagé n'est pas responsable de l'inexécution de ses devoirs/obligations pour des raisons indépendantes de sa volonté, mais il est responsable de la divulgation inopportune du secret ou de l'omission de notifier à l'émetteur du secret une divulgation inopportune ou une violation de la sécurité du secret résultant de l'erreur, de la négligence ou de l'irresponsabilité du propriétaire.

L'Autorité d'horodatage certSAFE crée une copie de sauvegarde des clés privées utilisées pour signer les horodatages. e. Les copies sont utilisées en cas de mise en œuvre de procédures de récupération des clés en cas d'urgence (par exemple, en cas de catastrophe). Les copies des clés privées sont protégées par le secret partagé créé lors de la génération des clés initiales.

L'opération d'insertion d'une clé privée dans un module cryptographique s'applique dans les cas suivants :

- Parfois, lors de la création de sauvegardes de clés privées stockées dans un module cryptographique (par exemple, en cas de compromission ou de défaillance du module), il peut être nécessaire d'entrer une paire de clés dans un module de sécurité différent,
- Lorsqu'il est nécessaire de transférer une clé privée du module opérationnel utilisé pour les opérations standard de l'entité vers un autre module ; cela peut se produire lorsque le plan de reprise après sinistre est invoqué ou lorsque le module opérationnel doit être détruit.

L'introduction d'une clé privée dans un module de sécurité est une opération critique ; par conséquent, des mesures et des procédures doivent être mises en place pour empêcher la divulgation, la modification ou la falsification de la clé privée.

L'introduction d'une clé privée dans le module de sécurité matériel du TSUTS de l'Autorité d'horodatage certSAFE nécessite la restitution de la clé à partir des cartes en présence d'un nombre suffisant de détenteurs de secrets partagés protégeant le module contenant les clés privées.

La méthode d'activation de la clé privée utilisée lors de la signature des horodateurs fait référence à l'activation de la clé avant toute utilisation de celle-ci.

Pendant l'importation, la génération ou la restauration, la clé privée des TSU est désactivée. La clé est activée lorsque le service est lancé.

Une fois activée, une clé peut être utilisée pendant que le service est en cours d'exécution. Lorsque le service est désactivé, la clé est désactivée.

L'activation des clés privées est toujours précédée d'une authentification de l'opérateur. L'authentification se fait sur la base d'une carte cryptographique détenue par l'opérateur. Après avoir inséré la carte dans le module cryptographique et utilisé le code PIN, la clé privée reste active jusqu'à ce que la carte soit retirée du module.

La méthode de désactivation de la clé privée consiste à désactiver la clé après son utilisation ou à la fin d'une session dans laquelle la clé a été utilisée.

Pour la clé privée du TSU, la désactivation est effectuée lorsque le service est arrêté pour une quelconque opération.

La protection matérielle de la clé privée fait référence au fait que la clé n'est jamais disponible en clair, pas même dans la mémoire de l'application.

Dans le cas de certSIGN, la désactivation d'une clé privée est effectuée par des personnes ayant un rôle de confiance, mais uniquement dans les cas où le service est hors service pour des mises à jour, de la maintenance ou d'autres raisons.

7.6.3 Certificat de clé publique d'TSU

L'AH garantit l'intégrité et l'authenticité des clés (publiques) de vérification de signature du TSU de la manière suivante :

a) (Les clés publiques pour la vérification des signatures des TSU sont disponibles pour les entités partenaires qui font confiance à un certificat de clé publique. Les certificats sont publiés à l'adresse suivante : https://www.certsign.ro/certificate_digitale/lantul_de_incredere.htm.
b) TSU n'émet pas d'horodatage avant la vérification de sa signature (clé publique). Lorsqu'un certificat est téléchargé vers TSU, l'AH vérifie que le certificat a été correctement signé (notamment en vérifiant le chemin de certification d'une autorité de certification de confiance).
c) Un seul certificat d'UH est émis, avec sa clé privée. d) Les certificats d'UH ne sont pas renouvelés.
d) La validité des informations des certificats des TSU est mise à jour régulièrement et des CRLs ou des services OCSP sont disponibles avec des références situées dans les certificats.

