YORYX® TRUST SASU

Conditions générales d’utilisation – personne morale

YT-CGU-PM

OID : 1.3.6.1.4.1.[PEN].1.4.2

Version 0.1

5 septembre 2026

Projet — en préparation de la déclaration préalable

Diffusion publique

Identification du document

Champ	Valeur
Titre du document	Conditions générales d’utilisation – personne morale
Identifiant du document	YT-CGU-PM
Identifiant d'objet (OID)	1.3.6.1.4.1.[PEN].1.4.2
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. Objet, parties et documents contractuels....5
1.1. Objet....5
1.2. Parties et positionnement....5
1.3. Identification du prestataire....6
1.4. Statut réglementaire....6
1.5. Conformité et évaluations....7
1.6. Mention de marque....7
1.7. Identification du document....7
1.8. Documents contractuels et ordre de prévalence....7
1.9. Acceptation et entrée en vigueur....8
1.10. Définitions....9
2. Services couverts, niveaux et limites d’usage....11
2.1. Services fournis....11
2.2. Niveaux et politiques de référence....11
2.3. Le modèle de cachet....12
2.4. Limites d’usage....13
3. Enregistrement, vérification de l’identité et délivrance....14
3.1. Demande et enregistrement....14
3.2. Vérification de l’identité....14
3.3. Délivrance, remise et acceptation du certificat....15
3.4. Données d’activation et contrôle exclusif....15
4. Obligations des parties....16
4.1. Obligations du prestataire....16
4.2. Engagements de disponibilité....16
4.3. Obligations de la plateforme, autorité d’enregistrement....17
4.4. Obligations du titulaire, personne morale....17
4.5. Obligations du représentant légal et des mandataires....18
4.6. Obligations de l’utilisateur de certificat....18
5. Cycle de vie du certificat....20
5.1. Durée de validité....20
5.2. Renouvellement....20
5.3. Révocation....20
5.3.1. Causes de révocation....20
5.3.2. Qui peut demander la révocation....21

5.3.3. Comment et dans quel délai....21
5.4. Suspension....21
5.5. Fin de la relation....22
6. Conditions financières....23
7. Responsabilité, garanties et assurance....24
8. Protection des données à caractère personnel....25
8.1. Cadre applicable et autorité compétente....25
8.2. Données traitées et finalités....25
8.3. Engagements du prestataire....25
8.4. Durées de conservation....26
8.5. Droits des personnes concernées....26
9. Preuve, conservation et archivage....27
10. Modification, publication, réclamations et litiges....28
10.1. Modification des présentes conditions....28
10.2. Publication....28
10.3. Cession....28
10.4. Réclamations, droit applicable et règlement des litiges....29
11. Références....30
11.1. Textes législatifs et réglementaires....30
11.2. Référentiels de l’autorité nationale....31
11.3. Normes et spécifications techniques visées....32
11.4. Documents du registre de publication cités....32

1. Objet, parties et documents contractuels

1.1. Objet

Les présentes conditions générales d’utilisation définissent les conditions dans lesquelles YORYX TRUST SASU délivre et gère les certificats de cachet électronique destinés aux personnes morales, ainsi que l’apposition de cachets électroniques par les systèmes de la personne morale à travers la plateforme. Elles énoncent les droits et les obligations réciproques du prestataire, du titulaire, de la plateforme et de l’utilisateur de certificat.

Elles complètent la politique de certification YT-PC-SEAL (OID 1.3.6.1.4.1.[PEN].1.1.2), dont elles ne modifient ni la portée ni les engagements de sécurité, et dont elles reprennent en termes opposables les responsabilités énoncées à son chapitre 1.9.

1.2. Parties et positionnement

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.

L’exigence 10 du référentiel [Ref_Serv_Conf_NonQual] admet expressément qu’un tiers exerce les fonctions d’autorité d’enregistrement pour le compte du prestataire, sous réserve d’un contrat écrit préalable ; l’article 33 c) de la loi n° 43-20 en constitue le fondement légal pour l’encadrement des sous-traitants.

Sur la voie de l’agrément, le paragraphe dérogatoire de l’article 33 de la loi n° 43-20 ajoute une condition : « Par dérogation aux dispositions de l’article 32 ci-dessus, ces informations peuvent être vérifiées par un tiers dans le cadre d’un contrat de sous-traitance liant ce dernier avec le prestataire concerné et approuvé par l’autorité nationale. » Le contrat de sous-traitance devra alors être approuvé par l’autorité nationale ; l’exigence 10 du référentiel [Ref_Serv_Conf_NonQual] demeure le fondement applicable au régime déclaratif sous lequel le présent document est publié.

Il en résulte que le titulaire est lié au prestataire par la politique de certification et par les présentes conditions, tandis que les conditions commerciales applicables à l’utilisateur final — souscription, facturation, assistance de premier niveau — relèvent de la plateforme.

1.3. Identification du prestataire

Identification du prestataire

Élément	Valeur
Dénomination sociale	YORYX TRUST SASU
Forme juridique	société par actions simplifiée à associé unique (SASU)
Capital social	100 000,00 dirhams, intégralement libéré en numéraire
Registre du commerce	RC Marrakech n° 184667, immatriculée le 28 juillet 2026
Identifiant commun de l’entreprise (ICE)	004013324000019
Identifiant fiscal	73266987
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

1.4. 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.

> **Niveau qualifié —** La signature électronique qualifiée, seule à bénéficier de la présomption de fiabilité, n’est pas encore proposée par YORYX TRUST : elle le sera après agrément par la DGSSI.

> **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.

1.5. Conformité et évaluations

Aucune évaluation de conformité de tiers n’a été conduite à ce jour et aucun schéma d’évaluation n’a délivré d’attestation portant sur les services couverts par les présentes conditions. Les normes et référentiels cités le sont comme cibles de conformité.

Le prestataire soumet ses composantes à un contrôle interne de conformité 1 fois par an et à un audit externe indépendant tous les 2 ans, portant sur la conformité de l’infrastructure de gestion de clés à la politique de certification, à la déclaration des pratiques et à la politique de sécurité. 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.

1.6. 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.

1.7. Identification du document

Le présent document est identifié par l’identifiant d’objet (OID) 1.3.6.1.4.1.[PEN].1.4.2. 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 d’une politique donne lieu à un nouvel identifiant d’objet (OID).

