YORYX® TRUST SASU

Guide d’installation et d’utilisation

YT-GUIDE-USE

OID : 1.3.6.1.4.1.[PEN].1.6.3

Version 0.1

5 septembre 2026

Projet — en préparation de la déclaration préalable

Diffusion publique

Identification du document

Champ	Valeur
Titre du document	Guide d’installation et d’utilisation
Identifiant du document	YT-GUIDE-USE
Identifiant d'objet (OID)	1.3.6.1.4.1.[PEN].1.6.3
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. Ce que vous n’avez pas à installer....4
   1.1. Identification du prestataire et du guide....4
   1.2. Statut réglementaire....5
   1.3. Portée de ce guide....5
   1.4. À qui s’adresse chaque chapitre....5
2. Signer, en tant que personne physique....6
   2.1. Le principe : le contrôle exclusif....6
   2.2. Autoriser une signature....6
   2.3. Les formats de signature....6
   2.4. Les limites d’usage....7
3. Apposer un cachet, en tant que personne morale....8
4. Vérifier une signature, un cachet ou un jeton....9
5. Pour les utilisateurs de certificats : reconnaître les autorités....10
   5.1. La procédure, une fois les certificats publiés....10
6. Échéance, renouvellement et révocation....12
   6.1. Échéance et renouvellement....12
   6.2. Révocation....12
7. Documents applicables, assistance et réclamations....13
   7.1. Le registre de publication....13
   7.2. Assistance et réclamations....13

1. Ce que vous n’avez pas à installer

Ce guide porte un titre hérité des services de certification traditionnels, où le titulaire recevait un support matériel et devait le faire reconnaître par son poste de travail. Dans le modèle décrit ici, cette étape n’existe plus : si vous êtes signataire, vous n’avez rien à installer.

Le signataire n’achète aucun matériel, n’installe aucun logiciel et signe depuis son téléphone ou son navigateur.

Le signataire n’a ni clé USB, ni carte à puce, ni lecteur à se procurer, et rien à installer sur son poste : le support physique est remplacé par le module cryptographique matériel exploité par YORYX TRUST.

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.

Vous n’avez donc rien à acheter, rien à recevoir par courrier et rien à retirer à un guichet. Aucun pilote, aucune extension de navigateur et aucun programme ne vous sont demandés : vous utilisez l’application de la plateforme sur votre téléphone, ou une session de navigateur à jour.

La seule installation dont traite ce guide est celle des certificats des autorités de certification, effectuée par une partie qui reçoit un document signé et souhaite le vérifier au moyen de son propre logiciel. Elle fait l’objet du chapitre 5, et elle ne concerne pas le signataire.

1.1. Identification du prestataire et du guide

Identification du prestataire et du présent guide

Élément	Valeur
Prestataire de services de confiance	YORYX TRUST SASU, société par actions simplifiée à associé unique (SASU)
Immatriculation	RC Marrakech n° 184667 — ICE 004013324000019
Siège social	57, rue Mauritania, BP 2609, Guéliz, 40000 Marrakech, Maroc
Adresse électronique	trust@yoryx.com
Guide	YT-GUIDE-USE — Guide d’installation et d’utilisation
Identifiant d’objet du guide	1.3.6.1.4.1.[PEN].1.6.3
Version et date	0.1 — 2026-09-05
Diffusion	Diffusion publique

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

1.2. 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 ; son article 32 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.

Le présent guide décrit donc un parcours cible : il vous explique comment le service fonctionnera, afin que vous puissiez l’examiner avant son ouverture. Aucun service n’est ouvert à ce jour et aucun certificat n’est délivré.

1.3. Portée de ce guide

> **Ce guide explique, il n’engage pas —** Le présent guide est un document d’explication. Il ne crée aucun droit ni aucune obligation. En cas de divergence, la politique de certification applicable, la déclaration des pratiques et les conditions générales d’utilisation prévalent sur lui ; leurs références figurent au dernier chapitre.