Les horodateurs émis par TSA certSIGN TSA sont des horodateurs électroniques qualifiés selon le Règlement (UE) No 910/2014 [i.4] et le Certificat de Vérification de Signature du TSU (clé publique) est émis par l'AC certSIGN QUALIFIED selon la politique de certification ETSI EN 319 411-2.

7.6.4 Renouvellement des clés des TSU

La durée de vie du certificat du TSU correspond à la période de l'algorithme et de la longueur de clé choisis.
Les clés des TSU auront une durée de vie maximale de 3 ans. Un certificat peut être délivré pour toute la durée de vie prévue. La durée de la classe TUS est limitée par :

- Période de validité du certificat racine de l'entité émettrice.
- Une fois par an ou lors de changements significatifs, la personne exerçant la fonction de « superviseur de la cryptographie » vérifie tous les algorithmes cryptographiques utilisés au sein de la TSA, en s'assurant que chaque algorithme est reconnu comme adéquat
- Si un algorithme est susceptible de provoquer une situation de risque, il ne sera plus considéré comme approprié ; le responsable de la sécurité donnera l'instruction à la TSA de cesser d'utiliser les clés concernées et de télécharger de nouvelles clés.

7.6.5 Gestion du cycle de vie du matériel cryptographique

CERTSIGN TSA assure que :

a) L'intégrité des modules de sécurité cryptographique n'a pas été affectée lors de leur expédition par le fabricant,

b) L'intégrité des modules de sécurité cryptographique n'a pas été affectée pendant le stockage de pré-installation,
c) Leur installation, leur administration et leur fonctionnement ne sont effectués que par du personnel de confiance,
d) Les modules de sécurité cryptographique fonctionnent correctement,
e) Les clés de signature privées stockées sur les modules de sécurité cryptographique sont détruites lorsqu'elles sont retirées de la production.

L'inspection suit les protocoles.

En outre, les dispositions suivantes s'appliquent :

a) L'installation et l'activation des clés de signature des TSU dans le matériel cryptographique ne sont effectuées que par du personnel ayant un rôle de confiance et utilisant au moins un double contrôle dans un environnement physiquement sécurisé.
b) Les clés de signature privées stockées dans un module cryptographique des TSU sont supprimées après la mise hors production de l'appareil d'une manière qui rend pratiquement impossible leur récupération.

7.6.6 Fin du cycle de vie des clés des TSU

Après l'expiration des clés privées, les clés privées du module cryptographique sont détruites de manière à ce qu'il soit impossible de les récupérer.

7.7 Horodatage

7.7.1 Émetteur d'horodatage

TSA CERTSIGN offre des services d'horodatage en utilisant le RFC 3161 « Time Stamping Protocol (TSP) ». L'URL du service est spécifié dans le contrat avec le bénéficiaire. Chaque TSP contient l'identifiant de la politique d'horodatage, un numéro de série unique et un certificat contenant les informations d'identification de l'UTS TSA CERTSIGN.

TSU dans les applications d'horodatage supporte les algorithmes de hachage SHA256 et utilise la fonction de hachage cryptographique SHA-256 pour la signature des TST.

Les clés des TSU sont des clés RSA de 2048 bits. La clé est uniquement utilisée pour signer les TST.

La TSA enregistre tous les TST émis. Les dossiers TST sont conservés pendant une période indéfinie. TSA CERTSIGN peut prouver l'existence d'une TST à la demande d'une entité partenaire. TSA CERTSIGN peut demander à l'entité partenaire de couvrir les coûts d'un tel service.

TSU n'émet plus de TST lorsque la clé privée du TSU atteint la fin de sa période de validité.

7.7.2 Synchronisation de l'horloge avec l'UTC

CERTSIGN garantit que son horloge est synchronisée avec le temps UTC avec une précision d'une seconde ou mieux en utilisant le protocole NTP.

CERTSIGN surveille la synchronisation de son horloge et s'assure que si l'heure indiquée dans une TST dévie ou perd sa synchronisation avec l'heure UTC, cela est détecté. Si l'horloge du TSA perd de sa précision, aucun horodateur n'est émis jusqu'à ce que l'horloge soit synchronisée.