1.8. Documents contractuels et ordre de prévalence

La relation est régie par les documents suivants, dans cet ordre de prévalence :

1. la politique de certification YT-PC-SEAL (OID 1.3.6.1.4.1.[PEN].1.1.2) ;
2. les présentes conditions générales d’utilisation ;
3. la déclaration des pratiques de certification YT-DPC (OID 1.3.6.1.4.1.[PEN].1.2) ;
4. les termes tarifaires YT-PRICING (OID 1.3.6.1.4.1.[PEN].1.7.1) ;
5. le formulaire d’enregistrement signé par le demandeur, YT-FORM-LEGAL-REP (OID 1.3.6.1.4.1.[PEN].1.5.2), pour ce qui relève des déclarations qu’il porte.

La déclaration de divulgation YT-PDS-CERT (OID 1.3.6.1.4.1.[PEN].1.3.1) est un résumé publiable : elle n’a pas de valeur contractuelle propre et ne peut être opposée à la politique de certification.

Les guides YT-GUIDE-ENROLMENT, YT-GUIDE-IDENTITY et YT-GUIDE-USE sont des documents d’aide à la mise en œuvre ; ils n’ajoutent aucune obligation et ne dérogent à aucune des stipulations ci-dessous.

1.9. Acceptation et entrée en vigueur

L’acceptation des présentes conditions résulte de leur acceptation expresse par le représentant légal de la personne morale, ou par le mandataire qu’il a habilité par écrit, lors de la demande sur la plateforme et préalablement à toute délivrance de certificat. Elle engage la personne morale. Aucun certificat n’est délivré à un demandeur qui ne les a pas acceptées.

Les présentes conditions sont portées à la connaissance du demandeur, de manière claire et aisément accessible, avant l’entrée en relation contractuelle, dans un espace accessible au public et individuellement dans son espace sur la plateforme. Elles sont communiquées en français, sur un support durable qui en préserve l’intégrité dans le temps et sous une forme lisible par une personne ; cette communication peut être électronique.

L’acceptation résulte d’un acte volontaire et traçable du demandeur, recueilli par la plateforme, horodaté et conservé dans le dossier d’enregistrement ; elle est opposable au titulaire, qui reconnaît avoir été mis en mesure de prendre connaissance des présentes conditions avant de les accepter.

En acceptant les présentes conditions, le demandeur :

1. adhère aux obligations mises à sa charge par le chapitre relatif aux obligations des parties ;
2. accepte que les données de création de cachet soient générées et conservées dans le module cryptographique matériel exploité par le prestataire et mises en œuvre exclusivement par son intermédiaire ;
3. confirme l’exactitude des informations destinées à figurer dans le certificat ;
4. consent à la conservation par le prestataire des informations recueillies lors de l’enregistrement, des évènements de délivrance et de révocation, de l’identité et des attributs portés dans le certificat, pendant la durée fixée au chapitre relatif à la preuve et à l’archivage ;
5. consent à la transmission de ces mêmes informations à un autre prestataire, dans les mêmes conditions de protection que celles des présentes conditions, dans le seul cas d’une cessation d’activité avec reprise du service ;
6. prend acte de ce que les certificats de titulaires ne sont pas publiés et ne font l’objet d’aucun annuaire.

Le représentant légal informe des obligations qui en résultent les personnes physiques qu’il habilite à administrer les systèmes appelant le service ; ces personnes agissent au nom de la personne morale et ne sont identifiées dans aucun certificat.

Les présentes conditions entrent en vigueur à la date de leur publication dans le registre de publication et s’appliquent jusqu’à la publication d’une version postérieure. La version opposable au titulaire est celle en vigueur à la date de délivrance de son certificat, sous réserve du chapitre relatif à la modification des présentes conditions.

1.10. Définitions

Termes employés dans les présentes conditions

Terme	Définition
Prestataire	YORYX TRUST SASU, prestataire de services de confiance qui délivre et gère les certificats couverts par les présentes conditions.
Plateforme	La plateforme SELLO, canal d’enregistrement et de fourniture du service, qui exerce les fonctions d’autorité d’enregistrement pour le compte du prestataire et qui est la contrepartie commerciale de l’utilisateur final.
Autorité d’enregistrement	Fonction qui prend en compte et vérifie les informations d’identité de la personne morale et de son représentant, et constitue le dossier d’enregistrement correspondant.
Titulaire	La personne morale identifiée dans le certificat, pour le compte de laquelle les données de création de cachet correspondant à la clé publique qui y figure sont mises en œuvre.
Créateur du cachet	La personne morale titulaire, agissant par ses systèmes à travers la plateforme ; les personnes physiques qui administrent ces systèmes agissent en son nom et ne sont pas identifiées dans le certificat.
Représentant légal	La personne physique qui dispose du pouvoir d’engager la personne morale, qui présente la demande, accepte les présentes conditions et exerce, pour le compte de la personne morale, les droits attachés au certificat.
Mandataire	La personne physique désignée par écrit par le représentant légal pour exercer, dans la limite du mandat qui lui est conféré, tout ou partie de ces droits ; le mandat est consigné dans le formulaire prévu à cet effet.
Personne autorisée	Personne, autre que le représentant légal et le mandataire, habilitée par la politique de certification ou par contrat à accomplir certaines actions pour le compte du titulaire, notamment une demande de révocation.
Utilisateur de certificat	Personne ou entité qui reçoit un certificat et s’y fie pour vérifier un cachet électronique.
Données de création de cachet	Données propres au titulaire au moyen desquelles un cachet électronique est apposé ; elles sont générées et conservées dans le module cryptographique matériel exploité par le prestataire.
Données d’activation	Les moyens d’authentification des systèmes de la personne morale auprès de la plateforme, dont la mise en œuvre conditionne chaque apposition de cachet.

Terme	Définition
Module cryptographique matériel	Équipement matériel dédié aux opérations cryptographiques, à l’intérieur duquel les données de création de cachet sont générées et conservées, et dont elles ne sortent jamais en clair.
Révocation	Fin anticipée et définitive de la validité d’un certificat, portée à la connaissance des tiers par les informations d’état publiées par le prestataire.
Registre de publication	L’espace de publication documentaire du site institutionnel du prestataire, où sont mis à disposition les documents énumérés au chapitre relatif à la publication.

