YORYX® TRUST SASU

Politique d’horodatage

YT-PH-TSA

OID : 1.3.6.1.4.1.[PEN].1.1.3

Version 0.1

5 septembre 2026

Projet — en préparation de la déclaration préalable

Diffusion publique

Identification du document

Champ	Valeur
Titre du document	Politique d’horodatage
Identifiant du document	YT-PH-TSA
Identifiant d'objet (OID)	1.3.6.1.4.1.[PEN].1.1.3
Version	0.1
Date de version	2026-09-05
Statut	Projet — en préparation de la déclaration préalable
Classification	Diffusion publique
Éditeur	YORYX® TRUST SASU

Historique des révisions

Version	Date	Auteur	Nature de la modification
0.1	2026-09-05	YORYX® TRUST SASU	Version initiale (projet)

Table des matières

1. Introduction et objet du document....6
1.1. Objet et champ d’application....6
1.2. Présentation du prestataire....6
1.3. Statut réglementaire....7
1.4. Positionnement et canal de fourniture....7
1.5. Mention de marque....8
1.6. Identification du document....8
1.7. Responsabilités, garanties et limites....8
1.8. Terminologie....9
1.9. Documents liés....9
2. Acteurs de l’horodatage....11
2.1. Services d’horodatage....11
2.2. Autorité d’horodatage....11
2.3. Service demandeur....11
2.4. Commission d’approbation....12
3. Politique d’horodatage....13
3.1. Définition....13
3.2. Identification....13
3.3. Conformité....13
3.4. Certificats d’horodatage....14
4. Obligations....16
4.1. Obligation de l’autorité d’horodatage....16
4.2. Obligation de l’opérateur du service d’horodatage....16
4.3. Obligations et responsabilités des services demandeurs....17
4.3.1. Vérification de la validité des jetons dès réception....17
4.3.2. Archivage des jetons d’horodatage....17
4.4. Obligations des utilisateurs finaux....17
5. Exigences concernant les pratiques d’horodatage....18
5.1. Déclaration des pratiques d’horodatage et résumé publiable....18
5.1.1. Déclaration des pratiques d’horodatage de l’opérateur....18
5.1.2. Résumé publiable des politiques....18
5.2. Cycle de vie des clés de l’autorité d’horodatage....18
5.2.1. Génération des clés....18
5.2.2. Protection des clés privées....19

5.2.3. Renouvellement des clés....19
5.2.4. Fin du cycle de vie des clés cryptographiques....20
5.2.5. Gestion du cycle de vie des unités d'horodatage....20
5.3. Production des jetons d'horodatage....20
5.3.1. Jeton d'horodatage....20
5.3.2. Synchronisation avec le temps universel coordonné....21
5.3.3. Disponibilité du service....21
5.4. Validité d'un jeton d'horodatage....22
5.4.1. Durée de validité d'un jeton d'horodatage....22
5.4.2. Vérification d'un jeton par le service demandeur....22
5.5. Gestion et exploitation de l'autorité d'horodatage....22
5.5.1. Gestion de la sécurité....22
5.5.2. Classification des biens....22
5.5.3. Sécurité du personnel....23
5.5.4. Sécurité physique....23
5.5.5. Sécurité d'exploitation....24
5.5.6. Zonage des locaux....24
5.5.7. Gestion des accès aux composantes du système d'horodatage....24
5.5.8. Maintenance et déploiement....24
5.5.9. Mesures à prendre en cas de compromission....24
5.5.10. Fin du cycle de vie de l'autorité d'horodatage....25
5.5.11. Données enregistrées par l'autorité d'horodatage....25
6. Administration de la politique d'horodatage....27
6.1. Procédures de modification de la politique d'horodatage....27
6.2. Procédures de publication et de notification....27
7. Dispositions juridiques et diverses....29
7.1. Protection des données à caractère personnel....29
7.2. Conditions financières....29
7.3. Réclamations, droit applicable et règlement des litiges....30
7.4. Points ouverts....30
8. Annexes....31
8.1. Profil du jeton d'horodatage....31
8.2. Profil du certificat d'unité d'horodatage....32
8.3. Algorithmes et longueurs de clés....32
8.4. Correspondance avec la norme ETSI EN 319 421....33

9. Références..... 35
9.1. Textes législatifs et réglementaires..... 35
9.2. Référentiels de l’autorité nationale..... 36
9.3. Normes et spécifications techniques visées..... 37

1. Introduction et objet du document

1.1. Objet et champ d’application

La présente politique d’horodatage définit les règles que YORYX TRUST SASU s’impose pour la fourniture de son service d’horodatage électronique, ainsi que les engagements qu’elle prend à l’égard des services demandeurs et des utilisateurs finaux. Elle énonce ce qui est fait et pourquoi ; les modalités opérationnelles correspondantes — comment cela est fait — relèvent de la déclaration des pratiques, publiée séparément.

Le service objet du présent document est : « Horodatage électronique simple ». Il relève des services de confiance énumérés à l’article 3 de la loi n° 43-20 et est fourni en dehors du régime des services qualifiés.

Le service est identifié, pour les besoins de la déclaration préalable, par l’identifiant d’objet 1.3.6.1.4.1.[PEN].1.1.3.1, et la norme visée est la norme ETSI EN 319 421.

L’horodatage électronique qualifié au sens de la loi n° 43-20 n’est pas fourni. Il constitue une cible, ouverte après agrément par l’autorité nationale.

La présente politique s’applique à l’ensemble des jetons d’horodatage délivrés sous l’identifiant d’objet 1.3.6.1.4.1.[PEN].1.1.3.1, quelle que soit l’origine de la demande. Elle ne s’applique ni aux certificats de signature électronique, régis par YT-PC-SIGN (OID 1.3.6.1.4.1.[PEN].1.1.1), ni aux certificats de cachet électronique, régis par YT-PC-SEAL (OID 1.3.6.1.4.1.[PEN].1.1.2).

La politique d’horodatage suit le plan type détaillé de l’annexe 9.8 de la PC-type de la DGSSI, complété par le chapitre 6 de la norme ETSI EN 319 421.

1.2. Présentation du prestataire

Le présent document est publié par YORYX TRUST SASU, société par actions simplifiée à associé unique (SASU), au capital de 100 000,00 dirhams, intégralement libéré en numéraire, immatriculée au registre du commerce tenu par le tribunal de commerce de Marrakech sous le numéro 184667, et constituée pour une durée de quatre-vingt-dix-neuf (99) années à compter de son immatriculation au registre du commerce.

La Société a pour objet la fourniture de services de confiance au sens de la loi n° 43-20, en ce compris la certification électronique, la signature électronique et le cachet électronique — simples, avancés ou qualifiés —, l’horodatage électronique ainsi que la délivrance et la gestion des certificats électroniques, sous réserve de l’obtention préalable des agréments et autorisations requis auprès de l’autorité nationale compétente. Son associé unique est YORYX HOLDING, société par actions simplifiée, RC Marrakech n° 184339.

Identification du prestataire

Élément	Valeur
Dénomination sociale	YORYX TRUST SASU
Forme juridique	société par actions simplifiée à associé unique (SASU)
Registre du commerce	RC Marrakech n° 184667, immatriculée le 28 juillet 2026
Identifiant commun de l’entreprise (ICE)	004013324000019

Élément	Valeur
Identifiant fiscal	73266987
Taxe professionnelle	11000|2026|65490
Siège social	57, rue Mauritania, BP 2609, Guéliz, 40000 Marrakech, Maroc
Adresse électronique	trust@yoryx.com
Publication légale	Bulletin officiel n° 5938 du 19 août 2026
Statuts	signés le 18 juillet 2026

1.3. Statut réglementaire

L'article 35 de la loi n° 43-20 impose à toute personne qui se propose de fournir des services de confiance autres que qualifiés de se déclarer au préalable auprès de l'autorité nationale. L'article 32 de la même loi réserve aux seuls prestataires agréés la fourniture des services de confiance qualifiés.

YORYX TRUST prépare sa déclaration et sa demande d'agrément auprès de la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) au titre de la loi n° 43-20 relative aux services de confiance pour les transactions électroniques. À ce jour, YORYX TRUST n'est ni déclaré ni agréé.

> **Portée du présent document —** Le présent document est établi dans la perspective de la déclaration préalable prévue à l'article 35 de la loi n° 43-20. Il ne vaut ni déclaration ni agrément et ne préjuge pas des décisions de l'autorité nationale. Les normes et référentiels qu'il cite sont des cibles de conformité : aucune attestation de tiers n'est revendiquée à ce jour.

1.4. Positionnement et canal de fourniture

YORYX TRUST est le prestataire de services de confiance dont les politiques lient le titulaire du certificat ; la plateforme SELLO est le canal d'enregistrement et de fourniture du service ainsi que la contrepartie commerciale de l'utilisateur final.

L'enrôlement s'effectue par la plateforme SELLO : YORYX TRUST ne contracte pas avec les utilisateurs finaux et n'ouvre aucun compte en son nom propre.