Plus précisément, les sujets suivants sont couverts :

- Calibrage continu de l'horloge du TSU,
- Surveillance de la précision de l'horloge du TSU,
- Analyse des fils contre les attaques sur les signaux temporels

- Comportement lorsque des secondes intercalaires sont sautées/ajoutées
- Comportement en cas d'écart de plus de 1s par rapport au temps UTC

7.8 Sécurité physique et environnementale

Les systèmes informatiques, les terminaux des opérateurs et les ressources d'information des opérateurs certSIGN sont situés dans une zone dédiée, physiquement protégée contre tout accès non autorisé, toute destruction ou perturbation. Ces endroits sont surveillés. Chaque entrée et sortie est enregistrée dans le journal des événements (journaux du système) ; la stabilité de l'alimentation électrique ainsi que la température sont également surveillées et contrôlées.

Localisation

certSIGN est situé à Bucarest, à l'adresse suivante. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, Bucarest, Roumanie

Accès physique

L'accès physique à certSIGN est contrôlé et surveillé par un système d'alarme intégré. certSIGN dispose de systèmes de prévention des incendies, de systèmes de détection des intrusions et de systèmes d'alimentation électrique de secours.

Les locaux de certSIGN sont ouverts au public tous les jours ouvrables entre 10h00 et 18h00. A tout autre moment, l'accès n'est accordé qu'aux personnes autorisées par la direction de certSIGN. Les visiteurs des locaux de certSIGN doivent être accompagnés à tout moment par des personnes autorisées.

Les zones appartenant à certSIGN sont divisées en :

- Zone du serveur,
- Zone des opérateurs,
- Espace administrateurs,
- Zone de développement et d'essai
- Zone de bureaux.

La zone des serveurs est équipée d'un système de sécurité surveillé en permanence, composé de capteurs de mouvement, d'intrusion et d'incendie. L'accès à cette zone est réservé au personnel autorisé, par exemple l'administrateur de la sécurité, l'administrateur du système. Les droits d'accès sont contrôlés à l'aide de cartes et de lecteurs, montés à proximité du point d'accès. Chaque entrée et sortie de la zone est automatiquement enregistrée dans le journal des événements.

Le contrôle d'accès dans la **zone des opérateurs** et des **administrateurs** se fait par le biais de cartes et de lecteurs de cartes. Comme toutes les informations sensibles sont protégées par l'utilisation de coffres-forts et que l'accès aux terminaux des opérateurs et des administrateurs nécessite une autorisation préalable, la sécurité physique dans ce domaine est considérée comme adéquate. Seuls les employés de certSIGN et les personnes autorisées ont accès à cette zone ; ces dernières ne sont pas autorisées à y pénétrer sans être accompagnées.

La zone de développement est protégée de manière similaire à la zone des opérateurs et des gestionnaires. Les projets en cours de réalisation et les logiciels associés sont testés dans l'environnement de développement certSIGN.

Alimentation électrique et climatisation

La zone des opérateurs et des administrateurs ainsi que la zone de développement et de test sont climatisées. À partir du moment où l'alimentation électrique est interrompue, les alimentations de secours (UPS) permettent de poursuivre le travail sans être perturbé jusqu'à ce que le générateur du bâtiment intervienne automatiquement.

Exposition à l'eau

Le risque d'inondation du serveur est faible car la distance aux conduites d'eau est importante. De plus, des capteurs d'inondation sont installés dans les salles de données et sont surveillés 24 heures sur 24 par le personnel de sécurité situé à proximité immédiate des serveurs et qui a pour instruction d'avertir immédiatement l'administrateur certSIGN ou le gestionnaire du bâtiment en cas d'incident.

Prévention des incendies

Le site certSIGN dispose d'un système de prévention et de protection contre l'incendie conforme aux normes et réglementations en vigueur.

Stockage des supports d'information

En fonction de la sensibilité des informations, les supports électroniques contenant les archives et les sauvegardes des données actuelles sont stockés dans des coffres métalliques situés dans une salle de haute sécurité. L'accès à la salle et aux chambres fortes n'est permis qu'aux personnes autorisées.

Elimination des déchets

Les supports papier et électroniques contenant des informations sensibles de sécurité certSIGN doivent être détruits après l'expiration de la période de conservation. Les modules de sécurité matériels doivent être réinitialisés et supprimés conformément aux recommandations du fabricant.