2. Services couverts, niveaux et limites d’usage

2.1. Services fournis

Les services couverts par les présentes conditions sont les suivants :

Services de confiance couverts par les présentes conditions

Service	Niveau et sujet	Norme visée et identifiant du service
Délivrance de certificats de cachet électronique — niveau simple	simple — personne morale	ETSI EN 319 411-1 1.3.6.1.4.1.[PEN].1.1.2.1
Délivrance de certificats de cachet électronique — niveau avancé	avancé — personne morale	ETSI EN 319 411-1 1.3.6.1.4.1.[PEN].1.1.2.2
Apposition de cachets électroniques par les systèmes du titulaire	avancé — personne morale	CEN EN 419 241-1 et -2 en cible 1.3.6.1.4.1.[PEN].1.1.2.2

Ces services relèvent des services de confiance énumérés à l’article 3 de la loi n° 43-20 et sont fournis en dehors du régime des services qualifiés.

Les services de confiance qualifiés au sens de la loi n° 43-20 ne font pas partie des présentes conditions : ils constituent une cible, ouverte après agrément par l’autorité nationale. L’article 15 de la même loi subordonne en effet le cachet électronique qualifié à un dispositif qualifié de création de cachet et à un certificat qualifié, et son article 32 réserve la fourniture d’un service qualifié aux prestataires agréés.

2.2. Niveaux et politiques de référence

L’article 4 de la loi n° 43-20 distingue trois niveaux pour la signature électronique — simple, avancée et qualifiée — et la même gradation vaut pour le cachet électronique, dont l’article 15 de la même loi définit le niveau qualifié. Les présentes conditions couvrent les deux premiers niveaux, qui relèvent du régime déclaratif des services de confiance autres que qualifiés.

Niveaux proposés et politiques de référence

Niveau	OID de la politique	Politique ETSI de référence	Validité du certificat
Niveau simple	1.3.6.1.4.1.[PEN].1.1.2.1	LCP — Lightweight Certificate Policy 0.4.0.2042.1.3	1 an
Niveau avancé	1.3.6.1.4.1.[PEN].1.1.2.2	NCP+ — Normalized Certificate Policy requiring a secure cryptographic device 0.4.0.2042.1.2	3 ans

Les données de création de signature ou de cachet sont générées et conservées dans un module cryptographique matériel exploité par le prestataire et ne sont utilisées qu’après authentification

forte du signataire ou du créateur du cachet : l’architecture décrite répond, en cible, à la condition propre à NCP+ — l’emploi d’un dispositif cryptographique sécurisé — dont la conformité n’est pas encore constatée.

Le niveau porté par un certificat est inscrit dans son extension certificatePolicies : l’utilisateur de certificat lit cet identifiant pour connaître le niveau sous lequel le certificat a été délivré, et n’a pas à s’en remettre à une déclaration extérieure.

> **Niveau qualifié —** La signature électronique qualifiée, seule à bénéficier de la présomption de fiabilité, n’est pas encore proposée par YORYX TRUST : elle le sera après agrément par la DGSSI.

2.3. Le modèle de cachet

Le cachet est apposé par les systèmes de la personne morale à travers la plateforme, sans geste manuel et sans support remis à une personne physique.

Le cachet électronique est imputable à la personne morale titulaire et non à une personne physique : il garantit l’origine et l’intégrité des données cachetées. Il ne se substitue pas à la signature électronique d’une personne physique, laquelle exprime un consentement ou un engagement personnel.

Les données de création de cachet du titulaire sont générées à l’intérieur du module cryptographique matériel exploité par YORYX TRUST et n’en sortent jamais en clair ; elles ne sont copiées sur aucun support, exportées vers aucun poste et remises à aucun tiers.

L’utilisation des données de création de cachet est subordonnée à une authentification forte du créateur du cachet, exercée par les systèmes de la personne morale à travers la plateforme.

Aucun matériel n’est remis à la personne morale ni à aucune des personnes physiques qui administrent ses systèmes : ni clé USB, ni carte à puce, ni lecteur, ni programme à installer. Le support physique est remplacé par le module cryptographique matériel exploité par le prestataire, et l’accès au service est commandé par les moyens d’authentification enrôlés pour le compte de la personne morale.

L’intégration du cachet dans les systèmes de la personne morale s’effectue par les interfaces de la plateforme. La personne morale détermine librement les traitements qui appellent le service, tient à jour la liste des personnes qu’elle habilite à les administrer et répond des cachets apposés pour son compte.

Ce modèle de signature côté serveur est décrit par les normes CEN EN 419 241-1 et CEN EN 419 241-2, que le référentiel [Ref_QSCD] de la DGSSI recense parmi les textes applicables aux dispositifs de création de signature soumis à l’agrément. Ces normes sont des cibles de travail : aucune conformité n’est constatée à ce jour et aucune attestation de tiers n’est revendiquée.

Les formats de cachet et de conteneur admis pour le niveau avancé sont ceux fixés par l’exigence 25 du référentiel [Ref_Serv_Conf_NonQual] :

- PAdES (ETSI EN 319 142-1)
- XAdES (ETSI EN 319 132-1)
- CAdES (ETSI EN 319 122-1)
- ASiC (ETSI EN 319 162-1)

La vérification d’une signature, d’un cachet ou d’un jeton d’horodatage est publique : le destinataire d’un document n’a besoin ni d’un compte, ni d’un logiciel, ni d’un abonnement.

2.4. Limites d’usage

La bi-clé et le certificat d’un titulaire servent exclusivement à l’apposition et à la vérification de cachets électroniques imputables à une personne morale. Les usages admis sont les suivants :

- cachet électronique apposé sur les documents émis par la personne morale, notamment factures, attestations, relevés et pièces justificatives ;
- cachet électronique apposé sur des flux de données échangés avec une administration ou une entreprise, lorsque celle-ci accepte le niveau du certificat présenté ;
- vérification, par tout utilisateur de certificat, d’un cachet électronique apposé par le titulaire pendant la période de validité du certificat.

Sont exclus : le chiffrement de données, l’authentification de serveur, la signature de code, l’authentification d’un site internet au sens de l’article 30 de la loi n° 43-20, l’usage du cachet en lieu et place de la signature d’une personne physique, l’apposition d’un cachet sur des données dont la personne morale n’est pas à l’origine et dont elle n’assume pas l’émission, ainsi que tout usage pour lequel la réglementation exige un certificat qualifié.

Le titulaire s’interdit tout usage des services à des fins de perturbation, d’intrusion, de contournement des contrôles d’accès, de charge anormale ou d’analyse non autorisée des composantes du prestataire.

Un usage en dehors des limites énoncées ci-dessus est un manquement du titulaire ; il exonère le prestataire dans les conditions du chapitre relatif à la responsabilité et peut justifier la révocation du certificat.