Cette organisation découle des statuts de la Société, aux termes desquels la Société n'a pas vocation à exercer une exploitation commerciale directe auprès d'une clientèle ; elle ne conclut pas de contrats avec les clients finaux des produits et services édités, exploités ou distribués par ses filiales.

Les fonctions d'autorité d'enregistrement exercées par la plateforme sont régies par un contrat écrit préalable qui lie le prestataire au tiers, encadre les obligations, rôles et responsabilités de celui-ci, précise les moyens de contrôle dont dispose le prestataire et fixe les modalités d'établissement des preuves de vérification de l'identité.

1.5. Mention de marque

YORYX® — marque utilisée sous licence. La Société fait usage du signe « YORYX » en vertu d’un contrat de licence de marque consenti par la société MEDINA HOLDING, titulaire des marques correspondantes ; cet usage ne confère à la Société aucun droit de propriété sur lesdites marques.

Référence de la marque : marque YORYX, enregistrement OMPIC n° 298652 du 28 février 2026.

1.6. Identification du document

Le présent document est identifié par l’identifiant d’objet (OID) 1.3.6.1.4.1.[PEN].1.1.3. Il est publié en version 0.1, sous le statut « Projet — en préparation de la déclaration préalable » et la classification « Diffusion publique ».

L’ensemble des identifiants d’objet du prestataire est délivré sous l’arc 1.3.6.1.4.1.[PEN].1, lui-même dérivé de l’arc des numéros d’entreprise privée attribués par l’IANA.

Le jeton [PEN] désigne le numéro d’entreprise privée (Private Enterprise Number) attribué à YORYX TRUST SASU par l’IANA : [À COMPLÉTER — PEN].

Toute évolution modifiant le niveau d’exigence ou le champ d’application du présent document donne lieu à un nouvel identifiant d’objet, dans les conditions énoncées au chapitre relatif à l’administration du document.

1.7. Responsabilités, garanties et limites

La responsabilité du prestataire au titre d’un jeton d’horodatage est plafonnée à [À COMPLÉTER — PLAFOND-RESPONSABILITE] par jeton d’horodatage et par sinistre, tous préjudices confondus. Cette limitation ne s’applique pas en cas de dol ou de faute lourde du prestataire.

Le prestataire souscrit une assurance couvrant sa responsabilité professionnelle auprès de [À COMPLÉTER — ASSUREUR], conformément à l’article 33 de la loi n° 43-20.

La responsabilité du prestataire n’est pas engagée dans les cas suivants :

- l’usage d’un jeton d’horodatage en dehors des limites d’usage fixées par la politique d’horodatage applicable
- le défaut de vérification, par le destinataire d’un jeton, de l’état du certificat de l’unité d’horodatage et de la signature du jeton au moment où il s’y fie
- le fait de se fier à un jeton postérieurement à la notification de la compromission de la clé de l’unité d’horodatage qui l’a produit
- l’inexactitude des données soumises à l’horodatage par le service demandeur
- les faits imputables à un tiers ou constitutifs d’un cas de force majeure

Avant de se fier à un jeton d’horodatage, le destinataire d’un jeton en vérifie la signature, la chaîne de certification de l’unité d’horodatage qui l’a produit, la validité de ce certificat à la date portée par le jeton, son état de révocation à cette même date ainsi que la robustesse des algorithmes employés.

Un jeton d’horodatage atteste que l’empreinte qu’il porte existait à la date indiquée. Il n’emporte aucune constatation quant au contenu des données correspondantes, quant à leur licéité, quant à l’identité de leur auteur ni quant à la validité juridique de l’acte qu’elles constatent.

1.8. Terminologie

Les termes ci-après sont employés dans le sens que leur donne la présente politique. Les acronymes AH, OSH et UH sont ceux du plan type de l’autorité nationale.

Termes et acronymes de l’horodatage

Terme	Définition
Autorité d’horodatage (AH)	Fonction du prestataire qui assume la responsabilité de la délivrance des jetons d’horodatage et de la conformité du service à la présente politique.
Opérateur du service d’horodatage (OSH)	Fonction qui exploite les composantes techniques du service pour le compte de l’autorité d’horodatage et applique la déclaration des pratiques d’horodatage.
Unité d’horodatage (UH)	Ensemble matériel et logiciel qui produit et signe les jetons d’horodatage, caractérisé par une bi-clé de signature et un certificat qui lui sont propres.
Service demandeur	Entité qui soumet une demande d’horodatage et reçoit le jeton correspondant. Dans le modèle du prestataire, la plateforme et les systèmes qu’elle dessert sont des services demandeurs.
Utilisateur final	Personne physique ou morale qui se fie à un jeton d’horodatage, sans être nécessairement le service demandeur qui l’a obtenu.
Destinataire d’un jeton	L’utilisateur final auquel un jeton d’horodatage est présenté et qui s’y fie. C’est en cette qualité que les vérifications énoncées par le présent document lui incombent ; le terme est employé dans les clauses opposables, où l’obligation de vérification pèse sur celui qui se fie au jeton.
Jeton d’horodatage	Donnée signée par une unité d’horodatage qui lie une empreinte cryptographique à une date et à une heure, et atteste ainsi de l’existence de la donnée correspondante à cet instant.
Empreinte cryptographique	Résultat de l’application d’une fonction de hachage aux données à horodater, calculé par le service demandeur et seul élément transmis au service.
Temps universel coordonné (UTC)	Échelle de temps de référence à laquelle le temps porté par les jetons d’horodatage est traçable.
Exactitude	Écart maximal déclaré entre le temps porté par un jeton d’horodatage et le temps universel coordonné.

1.9. Documents liés

La présente politique s’articule avec les autres documents du registre de publication du prestataire :

Documents du registre auxquels la présente politique renvoie

Document	Identifiant d’objet	Objet du renvoi
YT-DPC	1.3.6.1.4.1.[PEN].1.2	Déclaration des pratiques : mise en œuvre opérationnelle des règles énoncées ici, y compris la déclaration des pratiques d’horodatage.
YT-PDS-TSA	1.3.6.1.4.1.[PEN].1.3.2	Résumé publiable de la présente politique, destiné aux utilisateurs finaux.
YT-CGU-TSA	1.3.6.1.4.1.[PEN].1.4.3	Conditions générales d’utilisation du service d’horodatage, opposables au service demandeur.
YT-PC-SIGN	1.3.6.1.4.1.[PEN].1.1.1	Politique de certification des certificats de signature électronique.
YT-PC-SEAL	1.3.6.1.4.1.[PEN].1.1.2	Politique de certification des certificats de cachet électronique.
YT-PRICING	1.3.6.1.4.1.[PEN].1.7.1	Termes tarifaires du service (unités de facturation, prestations sans frais, remboursement) ; aucun montant n’est publié.
YT-COMPLAINTS	1.3.6.1.4.1.[PEN].1.7.2	Procédure de réclamation et voies de recours.

2. Acteurs de l’horodatage

2.1. Services d’horodatage

Le service d’horodatage est constitué des fonctions suivantes, exercées sous la responsabilité unique de l’autorité d’horodatage :

- la fonction de production, qui reçoit les demandes d’horodatage, construit les jetons et les signe au moyen d’une unité d’horodatage ;
- la fonction de temps, qui maintient la traçabilité du temps du service au temps universel coordonné et en contrôle l’exactitude ;
- la fonction de gestion des unités d’horodatage, qui couvre la génération, la protection, le renouvellement et la fin de vie de leurs bi-clés et de leurs certificats ;
- la fonction de publication, qui met à disposition la présente politique, la déclaration des pratiques, les certificats des autorités de certification et les informations d’état correspondantes ;
- la fonction de journalisation et d’archivage, qui enregistre les évènements et conserve les preuves ;
- la fonction d’information, qui répond aux demandes des services demandeurs et des utilisateurs finaux.

Le service met en œuvre une unité d’horodatage en service, une unité en secours sur le site secondaire. Chaque unité d’horodatage possède une bi-clé de signature et un certificat qui lui sont propres ; une bi-clé d’unité d’horodatage n’est jamais partagée entre deux unités.

2.2. Autorité d’horodatage

L’autorité d’horodatage est YORYX TRUST SASU. Elle approuve la présente politique, approuve la déclaration des pratiques d’horodatage, répond de la conformité du service à l’une et à l’autre, et demeure responsable de l’ensemble des fonctions énumérées ci-dessus, y compris de celles qu’elle confie à un tiers.

L’exploitation des composantes techniques est assurée par l’opérateur du service d’horodatage, fonction interne au prestataire. La séparation entre l’autorité, qui décide, et l’opérateur, qui exécute, est une séparation de rôles et non de personnes morales : la responsabilité juridique reste indivisible.

Les certificats des unités d’horodatage sont délivrés par l’autorité de certification émettrice des certificats des unités d’horodatage, dénommée « YORYX TRUST Timestamping CA G1 », elle-même certifiée par l’autorité de certification racine, maintenue hors ligne, dénommée « YORYX TRUST Root CA G1 ». Cette autorité émettrice ne délivre aucun certificat à un usage étranger au service d’horodatage du prestataire.