1.4. À qui s’adresse chaque chapitre

Plan du guide

Chapitre	Lecteur concerné	Objet
2	Le signataire, personne physique	Signer depuis son téléphone ou son navigateur.
3	La personne morale titulaire d’un cachet	Apposer un cachet par ses systèmes, à travers la plateforme.
4	Le destinataire d’un document	Vérifier une signature, un cachet ou un jeton, sans compte.
5	L’utilisateur de certificat outillé	Reconnaître les autorités de certification dans son propre logiciel.
6	Tout titulaire	Échéance, renouvellement, révocation.
7	Tout lecteur	Documents applicables, assistance et réclamations.

2. Signer, en tant que personne physique

2.1. Le principe : le contrôle exclusif

Les données de création de signature du signataire 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.

Chaque signature est autorisée par une action que le signataire seul peut accomplir, depuis l’application sur son téléphone ou depuis une session de navigateur, après une authentification forte ; sans cette action, le module ne produit aucune signature. L’authentification forte n’est pas un simple accès au service : elle est un composant du service de signature lui-même et matérialise le contrôle exclusif.

Retenez le point qui compte : la clé est gardée par le prestataire, mais elle n’est actionnée que par vous, pour un document précis et à un instant précis. Sans votre action, le module cryptographique matériel ne produit aucune signature.

2.2. Autoriser une signature

1. Vous recevez, dans votre espace ou par un message, une demande de signature portant sur un document précis.
2. Ouvrez le document et prenez-en connaissance. N’autorisez jamais une signature sans avoir lu ce que vous signez : c’est un engagement que vous prenez au titre des conditions générales d’utilisation.
3. Vérifiez le résumé présenté avant l’autorisation : le nom du document, son empreinte, et le certificat qui sera utilisé.
4. Authentifiez-vous fortement, au moyen d’au moins deux facteurs de natures différentes, puis autorisez l’opération.
5. La signature est produite à l’intérieur du module cryptographique matériel, puis le document signé vous est restitué.
6. Conservez le document signé tel qu’il vous est restitué. Une modification, même apparemment anodine, invalide la signature : ne le ré-enregistrez pas dans un autre format.

L’utilisation des données de création de signature du titulaire est subordonnée à une authentification forte multifacteur mettant en œuvre au moins deux facteurs d’authentification, propre à chaque opération de signature.

> **Si vous perdez votre téléphone —** Perdre son téléphone ne fait perdre aucune donnée de création de signature : cela révoque un moyen d’authentification, que le signataire réenrôle. Prévenez sans délai l’autorité d’enregistrement, puis réenrôlez vos facteurs. Si vous craignez qu’une signature ait pu être produite sans votre accord, demandez immédiatement la révocation de votre certificat, selon le chapitre 6.

2.3. Les formats de signature

Les signatures sont produites dans les formats normalisés suivants, selon la nature du document :

- PAdES (ETSI EN 319 142-1)

- XAdES (ETSI EN 319 132-1)
- CAdES (ETSI EN 319 122-1)

Plusieurs documents peuvent être réunis dans un conteneur normalisé ASiC (ETSI EN 319 162-1), qui conserve ensemble les fichiers et leurs signatures. Les suites cryptographiques mises en œuvre sont conformes à la norme ETSI TS 119 312 (version 1.4.2 ou ultérieure).

2.4. Les limites d’usage

Votre certificat sert exclusivement à signer. Il ne sert ni au chiffrement, ni à l’authentification d’un serveur, ni à la signature de code, ni à l’authentification d’un site internet au sens de l’article 30 de la loi n° 43-20. Le détail figure au chapitre 1.10.1.1 de YT-PC-SIGN (OID 1.3.6.1.4.1.[PEN].1.1.1).

3. Apposer un cachet, en tant que personne morale

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.