3. Enregistrement, vérification de l’identité et délivrance

3.1. Demande et enregistrement

L’enregistrement d’un titulaire personne morale se déroule selon les étapes suivantes.

1. Le représentant légal ouvre une demande sur la plateforme au nom de la personne morale et fournit les informations destinées à figurer dans le certificat, dont le nom du cachet.
2. Il produit les pièces établissant l’existence de la personne morale et son identifiant officiel, ainsi que les pièces établissant sa propre qualité et l’étendue de ses pouvoirs.
3. Il produit sa carte nationale d’identité électronique, référence d’identité retenue, ou une autre pièce officielle d’identité en cours de validité lorsque la première ne peut être produite.
4. L’autorité d’enregistrement contrôle les pièces produites et vérifie l’identité du représentant, en présence physique à titre de règle de base, ainsi que la cohérence des informations de la personne morale.
5. Le représentant enrôle les moyens d’authentification par lesquels les systèmes de la personne morale accèderont au service.
6. Il prend connaissance de la politique de certification YT-PC-SEAL, de la déclaration de divulgation YT-PDS-CERT et des présentes conditions, et les accepte expressément au nom de la personne morale.
7. L’autorité d’enregistrement clôt le dossier et transmet la demande validée à la fonction de génération des certificats.

Le dossier d’enregistrement comprend au minimum les pièces produites et le résultat de leur contrôle, la date, le mode de vérification retenu et la fonction ayant procédé au contrôle, ainsi que l’acceptation des présentes conditions. Il est conservé pendant la durée fixée au chapitre relatif à la preuve et à l’archivage. Le formulaire correspondant est publié dans le registre sous l’identifiant YT-FORM-LEGAL-REP.

Le demandeur atteste de l’exactitude et de la complétude des informations qu’il fournit. Une demande dont l’identité ou les pièces n’ont pu être vérifiées est rejetée ; le rejet est motivé, notifié et consigné. Un rejet fondé sur un doute sur l’identité n’est pas levé par une simple réitération de la demande.

3.2. Vérification de l’identité

La référence d’identité retenue est la carte nationale d’identité électronique (CNIE). Le contrôle d’identité est conduit en présence physique à titre de règle de base ; la vérification à distance s’effectue selon les modalités admises par le référentiel de la DGSSI.

L’exigence 11 du référentiel [Ref_Serv_Conf_NonQual] rend applicables — suffisantes sans être nécessaires — les dispositions de vérification de l’identité du référentiel [Ref_Deliv_Cert_Qual] pour la délivrance de certificats autres que qualifiés conformes à la norme ETSI EN 319 411-1, en particulier de type NCP et NCP+. Le prestataire s’y adosse pour le niveau avancé.

> **Point ouvert —** La vérification d’identité à distance est conduite selon les modalités admises par le référentiel de la DGSSI. Aucune méthode de vérification d’identité à distance n’est annoncée ici et aucune intégration de la carte nationale d’identité électronique n’existe à ce jour : elle est décrite comme une cible.

La demande étant toujours présentée pour le compte d’une personne morale, la vérification de l’autorité du demandeur est systématique : l’autorité d’enregistrement vérifie l’existence de la personne morale, la qualité du représentant légal et l’étendue de ses pouvoirs au vu de pièces officielles et, lorsque la demande est présentée par un mandataire, la désignation écrite de celui-ci et l’étendue du mandat. Les formulaires YT-FORM-LEGAL-REP et, le cas échéant, YT-FORM-MANDATE consignent ces éléments.

Aucune information non vérifiée n’est portée dans un certificat. Les informations recueillies pour les seuls besoins de la relation de service et non portées dans le certificat ne sont pas certifiées et n’engagent pas le prestataire à l’égard des tiers.

3.3. Délivrance, remise et acceptation du certificat

Le certificat est établi dès la validation complète du dossier. Aucun certificat n’est généré par anticipation. Le titulaire est informé de la délivrance dans son espace sur la plateforme et par un message adressé à l’adresse électronique de contact enregistrée.

Le titulaire prend connaissance du contenu du certificat et l’accepte explicitement avant tout usage. L’acceptation vaut reconnaissance de l’exactitude des informations portées dans le certificat. À défaut d’acceptation, ou en cas de contestation d’une information portée dans le certificat, celui-ci est révoqué et, à la demande du titulaire, une nouvelle demande est instruite.

Les certificats de titulaires ne sont pas publiés et ne font l’objet d’aucun annuaire. Sont publiés dans le registre de publication du site institutionnel de YORYX TRUST les certificats des autorités de certification, les listes de révocation et le point d’accès au service d’information sur l’état des certificats.

3.4. Données d’activation et contrôle exclusif

L’utilisation des données de création de cachet est subordonnée à une authentification forte du créateur du cachet, exercée par les systèmes de la personne morale à travers la plateforme.

Aucun code PIN, aucun support matériel et aucun logiciel installé ne sont remis au titulaire : les données d’activation sont les facteurs d’authentification du titulaire, qu’il est seul à détenir.

La personne morale protège les moyens d’authentification de ses systèmes auprès de la plateforme, en restreint l’usage aux personnes qu’elle habilite, tient à jour la liste de ces habilitations et signale sans délai toute compromission. La compromission d’un moyen d’authentification entraîne sa révocation et un nouvel enrôlement, les données de création de cachet demeurant dans le module cryptographique matériel.

Le prestataire ne détient pas les facteurs d’authentification du titulaire ; il n’en conserve que les éléments de vérification. Il ne peut donc ni les reconstituer, ni les communiquer, ni s’y substituer.

4. Obligations des parties

Les engagements ci-dessous reprennent, en termes opposables à la partie qui les souscrit, les responsabilités énoncées au chapitre 1.9 de la politique de certification YT-PC-SEAL (OID 1.3.6.1.4.1.[PEN].1.1.2). Ils s’ajoutent aux obligations légales et réglementaires.