2.3. Service demandeur

Le service demandeur est l’entité qui soumet une demande d’horodatage et reçoit le jeton correspondant. Il calcule lui-même l’empreinte cryptographique des données à horodater et ne transmet que cette empreinte : les données elles-mêmes ne quittent jamais son environnement.

Conformément au positionnement énoncé au chapitre premier, la plateforme et les systèmes qu’elle dessert constituent les services demandeurs du prestataire. La relation entre le service

demandeur et le prestataire est régie par YT-CGU-TSA (OID 1.3.6.1.4.1.[PEN].1.4.3) et, le cas échéant, par la convention de service conclue avec la plateforme.

2.4. Commission d’approbation

La commission d’approbation est la formation interne qui approuve la présente politique, la déclaration des pratiques d’horodatage et leurs révisions successives, avant toute publication et avant toute prise d’effet.

Elle est composée par fonction, et non par personne : la présidence de la Société, le responsable de sécurité, le responsable d’application concerné et le contrôleur. Elle se réunit au moins 1 fois par an, ainsi que chaque fois qu’une modification substantielle est envisagée ou qu’un écart de conformité le justifie. Ses décisions font l’objet d’un procès-verbal conservé au dossier d’audit.

La commission d’approbation apprécie l’incidence de toute modification sur le niveau d’exigence et sur le champ d’application du service, et décide en conséquence de l’attribution d’un nouvel identifiant d’objet.

3. Politique d’horodatage

3.1. Définition

Une politique d’horodatage est l’ensemble des règles qui déterminent l’applicabilité d’un jeton d’horodatage à une communauté d’usage et à une classe d’applications ayant des exigences communes de sécurité. Elle énonce les engagements de l’autorité d’horodatage, les obligations des services demandeurs et des utilisateurs finaux, et les propriétés vérifiables du service.

La présente politique ne décrit pas les procédures d’exploitation. Celles-ci figurent dans la déclaration des pratiques, YT-DPC (OID 1.3.6.1.4.1.[PEN].1.2), qui en est le pendant opérationnel et qui lui est subordonnée : en cas de divergence, la présente politique prévaut.

3.2. Identification

Identifiants d’objet du service d’horodatage

Objet identifié	Identifiant d’objet
Arc des services de confiance du prestataire	1.3.6.1.4.1.[PEN].1
Politique d’horodatage (le présent document)	1.3.6.1.4.1.[PEN].1.1.3
Service d’horodatage électronique simple	1.3.6.1.4.1.[PEN].1.1.3.1
Déclaration des pratiques	1.3.6.1.4.1.[PEN].1.2
Déclaration de divulgation PKI — horodatage	1.3.6.1.4.1.[PEN].1.3.2
Conditions générales d’utilisation — horodatage	1.3.6.1.4.1.[PEN].1.4.3

L’identifiant 1.3.6.1.4.1.[PEN].1.1.3.1 est porté par le champ de politique de chaque jeton d’horodatage délivré au titre de la présente politique. Un service demandeur peut donc, à la seule lecture d’un jeton, déterminer la politique applicable et en retrouver le texte dans le registre de publication.

C’est également cet identifiant qui est communiqué à l’autorité nationale au titre de la déclaration préalable, avec le type de service, son nom commercial, sa description sommaire et l’adresse de la présente politique.

3.3. Conformité

Le service d’horodatage vise la conformité aux textes suivants, cités comme cibles :

- ETSI EN 319 421, exigences de politique et de sécurité applicables aux prestataires délivrant des jetons d’horodatage, dont le référentiel des services de confiance non qualifiés fait la norme du service d’horodatage électronique ;
- ETSI EN 319 401, exigences générales de politique applicables aux prestataires de services de confiance ;

- ETSI EN 319 422, profil du protocole et des jetons d’horodatage ;
- ETSI TS 119 312, suites cryptographiques ;
- le plan type détaillé d’une politique d’horodatage de la politique de certification de référence de l’autorité nationale, qui fixe la structure du présent document.

Le référentiel d’exigences relatif au service d’horodatage électronique qualifié constitue la cible du service qualifié : il ne s’applique pas au service déclaré, qui n’est pas un service qualifié, mais les exigences de conservation, de journalisation et d’identification du service qu’il énonce sont d’ores et déjà prises pour référence.

Le respect de la présente politique fait l’objet d’un contrôle interne 1 fois par an, portant sur le contrôle de conformité de l’ensemble de l’infrastructure de gestion de clés à la politique de certification, à la déclaration des pratiques et à la politique de sécurité, et d’un audit externe tous les 2 ans : audit indépendant de conformité aux normes cibles, conduit par un auditeur externe n’ayant pris part ni à la conception ni à l’exploitation des composantes auditées.

Chaque écart constaté donne lieu à un plan d’action daté, à un responsable désigné par sa fonction et à une vérification de clôture ; un écart critique suspend l’émission jusqu’à sa correction.

Préalablement à toute demande d’agrément, le demandeur est soumis, à ses frais, à une évaluation sur pièces et sur place par un organisme désigné à cet effet par l’autorité nationale.

Les résultats des évaluations sont communiqués à l’autorité nationale sur sa demande. Ils ne sont pas publiés, la description détaillée des mesures de sécurité ne pouvant être rendue publique sans affaiblir celles-ci.

3.4. Certificats d’horodatage

Le certificat d’une unité d’horodatage identifie l’unité, porte sa clé publique de vérification et restreint son usage à l’horodatage. Il est délivré par l’autorité émettrice dédiée au service et n’est jamais délivré avant que la bi-clé correspondante n’ait été générée dans le module cryptographique matériel.

Caractéristiques des certificats du service d’horodatage

Élément	Valeur
Autorité racine	YORYX TRUST Root CA G1 — autorité de certification racine, maintenue hors ligne
Autorité émettrice	YORYX TRUST Timestamping CA G1 — autorité de certification émettrice des certificats des unités d’horodatage
Unité d’horodatage	YORYX TRUST TSU 1 G1 — unité d’horodatage (TSU) signant les jetons d’horodatage
Durée de validité du certificat d’unité d’horodatage	5 ans
Durée de validité du certificat d’autorité émettrice	6 ans

Élément	Valeur
Durée de validité du certificat racine	10 ans
Algorithme et taille de clé de l’unité d’horodatage	RSA 3072 bits
Algorithme de signature des jetons	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
Règle de génération	Le suffixe « G<n> » désigne la génération de la bi-clé ; il est incrémenté à chaque renouvellement de clé et n’est jamais réutilisé.

La période de validité d’un certificat d’autorité émettrice est strictement supérieure à celle des certificats qu’elle délivre ; aucun certificat n’est délivré dont la fin de validité dépasserait celle du certificat de l’autorité émettrice.

L’état des certificats d’unité d’horodatage est publié par les mêmes fonctions que celles des autres autorités émettrices du prestataire : listes de révocation publiées toutes les 24 heures et service d’information sur l’état des certificats conforme au protocole IETF RFC 6960, l’un et l’autre accessible publiquement, sans contrôle d’accès ni frais.

La révocation du certificat d’une unité d’horodatage met fin immédiatement à la délivrance de jetons par cette unité. Elle n’invalide pas rétroactivement les jetons délivrés avant la date de révocation, dont la vérification s’apprécie à la date qu’ils portent.

4. Obligations

4.1. Obligation de l’autorité d’horodatage

L’autorité d’horodatage s’engage à :

- délivrer des jetons d’horodatage conformes à la présente politique et au profil de jeton défini en annexe ;
- porter dans chaque jeton un temps traçable au temps universel coordonné, avec l’exactitude déclarée de 1 seconde ou mieux ;
- cesser immédiatement de délivrer des jetons lorsque l’exactitude déclarée ne peut plus être garantie ;
- générer, protéger, renouveler et détruire les bi-clés des unités d’horodatage dans les conditions énoncées au chapitre relatif aux pratiques ;
- publier la présente politique, la déclaration des pratiques et le résumé publiable dans le registre de publication, sans contrôle d’accès ni frais ;
- journaliser les évènements énumérés au présent document et conserver les preuves correspondantes pendant la durée annoncée ;
- informer les services demandeurs de toute compromission avérée ou suspectée d’une clé d’unité d’horodatage et de toute perte de synchronisation ayant affecté le service ;
- notifier à l’autorité nationale toute atteinte à la sécurité ou toute perte d’intégrité ayant une incidence sur le service ;
- maintenir une organisation, des rôles de confiance et des contrôles conformes au chapitre relatif à la gestion et à l’exploitation.

L’autorité d’horodatage ne prend aucun engagement quant à l’usage que le service demandeur ou l’utilisateur final fait d’un jeton, ni quant aux conséquences d’un usage contraire aux limites énoncées ici.