Il n’y a donc, là encore, aucun support remis à une personne physique et aucun programme fourni par le prestataire. Vos systèmes s’adressent à la plateforme, qui sollicite le service de cachet du prestataire.

1. Le représentant légal, ou la fonction mandataire désignée dans YT-FORM-MANDATE (OID 1.3.6.1.4.1.[PEN].1.5.4), prend en possession le certificat dans l’espace de la personne morale et l’accepte explicitement.
2. Il enrôle les moyens d’authentification par lesquels vos systèmes accéderont au service : ils constituent les données d’activation du cachet.
3. Il désigne, au sein de la personne morale, les personnes habilitées à mettre en œuvre le cachet, et tient cette liste à jour.
4. Vos systèmes transmettent à la plateforme les données à cacheter, et reçoivent en retour le document ou le flux cacheté.
5. Chaque opération est journalisée. Conservez ces journaux : ils sont votre preuve interne de l’origine d’un cachet.

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.

Le cachet engage la personne morale, non la personne qui l’administre : n’apposez de cachet que sur des données dont votre organisation est à l’origine ou dont elle assume l’émission. Le cachet ne remplace pas la signature d’une personne physique lorsque celle-ci est requise.

Si un moyen d’authentification de vos systèmes est compromis, révoquez ce moyen et réenrôlez-le : les données de création de cachet demeurent dans le module cryptographique matériel. Demandez en revanche la révocation du certificat dès lors que vous craignez qu’un cachet ait pu être apposé sans l’accord de la personne morale. Le détail figure au chapitre 3.9 de YT-PC-SEAL (OID 1.3.6.1.4.1.[PEN].1.1.2).

4. Vérifier une signature, un cachet ou un jeton

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.

Le service de vérification publique vous indique qui a signé, quand, sous quelle politique, et si le document a été modifié depuis. Il ne vous demande ni compte, ni abonnement, ni programme : vous déposez le document et vous lisez le résultat.

1. Déposez le document signé, ou le conteneur qui réunit les fichiers et leurs signatures.
2. Lisez l’identité du signataire ou la dénomination de la personne morale, telle qu’elle figure dans le certificat.
3. Lisez le niveau sous lequel le certificat a été délivré : il est porté par l’identifiant de politique inscrit dans l’extension certificatePolicies.
4. Vérifiez que la date de l’opération se situe dans la période de validité du certificat, et que celui-ci n’était pas révoqué à cette date.
5. Vérifiez que l’usage relevé entre bien dans les domaines d’utilisation déclarés par la politique applicable.
6. Conservez le résultat de la vérification avec le document : il fait partie de votre dossier de preuve.

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.

Un utilisateur qui s’abstient de l’une de ces vérifications ne peut se prévaloir d’un préjudice qu’elle aurait permis d’éviter. La vérification publique est sans frais, comme l’accès aux listes de révocation et au service d’information sur l’état des certificats.

Pour un jeton d’horodatage, la démarche est la même et la politique applicable est YT-PH-TSA (OID 1.3.6.1.4.1.[PEN].1.1.3). 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.

5. Pour les utilisateurs de certificats : reconnaître les autorités

Ce chapitre s’adresse aux parties qui vérifient les signatures au moyen de leur propre logiciel plutôt que par le service de vérification publique : une administration, une entreprise, un service applicatif. Il ne concerne ni le signataire, ni la personne morale titulaire d’un cachet.

Pour qu’un logiciel accepte une signature, il doit pouvoir construire la chaîne de certification jusqu’à une autorité racine dont il tient l’authenticité pour établie. Cela suppose d’ajouter les certificats des autorités de certification du prestataire à son magasin de confiance.