4.1. Obligations du prestataire

Quelle que soit l’organisation opérationnelle mise en œuvre, le prestataire demeure responsable, vis-à-vis de toute partie externe à son infrastructure, des prestations fournies et du respect des engagements pris. Le prestataire s’engage à :

- appliquer la politique de certification applicable et faire appliquer, par chacune de ses composantes, les procédures correspondantes de sa déclaration des pratiques ;
- vérifier, avant toute délivrance, l’identité du futur titulaire dans les conditions du chapitre 3 des présentes conditions, et conserver les preuves de cette vérification ;
- générer les données de création de cachet des titulaires à l’intérieur du module cryptographique matériel et garantir qu’elles n’en sortent jamais en clair ;
- ne délivrer que des certificats conformes au profil publié par la politique de certification et à la politique dont l’identifiant y est inscrit ;
- publier et maintenir accessibles, 24 heures sur 24, 7 jours sur 7, sans contrôle d’accès ni frais, les certificats d’autorité, les listes de révocation et le service d’information sur l’état des certificats ;
- traiter toute demande de révocation valide dans un délai maximal de 24 heures et publier l’information d’état correspondante dans un délai maximal de 24 heures ;
- conserver les données relatives à la fourniture du service pendant 7 ans au moins, conformément aux articles 18 et 23 du décret n° 2-22-687 ;
- notifier à l’autorité nationale, conformément à l’article 40 de la loi n° 43-20, toute atteinte à la sécurité ou toute perte d’intégrité ayant une incidence sur le service ou sur les données à caractère personnel conservées ;
- informer préalablement l’autorité nationale, dans un délai minimum de 2 mois, avant toute cessation d’activité, et informer les titulaires dans le même délai ;
- souscrire et maintenir une assurance couvrant sa responsabilité professionnelle au titre de l’activité de services de confiance ;
- traiter les réclamations selon la procédure publiée.

Le recours par le prestataire à un tiers pour l’exécution de tout ou partie du service ne modifie ni l’étendue de ses obligations ni sa responsabilité à l’égard du titulaire et de l’utilisateur de certificat.

4.2. Engagements de disponibilité

Le prestataire prend les engagements de disponibilité suivants sur les fonctions accessibles au titulaire et à l’utilisateur de certificat :

Engagements de disponibilité des fonctions publiques

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

Ces valeurs sont mesurées et vérifiées lors du contrôle de conformité annuel. Les opérations de maintenance ayant une incidence sur la disponibilité sont annoncées préalablement dans le registre de publication ; une intervention d’urgence justifiée par la sécurité du service peut être conduite sans préavis et est portée à la connaissance des titulaires dès que possible.

Le niveau de service applicable aux fonctions consommées par la plateforme pour le compte de l’utilisateur final est stipulé dans la convention conclue avec elle.

4.3. Obligations de la plateforme, autorité d’enregistrement

La plateforme, qui exerce les fonctions d’autorité d’enregistrement pour le compte du prestataire dans le cadre du contrat écrit préalable mentionné au chapitre 1, s’engage à :

- recueillir la demande, vérifier l’identité du demandeur et, le cas échéant, la qualité et les pouvoirs de son représentant ;
- constituer et transmettre le dossier d’enregistrement, et en conserver les preuves selon les modalités fixées par le contrat écrit qui la lie au prestataire ;
- refuser toute demande dont l’identité ou les pièces produites n’ont pu être vérifiées, et consigner le motif du refus ;
- ne traiter les données à caractère personnel que dans le cadre des instructions reçues du prestataire et de l’autorisation reçue de la personne concernée ;
- transmettre sans délai au prestataire toute demande de révocation et toute information susceptible d’en constituer une cause ;
- se soumettre aux contrôles que le prestataire exerce sur l’exécution de ses fonctions, dans les conditions prévues par le contrat.

Le prestataire demeure responsable des fonctions d’enregistrement ainsi exercées : la délégation transfère l’exécution, jamais la responsabilité. Les conditions commerciales conclues entre l’utilisateur final et la plateforme sont étrangères aux présentes conditions et ne peuvent y déroger.

4.4. Obligations du titulaire, personne morale

La personne morale titulaire du certificat de cachet électronique s’engage, par son représentant légal, à :

- fournir des informations exactes et complètes lors de l’enregistrement et signaler sans délai tout changement de l’une des informations portées dans le certificat, notamment de sa dénomination ou de son identifiant officiel ;
- prendre connaissance du certificat et l’accepter explicitement avant tout usage, et vérifier à cette occasion l’exactitude des informations qu’il porte ;
- protéger les moyens d’authentification de ses systèmes auprès de la plateforme, en restreindre l’usage aux personnes qu’elle habilite et tenir à jour la liste de ces habilitations ;
- n’utiliser le certificat que dans les limites d’usage énoncées au chapitre 2 et dans les limites de l’extension Key Usage qu’il porte ;
- n’apposer de cachet que sur des données dont elle est à l’origine ou dont elle assume l’émission ;
- demander la révocation du certificat sans délai dès la connaissance d’une cause de révocation, notamment en cas de compromission ou de suspicion de compromission ;
- cesser tout usage du certificat dès son expiration ou sa révocation ;
- respecter les présentes conditions et la politique de certification applicable.

Un cachet apposé au moyen du certificat est imputable à la personne morale titulaire, quelle que soit la personne physique qui a administré le système l’ayant appelé, sauf à établir qu’il résulte d’une compromission qu’elle avait signalée avant l’opération.

4.5. Obligations du représentant légal et des mandataires

Le représentant légal de la personne morale, et le cas échéant le mandataire qu’il désigne par écrit, s’engagent à :

- justifier de leur identité, de leur qualité et de l’étendue de leurs pouvoirs, et conserver les preuves de cette justification ;
- attester auprès de l’autorité d’enregistrement de l’exactitude des informations transmises au nom de la personne morale ;
- n’exercer les droits attachés au certificat que dans la limite des pouvoirs qui leur sont conférés ;
- informer sans délai le prestataire de tout changement de représentant légal, de toute modification et de toute cessation d’un mandat ;
- signaler sans délai toute cause de révocation dont ils ont connaissance ;
- restituer leurs attributions dès la fin de leur mandat.

4.6. Obligations de l’utilisateur de certificat

L’utilisateur de certificat est la personne ou l’entité qui reçoit un certificat et s’y fie. Avant de s’y fier, il lui appartient de :

1. construire la chaîne de certification jusqu’à un certificat d’autorité racine dont l’authenticité a été établie à partir du registre de publication ;
2. vérifier que la date de l’opération se situe dans la période de validité du certificat ;

3. vérifier l’état du certificat, soit auprès de la liste de révocation en vigueur, soit auprès du service d’information en ligne, une réponse dont la date de production est antérieure de plus de 24 heures à l’instant de la vérification n’étant pas exploitée ;
4. vérifier que l’usage effectif du certificat entre dans les limites d’usage déclarées et dans la valeur de l’extension Key Usage ;
5. vérifier l’identifiant de politique inscrit dans l’extension certificatePolicies, afin de connaître le niveau sous lequel le certificat a été délivré ;
6. vérifier la robustesse des algorithmes employés au regard de la durée pendant laquelle il entend se fier à l’opération.