Ces dispositifs sont également réinitialisés et effacés lorsqu'ils sont envoyés au service ou ou réparés.

Stockage hors site des sauvegardes

Les cartes cryptographiques requises pour les services de recouvrement après sinistre sont stockées dans des conteneurs spéciaux situés hors site chez certSIGN.

Le stockage hors site s'applique également aux archives, aux copies actuelles des informations traitées par le système et aux kits d'installation des applications certSIGN. Cela permet de restaurer en urgence toute fonction de certSIGN dans les délais fixés par le plan de continuité de l'activité.

7.9 Sécurité des opérations

Les exigences techniques présentées dans ce chapitre concernent les contrôles de sécurité spécifiques des ordinateurs et des applications utilisés au sein de certSIGN. Des mesures de sécurité ont été prises à tous les niveaux, du niveau physique au niveau des applications.

Les contrôles TSA certSIGN possèdent les caractéristiques de sécurité suivantes :

- l'authentification obligatoire au niveau du système d'exploitation et des applications,
- le contrôle d'accès discrétionnaire,
- la possibilité d'être audité du point de vue de la sécurité,
- l'ordinateur n'est accessible qu'au personnel autorisé avec des rôles certSIGN de confiance,
- la séparation des tâches en fonction du rôle dans le système,
- l'identification et l'authentification des rôles et du personnel qui remplit ces rôles,
- empêcher la réutilisation d'un objet par un autre processus après sa libération par le processus autorisé,
- la protection cryptographique des échanges d'informations et la protection des bases de données,
- l'archivage de l'historique des opérations effectuées sur un ordinateur et des données nécessaires à l'audit,
- un moyen sûr d'identifier et d'authentifier les rôles et le personnel qui les remplit,
- les méthodes de restauration des clés (uniquement pour les modules matériels de sécurité), des applications et du système d'exploitation,
- des moyens de surveillance et d'alerte en cas d'accès non autorisé aux ressources informatiques.
- L'intégrité des systèmes et des informations de TSA doit être protégée contre les virus, les logiciels malveillants et non autorisés.
- Les supports utilisés dans les systèmes TSA doivent être manipulés en toute sécurité pour les protéger contre les dommages, le vol, les accès non autorisés et l'usure morale.
- Les procédures de gestion des supports doivent protéger contre l'usure et la détérioration des supports pendant la période de conservation des enregistrements.

CERTSIGN utilise des systèmes et des produits de confiance qui sont protégés contre la falsification et garantissent la sécurité et la fiabilité technique des processus qu'ils soutiennent.
Une analyse des exigences de sécurité est effectuée au stade de la conception et de la spécification des exigences de tout projet de développement de système entrepris par certSIGN ou au nom de CERTSIGN afin de garantir que la sécurité est intégrée dans les systèmes informatiques.
Chaque application, avant d'être utilisée en production au sein de CERTSIGN, est installée de manière à permettre le contrôle de la version en cours et à empêcher l'installation non autorisée de programmes ou l'altération de programmes existants.
Des règles similaires s'appliquent lors du remplacement de composants matériels, tels que :

- Le matériel est fourni de manière à permettre le suivi et l'évaluation de l'itinéraire du composant jusqu'au site d'installation,
- La livraison du matériel de remplacement est effectuée de manière similaire à la livraison du matériel d'origine ; le remplacement est effectué par du personnel fiable et formé.

L'objectif du contrôle de gestion de la sécurité est de superviser la fonctionnalité des systèmes CERTSIGN en s'assurant que le système fonctionne correctement et conformément à la configuration acceptée et mise en œuvre.
Les contrôles appliqués au système CERTSIGN permettent de vérifier en permanence l'intégrité de l'application, le versioning ainsi que l'authentification et la vérification de l'origine du matériel.
Les politiques et procédures de contrôle des changements sont appliquées aux versions, modifications et corrections logicielles d'urgence de tout logiciel opérationnel et aux changements de configuration qui appliquent la politique de sécurité CERTSIGN.
La configuration réelle du système CERTSIGN, les modifications qui y sont apportées, ainsi que les versions, les modifications et les solutions de contournement de tout logiciel opérationnel sont documentées.