4.2. Obligation de l’opérateur du service d’horodatage

L’opérateur du service d’horodatage s’engage à :

- appliquer la déclaration des pratiques d’horodatage approuvée, sans y déroger ;
- exploiter les composantes du service dans les zones et selon les contrôles d’accès définis, en respectant la séparation des rôles de confiance ;
- contrôler la synchronisation des unités d’horodatage et journaliser chaque contrôle, chaque recalibrage et chaque détection de perte de synchronisation ;
- n’opérer sur une clé d’unité d’horodatage que sous double contrôle et selon le quorum défini
- signaler sans délai à l’autorité d’horodatage tout incident, toute anomalie et toute tentative de compromission ;
- conserver les journaux et les procès-verbaux au dossier d’audit et les tenir à la disposition du contrôleur.

4.3. Obligations et responsabilités des services demandeurs

Le service demandeur accepte la présente politique et les conditions générales d’utilisation avant toute demande. Il s’engage à n’utiliser le service que dans les limites qu’elles fixent, à calculer les empreintes au moyen d’une fonction de hachage au moins équivalente à SHA-256, et à ne transmettre aucune donnée autre que l’empreinte.

4.3.1. Vérification de la validité des jetons dès réception

Le service demandeur vérifie la validité du jeton dès sa réception et l’archive avec les données horodatées.

La vérification porte au minimum sur les points suivants :

1. la correspondance entre l’empreinte portée par le jeton et celle des données horodatées ;
2. la validité de la signature du jeton et la référence au certificat de l’unité d’horodatage qui y est incluse ;
3. la chaîne de certification, jusqu’au certificat racine du prestataire ;
4. la validité du certificat de l’unité d’horodatage à la date portée par le jeton, et son état de révocation à cette même date ;
5. la présence de l’identifiant de politique attendu ;
6. la concordance du nombre aléatoire, lorsque la demande en comportait un.

Un jeton dont l’une de ces vérifications échoue est refusé par le service demandeur, qui en informe le prestataire. La délivrance d’un jeton de remplacement ne donne lieu à aucun frais.

4.3.2. Archivage des jetons d’horodatage

Le service demandeur archive chaque jeton avec les données auxquelles il se rapporte et avec les éléments nécessaires à sa vérification ultérieure : la chaîne de certification et l’information d’état du certificat de l’unité d’horodatage à la date du jeton.

Lorsque la conservation excède la période de fiabilité des algorithmes employés, il appartient au service demandeur de renouveler la preuve, notamment par un nouvel horodatage portant sur l’ensemble constitué des données et du jeton initial.

Le prestataire conserve de son côté les éléments énumérés au chapitre 5 pendant 7 ans ; cette conservation ne dispense pas le service demandeur de la sienne, dont la finalité et la maîtrise lui sont propres.

4.4. Obligations des utilisateurs finaux

L’utilisateur final qui se fie à un jeton d’horodatage procède aux vérifications énumérées ci-dessus, dans la mesure des éléments dont il dispose. Il tient compte des limites d’usage énoncées par la présente politique et de la portée exacte de l’attestation : la date d’existence d’une empreinte, et rien d’autre.

La vérification d’un jeton est publique et gratuite : elle ne suppose ni compte, ni abonnement, ni logiciel fourni par le prestataire. Les certificats des autorités de certification nécessaires à cette vérification sont publiés dans le registre de publication.

L’utilisateur final ne peut se prévaloir d’un jeton au-delà de la limite de responsabilité énoncée au chapitre premier, ni dans un cas relevant des exclusions qui y sont énumérées.

5. Exigences concernant les pratiques d’horodatage

5.1. Déclaration des pratiques d’horodatage et résumé publiable

5.1.1. Déclaration des pratiques d’horodatage de l’opérateur

L’opérateur du service d’horodatage établit une déclaration des pratiques d’horodatage qui décrit la mise en œuvre effective de la présente politique. Cette déclaration est intégrée à YT-DPC (OID 1.3.6.1.4.1.[PEN].1.2), dont elle constitue la partie relative au service d’horodatage.

Elle énonce au minimum :

- les fonctions de hachage admises pour l’empreinte transmise et les algorithmes de signature employés ;
- l’exactitude du temps porté par les jetons par rapport au temps universel coordonné ;
- les limites d’usage du service et les cas dans lesquels un jeton ne doit pas être utilisé ;
- les obligations du service demandeur et celles de l’utilisateur final ;
- la procédure de vérification d’un jeton et les éléments nécessaires à cette vérification ;
- les engagements de disponibilité et les modalités de reprise après incident ;
- les dispositions prises pour satisfaire aux obligations légales applicables au Maroc.

La déclaration des pratiques est approuvée par la commission d’approbation avant sa prise d’effet. Sa version en vigueur est publiée ; les parties dont la divulgation affaiblirait la sécurité du service ne sont pas publiées et sont communiquées à l’autorité nationale sur sa demande.

5.1.2. Résumé publiable des politiques

Le résumé publiable de la présente politique est YT-PDS-TSA (OID 1.3.6.1.4.1.[PEN].1.3.2). Il présente, sous une forme brève et destinée à un lecteur non spécialiste, le service, les types de jetons, les limites de confiance, les obligations réciproques, la responsabilité, la protection des données à caractère personnel, le droit applicable et les voies de recours.

Le résumé publiable ne crée aucune obligation nouvelle et n’en supprime aucune : en cas de divergence entre le résumé et la présente politique, celle-ci prévaut.

5.2. Cycle de vie des clés de l’autorité d’horodatage

5.2.1. Génération des clés

Toute génération de bi-clé d’autorité se déroule en cérémonie, selon un script écrit et approuvé avant exécution, en présence de témoins, avec séparation des rôles de porteur de part de secret, d’opérateur, de témoin et de contrôleur, et donne lieu à un procès-verbal signé conservé au dossier d’audit.

La bi-clé d’une unité d’horodatage est de type RSA 3072 bits. Elle est générée à l’intérieur du module cryptographique matériel, dans un environnement physiquement protégé, par des personnes tenant un rôle de confiance et sous double contrôle. L’activation de la clé privée d’une autorité de certification exige la réunion d’un quorum de 3 porteurs de parts de secret parmi 5, sous double contrôle ; aucune personne seule ne peut activer une clé d’autorité.

Les suites cryptographiques mises en œuvre sont conformes à la norme ETSI TS 119 312 (version 1.4.2 ou ultérieure).

MD5, SHA-1 et toute longueur de clé RSA inférieure à 2048 bits sont proscrits.

Une unité d’horodatage ne dispose que d’une seule bi-clé active à un instant donné, et une bi-clé générée pour la signature des jetons n’est employée à aucun autre usage.

5.2.2. Protection des clés privées

Les clés privées des unités d’horodatage sont détenues et utilisées exclusivement à l’intérieur du module cryptographique matériel, qui présente les propriétés suivantes :

- les bi-clés d’autorité et les clés privées des unités d’horodatage sont générées à l’intérieur du module et n’en sortent jamais en clair
- les clés sont non exportables et non extractibles ; aucune copie en clair n’existe hors du module
- toute opération sensible exige un double contrôle et le quorum défini ci-dessus
- le module détecte et signale les tentatives d’intrusion physique
- les sauvegardes de clés sont chiffrées et leur restauration est soumise au même quorum
- les journaux du module sont horodatés et protégés contre la modification

Les textes suivants constituent les cibles retenues pour ce module :

- CEN EN 419 221-5 — profil de protection des modules cryptographiques pour prestataires de services de confiance
- Critères Communs, niveau d’évaluation EAL4+
- CEN EN 419 241-1 et CEN EN 419 241-2 — systèmes de confiance pour la signature côté serveur

Ces textes sont des cibles : aucune conformité n’est constatée à ce jour et aucune attestation de tiers n’est revendiquée. Le matériel n’est jamais désigné par sa marque, son modèle ou son numéro de série.

Chaque part de secret est conservée dans un contenant scellé, dans un coffre distinct, sous la responsabilité nominative d’un porteur de part ; un registre daté atteste de chaque remise et de chaque restitution.

Les sauvegardes sont chiffrées, conservées hors site, et leur restauration est soumise au même quorum que les opérations sur les clés.

5.2.3. Renouvellement des clés

Le certificat d’une unité d’horodatage a une durée de validité de 5 ans. Une nouvelle bi-clé est générée et certifiée suffisamment tôt pour que le service ne connaisse aucune interruption au terme de la bi-clé précédente.

La bi-clé d’une autorité émettrice cesse d’être utilisée pour signer de nouveaux certificats au plus tard trois (3) ans avant l’expiration de son propre certificat, afin que tout certificat délivré expire avant celui de l’autorité.

Le suffixe « G<n> » désigne la génération de la bi-clé ; il est incrémenté à chaque renouvellement de clé et n’est jamais réutilisé.

La cérémonie est reproduite à chaque renouvellement de la clé racine ou de la clé d’une autorité émettrice.

La période d’emploi de la clé privée d’une unité d’horodatage est strictement inférieure à la période de validité du certificat correspondant, afin que tout jeton délivré puisse être vérifié pendant toute la durée restante du certificat.