Un utilisateur qui s’abstient de l’une de ces vérifications ne peut se prévaloir d’un préjudice qu’elle aurait permis d’éviter.

Ces vérifications sont publiques et gratuites : elles ne supposent ni compte, ni abonnement, ni logiciel fourni par le prestataire.

5. Cycle de vie du certificat

5.1. Durée de validité

La période de validité d’un certificat est de 1 an au niveau simple et de 3 ans au niveau avancé. 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’usage du certificat cesse à son expiration ou à sa révocation ; aucune opération n’est produite après l’un de ces deux évènements. Les opérations produites pendant la période de validité demeurent vérifiables au-delà de celle-ci, les éléments nécessaires à leur vérification étant conservés.

5.2. Renouvellement

Un certificat n’est jamais re-signé sur une bi-clé existante : le renouvellement s’entend de la délivrance d’un nouveau certificat sur une nouvelle bi-clé, générée dans le module cryptographique matériel. Cette règle borne la durée d’exposition d’une même clé privée à la durée de vie d’un seul certificat et n’impose au titulaire ni manipulation, ni support, ni coût supplémentaire au titre de la génération de la clé.

Une demande de renouvellement présentée avant l’expiration du certificat en cours de validité, et alors que celui-ci n’est ni révoqué ni expiré, est authentifiée par l’authentification forte du représentant légal, ou du mandataire habilité, dans l’espace de la personne morale sur la plateforme, au moyen des facteurs enrôlés lors de l’enregistrement. Un changement de représentant légal impose au préalable la mise à jour du dossier d’enregistrement et la vérification des pouvoirs du nouveau représentant.

En cas de changement de l’une des informations portées dans le certificat, la demande est traitée comme un premier enregistrement et le certificat en cours est révoqué pour inexactitude. Une re-vérification complète de l’identité est en tout état de cause conduite au moins une fois par période de 3 ans lorsque des renouvellements successifs se sont enchaînés sans nouvelle production de pièces.

Le titulaire est informé de l’échéance de son certificat suffisamment tôt pour que la continuité du service soit assurée ; les modalités pratiques figurent dans YT-GUIDE-USE.

5.3. Révocation

5.3.1. Causes de révocation

Un certificat est révoqué dans les cas suivants :

- compromission, suspicion de compromission, perte ou vol des données de création de signature ou de cachet du titulaire
- inexactitude ou changement d’une information portée dans le certificat
- cessation de la relation entre le titulaire et le prestataire, ou fin du mandat du représentant
- non-respect par le titulaire de ses obligations telles qu’elles résultent de la politique et des conditions générales d’utilisation
- compromission ou suspicion de compromission de la clé privée de l’autorité de certification émettrice

- décision de l’autorité nationale ou décision de justice
- cessation d’activité du prestataire sans reprise par un autre prestataire

La cessation ou la modification du mandat en vertu duquel la demande a été présentée est une cause de révocation lorsqu’elle prive le certificat de son fondement, notamment lorsque le représentant légal ou le mandataire perd les pouvoirs au vu desquels le certificat a été délivré et que la personne morale n’a pas désigné de remplaçant. Le changement de représentant légal n’emporte pas par lui-même révocation du certificat, qui est délivré à la personne morale et non à son représentant, dès lors que la mise à jour du dossier d’enregistrement est effectuée sans délai. La compromission d’un moyen d’authentification des systèmes de la personne morale devient une cause de révocation dès lors qu’elle laisse craindre qu’un cachet ait pu être apposé sans l’accord de celle-ci.

5.3.2. Qui peut demander la révocation

Sont habilités à demander la révocation d’un certificat de titulaire : le représentant légal de la personne morale ; le mandataire habilité par écrit ; une personne autorisée au sens des définitions du chapitre 1 ; l’autorité d’enregistrement ; le prestataire, agissant de sa propre initiative lorsqu’une cause énumérée ci-dessus est constatée ; l’autorité nationale ou une autorité judiciaire dans l’exercice de leurs attributions.

5.3.3. Comment et dans quel délai

Le titulaire, ou toute personne habilitée, formule sa demande de révocation sans délai, dès la connaissance de la cause de révocation. Un retard dans la formulation de la demande lui est opposable.

Les canaux de demande sont disponibles 24 heures sur 24, 7 jours sur 7 : l’espace du titulaire sur la plateforme, l’adresse électronique trust@yoryx.com et le courrier postal adressé au siège social. Le formulaire de demande de révocation est publié dans le registre sous l’identifiant YT-FORM-REVOCATION.

Une demande présentée par un canal ne permettant pas l’authentification immédiate est recevable lorsqu’elle émane manifestement d’une personne habilitée et que l’urgence le justifie ; elle est alors traitée sans délai et la vérification de l’origine est menée en parallèle, le doute profitant à la sécurité du titulaire.

Une demande de révocation valide est traitée dans un délai maximal de 24 heures à compter de sa réception, et l’information d’état correspondante est mise à disposition des utilisateurs de certificats dans un délai maximal de 24 heures. La liste de révocation est établie au moins toutes les 24 heures et immédiatement après toute révocation ; le service d’information en ligne est disponible 24 heures sur 24, 7 jours sur 7.

Une révocation est définitive et irréversible. Une demande présentée par erreur n’est pas annulée : un nouveau certificat est délivré selon la procédure de renouvellement. La révocation d’un certificat ne prive d’effet aucune opération produite avant la date de révocation.

La révocation est gratuite, quelle qu’en soit la cause.

5.4. Suspension

Sans objet : la suspension des certificats n’est pas proposée. Une demande motivée par une suspicion de compromission est traitée comme une demande de révocation.

Ce choix évite l’état intermédiaire « certificateHold », dont l’interprétation par les logiciels de vérification est inégale et qui peut être levé, alors que la révocation est définitive.

5.5. Fin de la relation

La relation prend fin à la demande de la personne morale, à l’expiration du dernier certificat sans renouvellement, en cas de dissolution ou de radiation de la personne morale, ou en cas de manquement grave non réparé trente jours après une mise en demeure restée sans effet.

La fin de la relation entraîne la révocation des certificats en cours de validité, la désactivation puis la destruction des données de création de cachet correspondantes, et la conservation du dossier de preuve pendant la durée fixée au chapitre relatif à la preuve et à l’archivage.