Les configurations des systèmes d'émission d'horodatage, des systèmes de support de sécurité[1] et des systèmes de support frontaux/interne sont examinées au moins une fois par semaine afin de déterminer toute modification qui violerait les politiques de sécurité de CA.
CERTSIGN met en place des procédures de sécurité internes pour s'en assurer :

- Les correctifs de sécurité sont appliqués dans un délai raisonnable après leur mise à disposition ;
- Les correctifs de sécurité ne sont pas applicables s'ils introduisent des vulnérabilités ou des instabilités supplémentaires qui l'emportent sur les avantages de leur application ;
- Les raisons de la non-application des correctifs de sécurité sont documentées.

Le CERTSIGN met en œuvre une procédure interne de gestion de la capacité qui assure le suivi des besoins en capacité de l'infrastructure TIC pour les services TSA et les projections des besoins futurs en capacité afin de garantir la disponibilité d'une capacité d'alimentation et de stockage adéquate.

7.10 Sécurité du réseau

CERTSIGN protège son réseau et ses systèmes contre les attaques. À cette fin et sur la base d'évaluations des risques et des meilleures pratiques, nous mettons en œuvre un ensemble intégré de contrôles de sécurité :

a) Nos systèmes sont segmentés en réseaux ou en zones sur la base de la relation fonctionnelle, logique et physique (y compris l'emplacement) entre les systèmes et services fiables. CERTSIGN applique les mêmes contrôles de sécurité à tous les systèmes co-localisés dans la même zone.

b) L'accès et les communications entre les zones sont limités aux personnes nécessaires au fonctionnement des services de certification. Les connexions et services nécessaires ne sont pas strictement interdits ou désactivés. L'ensemble des règles établies est revu régulièrement.

c) Tous les systèmes critiques pour le fonctionnement des services de certification doivent être conservés dans une ou plusieurs zones sécurisées.

d) Le réseau dédié à l'administration des systèmes informatiques et le réseau opérationnel sont séparés. Les systèmes utilisés pour l'administration de la mise en œuvre de la politique de sécurité ne sont pas utilisés à d'autres fins. Les systèmes de production pour les services de certification sont séparés des systèmes utilisés pour le développement et les essais (par exemple, les systèmes de développement, d'essais et stationnaires).

e) La communication entre des systèmes de confiance distincts ne doit être établie que par des canaux de confiance logiquement distincts des autres canaux de communication, qui assurent une identification sûre de leurs extrémités et une protection des données du canal contre toute modification ou divulgation.

f) Si un niveau élevé de disponibilité de l'accès externe à un service de certification particulier est requis, la connexion au réseau externe doit être redondante pour garantir la disponibilité des services en cas de défaillance d'une unité.

g) Effectuer un scan périodique de vulnérabilité sur les adresses IP publiques et privées identifiées par CERTSIGN et enregistrer les preuves que chaque scan de vulnérabilité a été effectué par une personne ou une entité ayant les aptitudes, les outils, les compétences, le code d'éthique et l'indépendance nécessaires pour fournir un rapport fiable.

[1] Tous les systèmes mentionnés ci-après sont définis dans le document sur les exigences de sécurité des systèmes de réseaux et de certificats de l'AC et du Browser Forum.

h) Les Services de Certification CERTSIGN doivent se soumettre à un test de pénétration des systèmes concernés lors de leur installation et après des mises à jour ou des modifications de l'infrastructure ou des applications que CERTSIGN juge significatives. Les preuves sont enregistrées que chaque test de pénétration a été effectué par une personne ou une entité ayant les compétences, les outils, la compétence, le code d'éthique et l'indépendance nécessaires pour fournir un rapport fiable.

Les serveurs et les postes de travail de confiance du système CERTSIGN sont connectés via un réseau local (LAN), conçu en plusieurs sous-réseaux à accès contrôlé. L'accès de l'Internet à tout segment est protégé par un pare-feu intelligent.

Les contrôles de sécurité sont développés sur la base d'un pare-feu et d'un filtrage du trafic sur les routeurs et les services proxy qui protègent les domaines du réseau interne de CERTSIGN contre tout accès non autorisé, y compris l'accès par les sujets/bénéficiaires et les tiers. Les firewalls sont configurés pour empêcher tous les protocoles et accès qui ne sont pas nécessaires au fonctionnement de CERTSIGN TSA.