5.2.4. Fin du cycle de vie des clés cryptographiques

Au terme de sa période d’emploi, la clé privée d’une unité d’horodatage cesse d’être utilisée. Le service refuse toute demande d’horodatage dès que cette échéance est atteinte, y compris lorsque le certificat correspondant est encore en cours de validité.

La clé privée est ensuite détruite, ainsi que ses sauvegardes et toutes les parts de secret associées. La destruction est réalisée sous double contrôle, en présence de témoins, et donne lieu à un procès-verbal conservé au dossier d’audit. Aucune clé détruite n’est régénérée ni réutilisée.

Le certificat d’une unité d’horodatage dont la clé a été détruite avant son terme est révoqué, et la révocation est publiée dans les conditions de droit commun du prestataire.

5.2.5. Gestion du cycle de vie des unités d’horodatage

Le matériel qui met en œuvre une unité d’horodatage est suivi de sa réception à son retrait. Il est protégé contre toute manipulation pendant son acheminement et pendant son entreposage ; son installation, son activation et toute duplication de son contenu sont réalisées par des personnes tenant un rôle de confiance, sous double contrôle, dans un environnement physiquement protégé.

Au retrait d’un matériel, les clés privées qu’il contient sont effacées de manière irréversible avant toute sortie de la zone sensible.

Sont journalisés, pour chaque unité d’horodatage :

- tous les évènements du cycle de vie de sa bi-clé : génération, sauvegarde, restauration, mise en service, retrait, destruction ;
- tous les évènements du cycle de vie de son certificat : demande, délivrance, publication, révocation, expiration ;
- tous les évènements de synchronisation de son horloge, y compris les recalibrages ;
- toutes les détections de perte de synchronisation et les arrêts de service qui en résultent.

5.3. Production des jetons d’horodatage

5.3.1. Jeton d’horodatage

Les jetons sont conformes au profil ETSI EN 319 422, protocole IETF RFC 3161. La demande d’horodatage ne comporte que l’empreinte cryptographique des données, l’identifiant de la politique demandée et, facultativement, un nombre aléatoire destiné à lier la réponse à la demande.

Le jeton délivré porte notamment le numéro de série qui l’identifie de manière unique au sein de l’unité d’horodatage, l’empreinte reçue et l’algorithme de hachage employé, la date et l’heure de génération, l’exactitude déclarée et l’identifiant de politique. Le profil détaillé figure en annexe.

Chaque jeton inclut la référence du certificat de l’unité d’horodatage qui l’a signé, de sorte que le vérificateur identifie sans ambiguïté la clé publique à employer.

Le service ne garantit pas l’ordonnancement de deux jetons dont les dates ne peuvent être distinguées au regard de l’exactitude déclarée. Un service demandeur qui a besoin d’un ordre strict entre deux évènements le construit lui-même, en horodatant le second sur un ensemble incluant le premier jeton.

5.3.2. Synchronisation avec le temps universel coordonné

Le temps porté par les jetons est issu d’une source de temps de confiance traçable à l’UTC, distincte des autorités de certification et redondée.

L’exactitude déclarée du temps contenu dans un jeton d’horodatage est de 1 seconde ou mieux par rapport au temps universel coordonné (UTC).

La synchronisation de l’unité d’horodatage avec le temps universel coordonné est vérifiée au moins toutes les 24 heures, et chaque vérification est journalisée.

Lorsque la perte de synchronisation avec l’UTC est détectée, ou lorsque l’exactitude déclarée ne peut plus être garantie, l’unité d’horodatage cesse immédiatement de délivrer des jetons.

L’ajustement dû à une seconde intercalaire intervient durant la dernière minute du jour où elle est programmée, et l’heure exacte du changement est enregistrée.

La source de temps est protégée contre toute altération et contre toute dérive non détectée. Elle est indépendante des autorités de certification du prestataire, de sorte qu’une atteinte à l’une n’emporte pas l’atteinte de l’autre.

> **Règle prépondérante —** L’arrêt de la délivrance en cas de perte de synchronisation prime sur tout engagement de disponibilité : il vaut mieux ne pas délivrer de jeton que d’en délivrer un dont la date ne peut être garantie.

5.3.3. Disponibilité du service

Le service d’horodatage repose sur une unité en service et une unité en secours installée sur le site secondaire, de sorte que la défaillance d’une composante n’interrompe pas durablement la production de jetons.

Engagements de disponibilité des fonctions publiques du prestataire

Fonction	Plage	Interruption maximale	Cumul mensuel maximal
Publication du registre et des certificats d’autorité	24 heures sur 24, 7 jours sur 7	1 heure	4 heures
Information sur l’état des certificats	24 heures sur 24, 7 jours sur 7	1 heure	4 heures
Traitement des demandes de révocation	24 heures sur 24, 7 jours sur 7	30 minutes	2 heures
Information et assistance	jours ouvrés	8 heures (jours ouvrés)	32 heures (jours ouvrés)
Production des jetons d’horodatage	24 heures sur 24, 7 jours sur 7	1 heure	4 heures

Le service de production des jetons d’horodatage est disponible 24 heures sur 24, 7 jours sur 7. La durée maximale d’indisponibilité par interruption, panne ou maintenance, est d’une (1) heure, et la durée maximale totale d’indisponibilité est de quatre (4) heures par mois. L’arrêt de la

délivrance de jetons consécutif à la détection d’une perte de synchronisation avec le temps universel coordonné n’est pas décompté de ces durées : il constitue le comportement exigé de l’unité d’horodatage, qui cesse d’émettre tant que l’exactitude déclarée n’est pas rétablie.

Les capacités du service sont suivies et les besoins futurs anticipés, afin que la montée en charge d’un service demandeur ne dégrade ni l’exactitude ni la disponibilité.

5.4. Validité d’un jeton d’horodatage

5.4.1. Durée de validité d’un jeton d’horodatage

Le jeton d’horodatage n’a pas de durée de validité propre : sa vérification dépend de la validité, à la date du jeton, du certificat de l’unité d’horodatage qui l’a signé et de la robustesse des algorithmes employés.

Il en résulte qu’un jeton demeure vérifiable au-delà de la période de validité du certificat de l’unité d’horodatage, à la condition que le vérificateur dispose de l’information d’état de ce certificat telle qu’elle existait à la date du jeton, et que les algorithmes employés soient encore réputés robustes à la date de la vérification.

Le prestataire ne fixe donc aucune durée de validité propre au jeton et n’en prononce aucune caducité.

5.4.2. Vérification d’un jeton par le service demandeur

La procédure de vérification est celle énoncée au chapitre relatif aux obligations des services demandeurs. Elle est conduite dès la réception du jeton, puis, autant que nécessaire, à chaque usage ultérieur. Le guide YT-GUIDE-USE (OID 1.3.6.1.4.1.[PEN].1.6.3) en décrit la mise en œuvre pratique.

Le prestataire met à disposition, sans frais, les certificats d’autorité et l’information d’état nécessaires à cette vérification, ainsi que le profil de jeton figurant en annexe.

5.5. Gestion et exploitation de l’autorité d’horodatage

5.5.1. Gestion de la sécurité

Le prestataire maintient un système de management de la sécurité de l’information couvrant l’ensemble des composantes du service d’horodatage. Une analyse de risque documentée en fixe le périmètre et les mesures ; elle est revue à chaque évolution substantielle du service et, à défaut, au moins une fois par an.

La direction de la Société approuve la politique de sécurité, alloue les moyens correspondants et désigne, par leur fonction, les responsables de sa mise en œuvre.

5.5.2. Classification des biens

Les biens du service — clés privées, parts de secret, matériels cryptographiques, journaux, archives, configurations, documentation d’exploitation — font l’objet d’un inventaire tenu à jour et d’une classification par niveau de sensibilité, dont découlent les règles de conservation, de transport, de communication et de destruction qui leur sont appliquées.

La description détaillée des mesures de sécurité n’est pas publiée : sa divulgation affaiblirait les mesures elles-mêmes.

5.5.3. Sécurité du personnel

Les rôles de confiance du service sont définis par fonction. Aucun document du registre de publication ne nomme la personne physique qui les exerce.

Rôles de confiance

Rôle	Attributions
Responsable de sécurité	met en œuvre la politique de sécurité de la composante, gère les contrôles d’accès physiques aux équipements, est habilité à prendre connaissance des archives et analyse les journaux d’évènements afin de détecter tout incident, anomalie ou tentative de compromission.
Responsable d’application	met en œuvre la politique de certification et la déclaration des pratiques au niveau de l’application dont il répond, et répond des fonctions rendues par celle-ci et des performances correspondantes.
Ingénieur système	assure la mise en route, la configuration et la maintenance technique des équipements, ainsi que l’administration technique des systèmes et des réseaux de la composante.
Opérateur	réalise, dans le cadre de ses attributions, l’exploitation des applications pour les fonctions mises en œuvre par la composante.
Contrôleur	procède de manière régulière aux contrôles de conformité de la mise en œuvre des fonctions par rapport à la politique de certification, à la déclaration des pratiques et à la politique de sécurité.
Porteur de part de secret	assure la confidentialité, l’intégrité et la disponibilité de la part de secret qui lui est confiée, et participe au quorum d’activation des clés d’autorité.