Elle n’efface pas les opérations déjà produites : les éléments permettant de les vérifier demeurent conservés, ce qui est la condition même de leur valeur probante.

6. Conditions financières

Les tarifs applicables aux services de confiance fournis par le prestataire figurent exclusivement dans YT-PRICING (OID 1.3.6.1.4.1.[PEN].1.7.1), publié dans le registre de publication. Aucun montant n’est énoncé dans les présentes conditions, afin qu’une évolution tarifaire n’emporte aucune modification des engagements qui y sont pris.

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.

Les unités de facturation sont libellées en dirham marocain (MAD) et s’entendent hors taxes ; la taxe sur la valeur ajoutée s’applique au taux en vigueur.

Les termes tarifaires du présent document s’appliquent à compter de leur publication dans le registre de publication et jusqu’à la publication d’une version postérieure. Toute modification est publiée dans les mêmes conditions et selon le préavis énoncé par les conditions générales d’utilisation applicables.

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.

Le prestataire ne perçoit aucun montant auprès de l’utilisateur final : une demande de remboursement présentée par celui-ci relève des conditions commerciales de la plateforme. Entre le prestataire et la plateforme, une prestation facturée qui n’a pas été fournie, ou qui l’a été en méconnaissance de la politique applicable, donne lieu à régularisation au titre de la convention de service. La révocation d’un certificat n’ouvre droit à aucun remboursement de la période de validité restant à courir, sauf lorsque la révocation est imputable au prestataire.

Les modalités de souscription, de facturation et de règlement applicables à l’utilisateur final relèvent de la plateforme et de la convention conclue avec elle. Un différend commercial avec la plateforme est sans effet sur les obligations de sécurité du prestataire, et notamment sur le traitement d’une demande de révocation.

Lorsqu’un certificat n’a pas été délivré conformément à la politique applicable, un certificat de remplacement est délivré sans frais ; à défaut de remplacement possible, la prestation est remboursée dans la limite de responsabilité énoncée au chapitre suivant.

7. Responsabilité, garanties et assurance

La responsabilité du prestataire au titre d’un certificat est plafonnée à [À COMPLÉTER — PLAFOND-RESPONSABILITE] par certificat 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.

Cette assurance est une condition de l’agrément posée par l’article 33 d) de la loi n° 43-20 ; le prestataire la souscrit indépendamment du calendrier de sa demande d’agrément, la couverture devant exister avant la première délivrance.

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

- l’usage d’un certificat en dehors des limites d’usage fixées par la politique applicable
- le défaut de vérification, par l’utilisateur du certificat, de l’état de révocation au moment de l’usage
- les conséquences d’une information inexacte fournie par le titulaire ou par son représentant
- les faits imputables à un tiers ou constitutifs d’un cas de force majeure

L’utilisateur d’un certificat vérifie, avant de s’y fier, la chaîne de certification, la période de validité, les limites d’usage et l’état de révocation du certificat.

Le prestataire ne garantit ni la valeur juridique qu’une autorité, une juridiction ou un tiers reconnaîtra à une opération produite au moyen d’un certificat autre que qualifié, ni l’acceptation de ce certificat par un service déterminé : la présomption de fiabilité est réservée par la loi n° 43-20 au niveau qualifié.

Aucune des parties ne répond de l’inexécution due à un cas de force majeure. La partie qui l’invoque en informe l’autre sans délai et met en œuvre les moyens raisonnables pour en limiter les effets.

8. Protection des données à caractère personnel

8.1. Cadre applicable et autorité compétente

Les traitements de données à caractère personnel réalisés à l’occasion des services 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).

La CNDP distingue la notification d’une déclaration et la demande d’autorisation préalable, ainsi que la demande de transfert à l’étranger. Ce régime est indépendant de celui de la loi n° 43-20 : un prestataire dépose auprès de la DGSSI au titre de la loi n° 43-20 et notifie séparément ses traitements à la CNDP au titre de la loi n° 09-08.

8.2. Données traitées et finalités

Les données traitées sont limitées à ce qui est nécessaire à la fourniture du service. Les données à caractère personnel se rapportent aux seules personnes physiques qui interviennent pour le compte de la personne morale : les prénom et nom du représentant légal ou du mandataire, les éléments de la pièce d’identité produite et le résultat de son contrôle, les pièces établissant leurs pouvoirs, leur adresse électronique de contact et les éléments de vérification des moyens d’authentification. Les données d’identification de la personne morale elle-même ne sont pas des données à caractère personnel.

Les finalités poursuivies sont la vérification de l’identité, la délivrance et la gestion des certificats, l’exécution des opérations couvertes par le certificat, la production des preuves exigées par la réglementation et le respect des obligations de conservation. Aucune donnée n’est traitée à des fins de prospection, de profilage ou de mesure d’audience, et aucune donnée n’est cédée à un tiers à des fins commerciales.

Le certificat lui-même ne porte que la dénomination de la personne morale, son identifiant officiel et le nom du cachet : ni le nom du représentant légal, ni celui d’un administrateur des systèmes n’y figurent. Les données cachetées ne sont pas transmises au prestataire : seule leur empreinte cryptographique l’est.

8.3. Engagements du prestataire

Le prestataire s’engage, au titre de la fourniture des services, 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

L’exigence 15 du référentiel [Ref_Serv_Conf_NonQual] subordonne au consentement de la personne concernée toute mise à disposition publique des données conservées ; les certificats de titulaires ne sont donc pas publiés et ne font l’objet d’aucun annuaire.

8.4. Durées de conservation

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.

La durée légale de conservation l’emporte sur une demande d’effacement pour les données qui composent une preuve : leur suppression priverait de valeur probante des opérations déjà produites. À l’issue de la période de conservation, les données archivées sont supprimées ou détruites de manière irréversible, et l’opération est journalisée.

8.5. Droits des personnes concernées

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.

Ces droits s’exercent auprès du point de contact indiqué au chapitre relatif aux réclamations, sur justification de l’identité du demandeur. Une réponse insatisfaisante ouvre la voie de la réclamation et, en dernier ressort, de la saisine de la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP).

> **Point ouvert —** 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.

9. Preuve, conservation et archivage

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.

Sont conservés, notamment : le dossier d’enregistrement et les preuves de la vérification d’identité, l’acceptation des présentes conditions, le certificat délivré et ses évènements de cycle de vie, les demandes de révocation et leur traitement, et les enregistrements d’évènements des composantes.