La protection de la sécurité du réseau signifie que seuls les messages envoyés par les protocoles http, https, NTP, POP3 et SMTP sont acceptés. Les événements (logs) sont enregistrés dans les journaux du système et permettent de contrôler l'exactitude de l'utilisation des services fournis par CERTSIGN.

CERTSIGN maintient et protège tous les systèmes TSA dans au moins une zone sécurisée et dispose d'une procédure de sécurité qui protège les systèmes et les communications entre les systèmes dans les zones sécurisées et les zones de haute sécurité.

CERTSIGN configure tous les systèmes TSA en supprimant ou en désactivant tous les comptes, applications, services, protocoles et ports qui ne sont pas utilisés dans les opérations TSA.

CERTSIGN accorde l'accès aux zones sécurisées et aux zones de haute sécurité aux seuls rôles de confiance.

7.11 Gestion des incidents

Les activités du système concernant l'accès aux systèmes informatiques, les systèmes des utilisateurs et les demandes de service sont surveillées. En particulier :

a) Les activités de surveillance doivent tenir compte de la sensibilité de toute information collectée ou analysée.

b) Une activité anormale du système indiquant une violation potentielle de la sécurité, y compris une intrusion dans le réseau du TSP, doit être détectée et signalée comme une alarme.

c) Les systèmes informatiques du TSP surveillent les événements suivants : fonctions de connexion et de déconnexion ; disponibilité et utilisation des services requis avec le réseau du TSP.

d) Le TSP agit de manière opportune et coordonnée pour réagir rapidement aux incidents et limiter l'impact des violations de la sécurité. Le TSP nomme des personnes de confiance qui assurent le suivi des alertes d'événements de sécurité potentiellement critiques et veille à ce que les incidents pertinents soient signalés conformément aux procédures du TSP.

e) Le TSP notifie aux entités appropriées, conformément aux règles réglementaires applicables, toute violation de sécurité ou perte d'intégrité ayant un impact significatif sur le service de confiance fourni et les données personnelles qu'il détient.

(f)L'organe national de surveillance est informé dans les 24 heures de la découverte d'une faille de sécurité critique.

g) Les journaux d'audit sont régulièrement contrôlés ou examinés pour identifier les preuves d'activités malveillantes.

h) Le TSP résout les vulnérabilités critiques dans un délai raisonnable après leur découverte. Si

cela n'est pas possible, le TSP créera et mettra en œuvre un plan d'atténuation pour la vulnérabilité critique ou le TSP documentera la base factuelle de la décision que la vulnérabilité ne nécessite pas de remédiation.
i) Des procédures de signalement et d'intervention en cas d'incident sont utilisées afin de minimiser les dommages causés par les incidents et les dysfonctionnements de sécurité.

7.12 Collecte des preuves

Les dossiers du TSP doivent être accessibles pendant une période appropriée, y compris après la fin des activités du TSP. Toutes les informations pertinentes sur les données émises ou reçues par TSP sont sauvegardées pour fournir des preuves dans le cadre de procédures judiciaires et pour assurer la continuité du service. En particulier :

a) La confidentialité et l'intégrité des dossiers courants et archivés relatifs au fonctionnement des services sont maintenues.
b) Les documents relatifs à la gestion des services sont confidentiels et classés conformément aux pratiques commerciales décrites.
(c) Si nécessaire, les documents relatifs à la gestion des services sont mis à disposition afin de prouver le bon fonctionnement des services dans le cadre de procédures judiciaires.
d) Le TSP enregistre à l'heure exacte les événements environnementaux significatifs, la gestion des clés et la synchronisation des horloges. L'heure utilisée pour enregistrer les événements, comme demandé dans le journal d'audit, est synchronisée en permanence avec l'UTC.
e) Les enregistrements de service seront conservés pendant une période après l'expiration de la validité des clés de signature ou de tout jeton de service afin de garantir la fiabilité des preuves légales requises, comme indiqué dans les présentes.
f) Les événements sont enregistrés de manière à ce qu'ils ne puissent être effacés ou détruits (sauf s'ils peuvent être transférés de manière fiable sur un support à long terme).