Une même personne ne cumule pas le rôle de contrôleur avec l’un des rôles d’opérateur, d’ingénieur système ou de responsable d’application, ni le rôle de responsable de sécurité avec celui d’ingénieur système. Un porteur de part de secret ne détient qu’une seule part. Chaque attribution de rôle est notifiée par écrit.

Chaque personne appelée à tenir un rôle de confiance fait l’objet, avant son affectation, d’une vérification d’identité, d’une vérification de ses antécédents professionnels dans les limites permises par la loi, d’un engagement de confidentialité écrit et d’une formation initiale, complétée par une formation continue au moins annuelle.

5.5.4. Sécurité physique

L’exploitation repose sur deux sites distincts, un site principal et un site secondaire, dont la localisation, la configuration et l’identité des équipements ne sont pas publiées.

L’accès aux composantes du service est contrôlé, nominatif et enregistré. Toute entrée et toute sortie de zone sensible sont journalisées, et une personne non habilitée y est accompagnée en permanence. Les mesures couvrent notamment le risque d’intrusion, d’incendie, de dégât des eaux, de défaillance des énergies et de vol de matériel.

Aucun matériel du service ne quitte le site sans autorisation formelle ; le matériel cryptographique fait l’objet d’un contrôle d’accès supplémentaire, distinct de celui de la salle qui l’héberge.

5.5.5. Sécurité d’exploitation

Les environnements de production, de recette et de développement sont séparés physiquement et logiquement ; aucune clé de production n’est transférée vers un environnement non productif.

Toute modification d’une composante du service suit une procédure de gestion des changements écrite : qualification préalable, approbation par la fonction habilitée, exécution tracée et possibilité de retour à l’état antérieur. Les comptes, applications, services et protocoles inutilisés sont supprimés ou désactivés.

Les composantes du service sont maintenues dans une zone réseau protégée, dont l’accès est réservé aux rôles de confiance.

5.5.6. Zonage des locaux

Chaque site est organisé en zones d’accès graduées — zone d’accueil, zone technique, zone sensible — avec contrôle d’accès nominatif et enregistré, registre des visites, détection d’intrusion et d’incendie, alimentation électrique et climatisation redondées.

Les unités d’horodatage et les modules cryptographiques matériels sont installés dans la zone sensible. Les activités qui ne concourent pas au service ne sont admises dans une zone que si elles n’en abaissent pas le niveau de contrôle.

5.5.7. Gestion des accès aux composantes du système d’horodatage

Chaque accès logique est nominatif, attribué en fonction du rôle tenu et selon le principe du moindre privilège. Les droits sont revus périodiquement et retirés dès la fin de l’affectation. Les accès d’administration s’effectuent depuis des postes dédiés et font l’objet d’une authentification renforcée.

Toute opération sensible sur une unité d’horodatage exige la présence simultanée de deux rôles distincts. Les tentatives d’accès infructueuses sont examinées toutes les 24 heures.

5.5.8. Maintenance et déploiement

Les opérations de maintenance sont planifiées, annoncées aux services demandeurs lorsqu’elles ont une incidence sur la disponibilité, et exécutées sous la surveillance d’un rôle de confiance. Une intervention à distance n’est admise que par un canal authentifié et chiffré, et elle est intégralement journalisée.

Le déploiement d’une nouvelle version d’une composante est précédé d’une qualification dans un environnement séparé de la production ; aucune clé de production n’y est transférée.

5.5.9. Mesures à prendre en cas de compromission

En cas de compromission avérée ou suspectée de la clé privée d’une unité d’horodatage, ou en cas de perte de la calibration de son horloge, le service cesse immédiatement de délivrer des jetons au moyen de cette unité et le certificat correspondant est révoqué.

Le prestataire met à la disposition des services demandeurs et des utilisateurs finaux une description de l’évènement et, lorsque l’atteinte est majeure, les éléments permettant d’identifier les jetons susceptibles d’être affectés, dans la mesure où cette communication ne porte atteinte ni à la sécurité du service ni à la vie privée des personnes.

Toute atteinte à la sécurité ou toute perte d’intégrité ayant une incidence sur le service de confiance fourni ou sur les données à caractère personnel conservées est notifiée à l’autorité nationale

immédiatement après en avoir eu connaissance, selon les modalités du référentiel de gestion des incidents de cybersécurité.

Une procédure de reprise qui n’a jamais été exécutée n’est pas une garantie : chaque test de restauration donne lieu à un procès-verbal conservé au dossier d’audit.

Le plan de continuité est testé 1 fois par an et les restaurations sont éprouvées 1 fois par an, au minimum. La reprise n’autorise la reprise de la délivrance qu’après vérification complète de l’intégrité des composantes et de la synchronisation.

5.5.10. Fin du cycle de vie de l’autorité d’horodatage

Le prestataire informe préalablement l’autorité nationale, dans un délai minimum de deux (2) mois, avant de mettre fin à ses activités.

En cas de cessation du service d’horodatage, le prestataire :

1. informe l’autorité nationale dans le délai énoncé ci-dessus, ainsi que les services demandeurs ;
2. cesse de délivrer des jetons à la date annoncée ;
3. révoque les certificats des unités d’horodatage non expirés ;
4. détruit les clés privées correspondantes, leurs sauvegardes et les parts de secret associées
5. n’attribue aucune nouvelle bi-clé à une unité retirée et ne délivre plus aucun jeton sous son identité ;
6. assure la conservation des archives pendant la durée annoncée, le cas échéant par la remise à un repreneur ou à l’entité désignée à cet effet ;
7. maintient l’accès aux informations d’état nécessaires à la vérification des jetons déjà délivrés.

La cessation du service ne prive pas les jetons déjà délivrés de leur valeur : elle organise au contraire les conditions de leur vérification ultérieure.

5.5.11. Données enregistrées par l’autorité d’horodatage

Sont enregistrés et conservés :

- les engagements souscrits par les services demandeurs et les conditions générales acceptées ;
- la présente politique, la déclaration des pratiques et leurs versions successives ;
- les certificats employés par le service et les informations d’état correspondantes ;
- les versions des composants logiciels et les configurations des équipements du service ;
- les journaux d’évènements et les pistes d’audit de toutes les composantes ;
- les évènements du cycle de vie des bi-clés et des certificats des unités d’horodatage ;
- les évènements de synchronisation, de recalibrage et de détection de perte de synchronisation ;
- les procès-verbaux de cérémonie, de test de restauration et de destruction de clés.

Les données relatives à la fourniture des services de confiance sont conservées pendant une durée minimale de sept (7) ans à compter de l’expiration du certificat ou du jeton d’horodatage auquel elles se rapportent, y compris après une cessation d’activité.

Journalisation, conservation et restitution

Élément	Valeur
Durée de conservation des données du service	7 ans
Conservation des journaux sur le site de production	1 mois
Analyse des journaux	1 fois par jour ouvré, et dès la détection d’une anomalie
Examen des tentatives d’accès infructueuses	toutes les 24 heures
Rapprochement des journaux entre composantes	1 fois par semaine
Délai de restitution d’une archive	2 jours ouvrés

Chaque dossier de preuve est scellé par un cachet électronique du prestataire afin d’en renforcer la fiabilité et l’intégrité.

À l’issue de la période de conservation, les données archivées sont supprimées ou détruites de manière irréversible, et l’opération est journalisée.

Les journaux sont horodatés, protégés en intégrité et accessibles aux seules fonctions habilitées. Ils ne contiennent aucune donnée horodatée, le service n’en recevant aucune.

6. Administration de la politique d’horodatage

6.1. Procédures de modification de la politique d’horodatage

Toute modification de la présente politique est préparée par le responsable d’application concerné, examinée par le responsable de sécurité et le contrôleur, puis approuvée par la commission d’approbation avant publication.

La commission qualifie chaque modification de mineure ou de substantielle. Une modification mineure — correction rédactionnelle, précision sans incidence sur les engagements — donne lieu à une nouvelle version publiée sans préavis. Une modification substantielle suit le régime énoncé ci-après.

Une modification substantielle d’une politique est annoncée dans le registre de publication 30 jours avant sa prise d’effet, sauf lorsqu’une exigence légale ou de sécurité impose un délai plus court.

Toute évolution modifiant le niveau d’exigence ou le champ d’application d’une politique donne lieu à un nouvel identifiant d’objet (OID).

Chaque version publiée porte son numéro, sa date de prise d’effet et la nature des modifications apportées. Les versions antérieures restent accessibles pendant la durée de conservation des archives, afin qu’un jeton ancien puisse toujours être rapporté à la politique en vigueur à sa date.