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

Une archive est restituée au titulaire, ou à toute personne qui en justifie l’intérêt, dans un délai maximal de 2 jours ouvrés. À l’issue de la période de conservation, les données archivées sont supprimées ou détruites de manière irréversible, et l’opération est journalisée.

Une convention de preuve définit la nature et la portée des preuves produites, leurs modalités d’établissement, de conservation, de mise à disposition et d’interprétation, ainsi que les engagements des parties sur leur acceptation.

La conservation assurée par le prestataire ne dispense pas la personne morale de la sienne : elle conserve les documents cachetés avec le cachet qui les accompagne, le certificat correspondant et la chaîne de certification, dont la fourniture par le prestataire est gratuite, ainsi que la trace interne des habilitations en vertu desquelles ses systèmes ont appelé le service.

Lorsque la conservation excède la période de fiabilité des algorithmes employés, il appartient au titulaire ou à l’utilisateur de certificat de renouveler la preuve, notamment par un horodatage portant sur l’ensemble constitué des données et de l’opération initiale.

Chaque partie tient confidentielles les informations techniques et opérationnelles portées à sa connaissance à l’occasion du service et qui ne sont pas publiées. Cette obligation survit à la fin de la relation pendant la durée de conservation des archives.

10. Modification, publication, réclamations et litiges

10.1. Modification des présentes conditions

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.

Une modification substantielle des présentes conditions est annoncée dans le registre de publication avant sa prise d’effet et notifiée au titulaire par le canal enregistré. Le titulaire qui n’accepte pas la nouvelle version peut demander la révocation de son certificat sans frais avant la date de prise d’effet ; la poursuite de l’usage du certificat après cette date vaut acceptation.

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

10.2. Publication

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.

Chaque document du registre est accessible par un chemin stable, formé de l’identifiant du document et de son numéro de version, de sorte qu’une référence faite dans un contrat, dans une décision de justice ou dans un dossier de preuve désigne durablement le même texte. Les versions antérieures demeurent accessibles sous leur propre chemin.

10.3. Cession

Le titulaire ne peut céder le bénéfice des présentes conditions ni transmettre son certificat à un tiers, le certificat étant attaché à l’identité qu’il porte. Le prestataire peut céder les siennes dans le cadre d’une transmission de son activité de services de confiance, à charge pour le cessionnaire de reprendre l’intégralité des engagements pris.

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 d’activité, le prestataire maintient, pendant la durée de conservation des archives, l’accès aux informations d’état nécessaires à la vérification des opérations produites, et restitue au titulaire, à sa demande, les éléments de preuve le concernant.

10.4. Réclamations, droit applicable et règlement des litiges

Toute réclamation relative aux services couverts par les présentes conditions 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). La CNDP est l’autorité compétente en matière de protection des données à caractère personnel au titre de la loi n° 09-08.

La saisine du prestataire n’est pas un préalable obligatoire à la saisine d’une autorité ou d’une juridiction, et l’exercice d’une voie de recours n’interrompt pas le traitement de la réclamation.

Les présentes conditions sont régies par le droit marocain. À défaut de règlement amiable, les litiges relèvent des tribunaux compétents de Marrakech.

Les présentes conditions sont conclues entre professionnels ; la personne morale titulaire déclare agir dans le cadre de son activité et disposer des compétences techniques nécessaires à l’intégration du service dans ses systèmes.

11. Références

11.1. 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 15	le cachet électronique qualifié est un cachet avancé produit par un dispositif qualifié de création de cachet (article 17) et reposant sur un certificat qualifié de cachet (article 18)
Article 30	l’authentification d’un site internet repose sur un certificat qualifié d’authentification, qui ne peut être délivré que par un prestataire agréé
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	Objet
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 63	sanction de la fourniture d’un service de confiance autre que qualifié sans la déclaration de l’article 35 : 50.000 à 100.000 dirhams d’amende

[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 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 20	sont des moyens d’identification électronique la carte nationale d’identité électronique régie par la loi n° 04-20 et tout autre document électronique permettant, conformément au texte qui l’institue, de prouver l’identité à distance de son titulaire et répondant aux spécifications techniques minimales fixées par l’autorité nationale
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.

11.2. 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.

11.3. 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 319 411-1] 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 EN 319 142-1] ETSI EN 319 142-1 — PAdES digital signatures — Part 1: Building blocks and PAdES baseline signatures.

[ETSI EN 319 132-1] ETSI EN 319 132-1 — XAdES digital signatures — Part 1: Building blocks and XAdES baseline signatures.

[ETSI EN 319 122-1] ETSI EN 319 122-1 — CAdES digital signatures — Part 1: Building blocks and CAdES baseline signatures.

[ETSI EN 319 162-1] ETSI EN 319 162-1 — Associated Signature Containers (ASiC) — Part 1: Building blocks and ASiC baseline containers.

[CEN EN 419 241-1] CEN EN 419 241-1 — Trustworthy Systems Supporting Server Signing — Part 1: General System Security Requirements.

[CEN EN 419 241-2] CEN EN 419 241-2 — Trustworthy Systems Supporting Server Signing — Part 2: Protection Profile for QSCD for Server Signing.

[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.

11.4. Documents du registre de publication cités

YT-PC-SEAL (OID 1.3.6.1.4.1.[PEN].1.1.2) — politique de certification applicable.

YT-DPC (OID 1.3.6.1.4.1.[PEN].1.2) — déclaration des pratiques de certification.

YT-PDS-CERT (OID 1.3.6.1.4.1.[PEN].1.3.1) — déclaration de divulgation PKI pour les services de certificats.

YT-FORM-LEGAL-REP (OID 1.3.6.1.4.1.[PEN].1.5.2) — formulaire d’enregistrement.

YT-FORM-REVOCATION (OID 1.3.6.1.4.1.[PEN].1.5.3) — formulaire de demande de révocation.

YT-FORM-MANDATE (OID 1.3.6.1.4.1.[PEN].1.5.4) — mandat et autorisation de retrait.

YT-PRICING (OID 1.3.6.1.4.1.[PEN].1.7.1) — termes tarifaires des services de confiance.

YT-COMPLAINTS (OID 1.3.6.1.4.1.[PEN].1.7.2) — procédure de réclamation.

YT-GUIDE-ENROLMENT — guide d’inscription et de demande en ligne.

YT-GUIDE-IDENTITY — guide de contrôle d’identité.

YT-GUIDE-USE — guide d’installation et d’utilisation.

Les guides ci-dessus sont cités par leur seul identifiant : ils n’ont pas de valeur contractuelle et ne créent aucune obligation.