7.13 Gestion de la continuité des activités

Des copies de sauvegarde de toutes les bases de données TST émises par TSA CERTSIGN sont conservées hors site. Si la clé privée des TSU est compromise ou suspectée de l'être, TSA CERTSIGN en informe les Bénéficiaires et les Entités Partenaires et cesse d'utiliser la clé compromise.
En cas de révocation du certificat du TSU, les actions nécessaires seront prises en accord avec le plan de recouvrement.

En cas de désynchronisation de l'horloge, TSA CERTSIGN suspend ses opérations afin de ne pas causer de dommages supplémentaires. Le plan de reprise est activé pour rétablir la synchronisation et le service.

Le service d'horodatage lui-même se trouve dans un environnement physiquement sécurisé qui minimise le risque de catastrophes naturelles (par exemple, un incendie).

Les clés privées du TSU sont stockées dans un module de sécurité cryptographique.

Si les clés privées sont compromises, l'archive des horodatages sauvegardés permet de différencier les horodatages corrects des faux dans une piste d'audit.

Le HSM est isolé du réseau public et les mesures suivantes seront prises si nécessaire :

- Le responsable de la sécurité sera informé afin de coordonner les mesures à prendre.
- Un audit de sécurité des clés privées restantes sera lancé (contrôles d'intégrité, journal d'analyse des fichiers).
- Les entités partenaires seront informées de l'incident.

- En cas de catastrophe naturelle (par exemple, incendie, tremblement de terre, tempête), s'il y a une perte de service, le service d'horodatage peut être suspendu jusqu'à ce que la reprise après sinistre soit activée.

7.14 Résiliation et plans de résiliation de TSA

Si la TSA cesse son activité pour quelque raison que ce soit, elle en informera l'organe national de surveillance avant de cesser son activité.

-Une notification sera envoyée en temps utile à toutes les entités partenaires afin de minimiser toute perturbation causée par l'arrêt du service.

-En outre, en collaboration avec l'entité de surveillance, le TSP coordonnera les mesures nécessaires pour assurer la conservation de tous les documents archivés pertinents avant la fin du service.

-Les dispositions suivantes s'appliquent également :

a) La TSP mentionne un plan de licenciement actualisé.

b) Avant que le TSP ne cesse ses activités, les procédures suivantes au moins doivent être appliquées :

i. Le TSP informera les personnes suivantes de la fin du service : tous les bénéficiaires et les autres entités avec lesquelles le TSP a des accords ou d'autres relations établies. Ces informations seront mises à la disposition des autres entités partenaires ;

ii. La TSP cessera d'autoriser tous les sous-traitants à agir pour le compte de la TSP dans l'exercice de toute fonction liée aux processus d'émission de jetons des services de confiance ;

iii. Le TSP transférera à une entité de confiance, pour une période raisonnable, ses obligations de conserver toutes les informations nécessaires pour fournir la preuve des opérations du TSP, sauf s'il peut prouver que le TSP n'est pas le détenteur de ces informations ;

iv. Les clés privées du TSP, y compris les sauvegardes, seront détruites, ou retirées de l'utilisation, de manière à rendre impossible leur récupération.

v. TSA CERTSIGN prend les mesures nécessaires pour la révocation des certificats des UH.

vi. Dans la mesure du possible, le TSP utilisera un système qui permet le transfert des services qu'il fournit à son client à un autre TSP.

c) le TSP a conclu un accord pour couvrir les coûts liés au respect de ces exigences minimales en cas de faillite du TSP ou pour d'autres raisons qui empêchent le TSP de couvrir lui-même les coûts, dans la mesure où cela est possible dans les limites de la législation applicable en matière de faillite.

d) le TSP mentionne et transfère à une entité de confiance ses obligations de mettre sa clé publique ou ses jetons de service de confiance à la disposition des entités partenaires pendant une période raisonnable.

7.15 Conformité

CERTSIGN TSA garantit à tout moment le respect de la législation applicable. Plus précisément, il assure la conformité avec :

a) Règlement (UE) n° 910/2014
b) Loi n° 451/2004 sur le marquage horaire
c) ETSI TS 119 421
d) IETF (RFC 3161)

La validation du respect de ces réglementations est effectuée dans le cadre de l'évaluation de

la conformité.