6.2. Procédures de publication et de notification

Le présent document est publié dans le registre de publication du site institutionnel de YORYX TRUST, accessible 24 heures sur 24, 7 jours sur 7, sans contrôle d’accès ni frais. Y sont également publiés :

- les politiques de certification et la politique d’horodatage
- la déclaration des pratiques de certification
- les déclarations de divulgation PKI
- les conditions générales d’utilisation de chaque service
- les formulaires d’enregistrement, de mandat et de révocation
- les guides d’inscription, de contrôle d’identité et d’utilisation
- les tarifs et la procédure de réclamation
- les certificats des autorités de certification
- les listes de révocation et le point d’accès au service d’information sur l’état des certificats

Toute nouvelle version d’un document du registre y est publiée au plus tard le jour de sa prise d’effet ; les versions antérieures restent accessibles pendant la durée de conservation des archives.

La consultation est libre ; seule l’écriture est restreinte aux fonctions habilitées, et toute modification est journalisée.

Une modification substantielle d’une politique est annoncée dans le registre de publication 30 jours avant sa prise d’effet, sauf lorsqu’une exigence légale ou de sécurité impose un délai plus court.

Toute évolution modifiant le niveau d’exigence ou le champ d’application d’une politique donne lieu à un nouvel identifiant d’objet (OID).

Une modification substantielle est en outre portée à la connaissance des services demandeurs par le canal contractuel convenu avec eux, et l’autorité nationale en est informée au titre des éléments au vu desquels la déclaration a été effectuée.

Le prestataire répond aux demandes d’information relatives à la présente politique à l’adresse trust@yoryx.com.

7. Dispositions juridiques et diverses

7.1. Protection des données à caractère personnel

Les traitements de données à caractère personnel réalisés à l’occasion du service d’horodatage sont soumis à la Loi n° 09-08 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel. L’autorité compétente est la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP).

Le service d’horodatage ne reçoit pas les données horodatées : la demande d’horodatage ne porte que l’empreinte cryptographique des données, calculée par le service demandeur. Le prestataire ne peut donc ni reconstituer, ni consulter, ni conserver le contenu horodaté, quel qu’il soit.

Le prestataire s’engage, au titre de la fourniture du service, à :

- préserver la sécurité et l’intégrité des données et empêcher toute utilisation détournée, malveillante ou frauduleuse
- empêcher tout accès ou toute publication non préalablement autorisés par l’utilisateur du service de confiance
- ne traiter les données que dans le cadre des instructions et de l’autorisation reçues de l’utilisateur
- s’assurer de la licéité des traitements réalisés dans le cadre de la prestation
- respecter l’obligation de secret, de sécurité et de confidentialité à l’occasion de toute opération de maintenance et de télémaintenance

Le prestataire met en œuvre les dispositions et moyens permettant à un utilisateur justifiant de son identité d’exercer son droit d’accès à ses données personnelles, son droit de rectification et son droit d’opposition, conformément à la législation en vigueur.

Les traitements de données à caractère personnel liés à la vérification d’identité font l’objet des formalités prévues par la loi n° 09-08 auprès de la CNDP, selon le régime que celle-ci retient pour ces traitements.

7.2. Conditions financières

Les conditions financières du service d’horodatage figurent dans YT-PRICING (OID 1.3.6.1.4.1.[PEN].1.7.1). Aucun montant n’est énoncé dans la présente politique, afin qu’une évolution tarifaire n’emporte aucune révision des engagements de sécurité.

Sont fournies sans frais :

- la révocation d’un certificat, quelle qu’en soit la cause
- l’accès aux listes de révocation et au service d’information sur l’état des certificats
- la vérification publique d’une signature, d’un cachet ou d’un jeton d’horodatage
- l’accès aux documents du registre de publication
- le traitement d’une réclamation

Les conditions commerciales applicables à l’utilisateur final relèvent de la plateforme SELLO ; les termes tarifaires du présent document sont ceux des services de confiance fournis par YORYX TRUST.

La grille des montants n’est pas publiée : YORYX TRUST fournit ses services de confiance à la plateforme SELLO dans le cadre d’une convention de service écrite, et les prix applicables à l’utilisateur final sont ceux des conditions commerciales de la plateforme.

7.3. Réclamations, droit applicable et règlement des litiges

Toute réclamation relative au service d’horodatage est adressée au prestataire par courrier électronique à trust@yoryx.com ou par courrier postal au siège social, 57, rue Mauritania, BP 2609, Guéliz, 40000 Marrakech, Maroc.

La réception d’une réclamation est accusée dans un délai de 5 jours ouvrés et une réponse motivée est apportée dans un délai de 30 jours calendaires à compter de la réception. À défaut de réponse satisfaisante, le réclamant peut demander le réexamen de son dossier dans un délai de 15 jours calendaires. La procédure complète est décrite dans YT-COMPLAINTS (OID 1.3.6.1.4.1.[PEN].1.7.2).

Chaque réclamation est enregistrée dans un registre interne portant sa date de réception, son objet, la fonction qui en a la charge, les suites données et sa date de clôture.

La DGSSI est l’autorité nationale des services de confiance ; elle contrôle a posteriori les prestataires non agréés (article 52 de la loi n° 43-20).

Le présent document est régi par le droit marocain. À défaut de règlement amiable, les litiges relèvent des tribunaux compétents de Marrakech.

7.4. Points ouverts

Les points suivants ne sont pas tranchés à la date de publication de la présente version. Ils sont énoncés comme tels plutôt que comblés par une affirmation, et seront levés dans une version ultérieure.

Points ouverts

Repère	Objet	Formulation retenue
OI-2	Délai statutaire de décision de l’autorité nationale sur une demande d’agrément, et frais de l’agrément.	selon les modalités et les délais fixés par l’autorité nationale
OI-5	Statut de certification du module cryptographique matériel effectivement mis en service.	Le module cryptographique matériel est retenu sur la base des profils de protection et des niveaux d’évaluation cités comme cibles au présent document ; la situation exacte de certification du matériel finalement mis en service est vérifiée avant toute affirmation, et aucune attestation de tiers n’est revendiquée à ce jour.

8. Annexes

8.1. Profil du jeton d’horodatage

Le profil ci-après précise le contenu des jetons délivrés, conformément à ETSI EN 319 422, protocole IETF RFC 3161.

Contenu du jeton d’horodatage

Champ	Présence	Contenu
version	obligatoire	Version de la structure du jeton.
policy	obligatoire	Identifiant de la politique applicable : 1.3.6.1.4.1.[PEN].1.1.3.1.
messageImprint	obligatoire	Empreinte reçue et identifiant de la fonction de hachage employée, au moins équivalente à SHA-256.
serialNumber	obligatoire	Entier identifiant le jeton de manière unique au sein de l’unité d’horodatage qui l’a délivré.
genTime	obligatoire	Date et heure de génération, exprimées en temps universel coordonné, avec une précision compatible avec l’exactitude déclarée.
accuracy	obligatoire	Exactitude déclarée du temps porté par le jeton : 1 seconde ou mieux.
ordering	absent ou faux	Le service ne garantit pas l’ordonnancement de deux jetons non distinguables au regard de l’exactitude déclarée.
nonce	conditionnel	Reproduit à l’identique lorsque la demande en comportait un.
tsa	facultatif	Nom de l’unité d’horodatage, lorsqu’il est présent, sans valeur d’identification autonome.
extensions	aucune critique	Aucune extension critique n’est employée.
Référence du certificat signataire	obligatoire	Attribut signé identifiant le certificat de l’unité d’horodatage, afin d’écarter toute ambiguïté sur la clé de vérification.

La demande d’horodatage comporte l’empreinte, l’identifiant de politique demandé, le cas échéant un nombre aléatoire, et l’indication de la demande de restitution du certificat signataire. Elle ne comporte jamais les données elles-mêmes.

8.2. Profil du certificat d’unité d’horodatage

Certificat d’unité d’horodatage

Champ	Valeur
Émetteur	YORYX TRUST Timestamping CA G1
Pays du sujet	MA
Organisation du sujet	YORYX TRUST SASU
Identifiant d’organisation	NTRMA-184667
Nom commun du sujet	YORYX TRUST TSU 1 G1, unique au sein du service
Clé publique	RSA 3072 bits
Algorithme de signature du certificat	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
Période de validité	5 ans
Usage de clé	signature numérique, à l’exclusion de tout autre usage
Usage étendu de clé	horodatage exclusivement, marqué critique (1.3.6.1.5.5.7.3.8)
Politique de certificat	1.3.6.1.4.1.[PEN].1.1.3.1
Point de distribution de liste de révocation	publié dans le registre de publication, accessible sans frais
Accès à l’information de l’autorité	service d’information sur l’état des certificats (IETF RFC 6960)

Le nom distinctif (DN) est unique au sein du domaine de l’autorité de certification ; un DN n’est jamais réattribué à un autre titulaire.

8.3. Algorithmes et longueurs de clés

Algorithmes du service d’horodatage

Emploi	Algorithme
Bi-clé de l’autorité racine	RSA 4096 bits
Signature de l’autorité racine	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
Bi-clé de l’autorité émettrice	RSA 4096 bits
Signature de l’autorité émettrice	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
Bi-clé de l’unité d’horodatage	RSA 3072 bits

Emploi	Algorithme
Signature des jetons d’horodatage	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
Bi-clé du répondeur d’état	RSA 3072 bits
Empreinte minimale admise	SHA-256

Les algorithmes sur courbes elliptiques (ECDSA sur courbe P-256 ou P-384) peuvent être introduits ultérieurement pour les certificats de titulaires ; leur mise en service donne lieu à une révision de la présente politique.

Les suites cryptographiques mises en œuvre sont conformes à la norme ETSI TS 119 312 (version 1.4.2 ou ultérieure).

8.4. Correspondance avec la norme ETSI EN 319 421

Le tableau ci-après indique, pour chaque chapitre de la norme visée, la section de la présente politique qui en traite. Il est fourni pour faciliter la lecture d’un évaluateur et n’emporte aucune constatation de conformité.

Chapitres de la norme et sections correspondantes

Chapitre de la norme	Section de la présente politique
Politiques d’horodatage — généralités et identification	3.1, 3.2
Appréciation des risques	5.5.1
Déclaration des pratiques	5.1.1
Conditions générales d’utilisation	1.7, 4.3 et YT-CGU-TSA
Politique de sécurité de l’information	5.5.1, 5.5.2
Obligations du prestataire	4.1, 4.2
Information des utilisateurs finaux	4.3, 4.4
Organisation interne	2.2, 2.4, 5.5.3
Sécurité du personnel	5.5.3
Gestion des biens	5.5.2
Contrôle d’accès	5.5.7
Contrôles cryptographiques et cycle de vie des clés	5.2.1 à 5.2.5
Délivrance des jetons et synchronisation	5.3.1, 5.3.2

Chapitre de la norme	Section de la présente politique
Sécurité physique et environnementale	5.5.4, 5.5.6
Sécurité d’exploitation	5.5.5, 5.5.8
Sécurité des réseaux	5.5.5, 5.5.7
Gestion des incidents	5.5.9
Collecte des preuves	5.5.11
Continuité d’activité	5.5.9
Cessation d’activité	5.5.10
Conformité et audits	3.3
Chaîne d’approvisionnement	5.5.8

9. Références

9.1. Textes législatifs et réglementaires

[Loi 43-20] Loi n° 43-20 relative aux services de confiance pour les transactions électroniques, promulguée par le dahir n° 1-20-100 du 31 décembre 2020, publiée au Bulletin officiel n° 6970 du 18 mars 2021.

Articles de la loi n° 43-20 cités au présent document

Article	Objet
Article premier	objet de la loi : régime applicable aux services de confiance pour les transactions électroniques, aux moyens et prestations de cryptologie, aux opérations des prestataires et aux règles que ceux-ci et les titulaires de certificats doivent respecter
Article 2	définition du prestataire de services de confiance : toute personne morale qui fournit un ou plusieurs services de confiance, agréé ou non agréé
Article 3	énumération des services de confiance : création de signatures, de cachets, d’horodatage électronique ou d’envoi recommandé électronique ; création des certificats correspondants ; validation ; conservation
Article 4	les trois niveaux : une signature électronique est soit simple, soit avancée, soit qualifiée
Article 32	seuls les prestataires agréés peuvent fournir un service de confiance qualifié, émettre et délivrer les certificats électroniques qualifiés et gérer les opérations y afférentes
Article 33	conditions de l’agrément : constitution en société de droit marocain (a), assurance de responsabilité professionnelle (d), plan de continuité d’activité (e), vérification de l’identité du titulaire du certificat, et encadrement des sous-traitants (c)
Article 35	toute personne qui se propose de fournir des services de confiance autres que qualifiés doit se déclarer au préalable auprès de l’autorité nationale, selon des modalités fixées par voie réglementaire
Article 37	le prestataire informe préalablement l’autorité nationale, dans un délai minimum de deux mois, avant de mettre fin à ses activités
Article 40	les prestataires agréés et non agréés notifient immédiatement à l’autorité nationale toute atteinte à la sécurité ou toute perte d’intégrité ayant une incidence sur le service ou sur les données à caractère personnel conservées
Article 52	missions de l’autorité nationale : fixer les normes et référentiels, agréer les prestataires qualifiés et contrôler leurs activités, contrôler a posteriori les prestataires non agréés, proposer les projets de textes

Article	Objet
Article 53	publication d’un extrait de la décision d’agrément au Bulletin officiel, tenue d’un registre annuel, et publication sur le site internet de l’autorité de la liste des prestataires agréés et de celle des prestataires non agréés ayant effectué leur déclaration préalable

[Décret 2-22-687] Décret n° 2-22-687 du 16 novembre 2022 pris pour l’application de la loi n° 43-20 relative aux services de confiance pour les transactions électroniques, Bulletin officiel n° 7162 du 19 janvier 2023.

Articles du décret n° 2-22-687 cités au présent document

Article	Objet
Article premier	l’autorité nationale des services de confiance est la direction générale de la sécurité des systèmes d’information relevant de l’Administration de la défense nationale
Article 18	sans préjudice des délais prévus par la législation en vigueur, les données relatives à la fourniture des services de confiance sont conservées pendant une durée minimale de sept (7) ans, les types de données étant définis dans les référentiels d’exigences
Article 19	la notification des atteintes à la sécurité ou des pertes d’intégrité prévues à l’article 40 de la loi s’effectue selon les modalités fixées dans le référentiel de gestion des incidents de cybersécurité
Article 21	la déclaration préalable prévue à l’article 35 de la loi est déposée auprès de l’autorité nationale contre récépissé ou lui est adressée par envoi recommandé postal ou électronique, accompagnée des documents fixés à l’annexe n° 3 ; le déclarant informe l’autorité de toute modification de l’un des éléments au vu desquels la déclaration a été effectuée
Article 23	les dispositions des articles 18 et 19 (conservation pendant sept ans et notification des incidents) s’appliquent aux prestataires fournissant des services de confiance autres que qualifiés

[Loi 09-08] Loi n° 09-08 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel.

9.2. Référentiels de l’autorité nationale

[Ref_PSCo_AG] Référentiel d’exigences relatif aux services de confiance qualifiés et aux prestataires fournissant ces services — Exigences générales de conformité des prestataires fournissant des services de confiance qualifiés, version 1.0, 13 juillet 2023.

[Ref_Serv_Conf_NonQual] Référentiel d’exigences de conformité relatives aux services de confiance non qualifiés, version 1.0, 13 juillet 2023.

[Ref_Horo_Qual] Référentiel d’exigences relatif au service d’horodatage électronique qualifié, version 1.0, 13 juillet 2023.

[Ref_Conserv_Qual] Référentiel d’exigences relatif au service de conservation qualifié, version 1.0, 13 juillet 2023.

[Ref_Deliv_Cert_Qual] Référentiel d’exigences relatif au service de délivrance de certificats électroniques qualifiés, version 1.0, 13 juillet 2023.

[Ref_QSCD] Référentiel d’exigences relatif aux dispositifs qualifiés de création de signature et de cachet électroniques, version 1.0, 13 juillet 2023.

[Ref_Valid_Qual] Référentiel d’exigences relatif au service de validation qualifié, version 1.0, 13 juillet 2023.

PC-type PSCE Politique de certification de référence — PC-type d’un prestataire de services de certification électronique (PSCE), version 1.3, mai 2015.

9.3. Normes et spécifications techniques visées

Les textes ci-après sont cités comme cibles de conformité. Leur mention n’emporte aucune constatation de conformité et aucune attestation de tiers n’est revendiquée.

[ETSI EN 319 401] ETSI EN 319 401, V3.2.1 — General Policy Requirements for Trust Service Providers.

[ETSI EN 319 421] ETSI EN 319 421, V1.3.1 — Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

[ETSI EN 319 422] ETSI EN 319 422, V1.1.1 — Time-stamping protocol and time-stamp token profiles.

[ETSI EN 319 411-1] ETSI EN 319 411-1, V1.5.1 (2025-04) — Policy and security requirements for Trust Service Providers issuing certificates — Part 1: General requirements.

[ETSI TS 119 312] ETSI TS 119 312, v1.4.2 ou ultérieure — Cryptographic Suites.

[IETF RFC 3161] IETF RFC 3161 — Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

[IETF RFC 5280] IETF RFC 5280 — Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

[IETF RFC 6960] IETF RFC 6960 — X.509 Internet Public Key Infrastructure Online Certificate Status Protocol — OCSP.

[IETF RFC 5905] IETF RFC 5905 — Network Time Protocol Version 4: Protocol and Algorithms Specification.

[CEN EN 419 221-5] CEN EN 419 221-5 — Protection Profiles for TSP Cryptographic Modules — Part 5: Cryptographic Module for Trust Services.

[CEN EN 419 231] CEN EN 419 231 — Protection profile for trustworthy systems supporting time stamping.

[Critères Communs (ISO/IEC 15408), niveau EAL4+] Critères Communs (ISO/IEC 15408), niveau EAL4+ — Common Criteria for Information Technology Security Evaluation, CC:2022 Release 1.

[IETF RFC 3647] IETF RFC 3647 — Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.