L’architecture de certification à reconnaître

Niveau	Rôle	Durée de validité
YORYX TRUST Root CA G1	autorité de certification racine, maintenue hors ligne	10 ans
YORYX TRUST Signature CA G1	autorité de certification émettrice des certificats de signature électronique	6 ans
YORYX TRUST Seal CA G1	autorité de certification émettrice des certificats de cachet électronique	6 ans
YORYX TRUST Timestamping CA G1	autorité de certification émettrice des certificats des unités d’horodatage	6 ans

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

5.1. La procédure, une fois les certificats publiés

> **Publication à venir —** Les certificats des autorités de certification figurent parmi les éléments que le registre de publication du site institutionnel de YORYX TRUST a vocation à publier. Ils n’y sont pas encore, aucun certificat n’étant délivré à ce jour. La procédure ci-dessous décrit la marche à suivre lorsqu’ils y seront ; elle est publiée à l’avance pour que les parties qui devront l’appliquer puissent l’examiner.

1. Depuis le registre de publication, téléchargez le certificat de l’autorité racine et celui de l’autorité émettrice concernée par le certificat que vous vérifiez.
2. Vérifiez l’empreinte du certificat racine avant toute installation, en la comparant à celle que le registre publie : c’est la seule étape qui vous protège d’un certificat substitué, et elle ne doit jamais être omise.
3. Installez le certificat racine dans le magasin des autorités de confiance de votre logiciel de vérification, et le certificat de l’autorité émettrice dans le magasin des autorités intermédiaires.
4. Configurez la vérification de l’état de révocation : votre logiciel doit interroger le service d’information en ligne, ou obtenir une liste de révocation à jour, avant d’accepter une signature.
5. Vérifiez que votre logiciel n’exploite pas une liste de révocation dont la date de prochaine mise à jour est dépassée : une telle liste n’est pas une vérification.

6. Renouvelez cette opération lorsqu’une nouvelle génération de clé est publiée ; le suffixe de génération du nom de l’autorité vous l’indique.

Cadence de l’information sur l’état des certificats

Élément	Valeur
Établissement de la liste de révocation	24 heures
Champ nextUpdate de la liste	72 heures
Publication après génération	Chaque liste de révocation est publiée dans les 30 minutes suivant sa génération et reste accessible sans contrôle d’accès ni frais.
Service d’information en ligne	IETF RFC 6960 — 24 heures sur 24, 7 jours sur 7
Fraîcheur maximale admise d’une réponse en ligne	24 heures
Listes de révocation delta	non mise en œuvre

N’installez jamais un certificat d’autorité obtenu autrement que par le registre de publication, et ne l’acceptez pas d’un correspondant qui vous l’adresserait avec un document : un magasin de confiance est le point unique par lequel une signature frauduleuse peut devenir crédible.

6. Échéance, renouvellement et révocation

6.1. Échéance et renouvellement

Durées de validité des certificats de titulaires

Certificat	Durée de validité
Signature électronique — niveau simple	1 an
Signature électronique — niveau avancé	3 ans
Cachet électronique — niveau simple	1 an
Cachet électronique — niveau avancé	3 ans

Vous êtes prévenu de l’échéance suffisamment tôt pour que la continuité de votre service soit assurée. Le renouvellement donne lieu à une nouvelle bi-clé, générée dans le module cryptographique matériel : un certificat n’est jamais re-signé sur une clé existante. Vous n’avez ni support à remplacer, ni programme à mettre à jour.

Une signature produite pendant la période de validité du certificat demeure vérifiable après l’expiration de celui-ci : les éléments de vérification sont conservés pendant 7 ans. Pour une conservation longue, horodatez vos documents signés et renouvelez la preuve lorsque la durée excède la période de fiabilité des algorithmes employés.

6.2. Révocation

Demandez la révocation sans délai, dès la connaissance de la cause de révocation. Les canaux sont disponibles 24 heures sur 24, 7 jours sur 7 ; une demande valide est traitée dans un délai maximal de 24 heures, et l’information d’état est publiée dans un délai maximal de 24 heures. La révocation est sans frais.

Demandez-la notamment 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

Le formulaire est YT-FORM-REVOCATION (OID 1.3.6.1.4.1.[PEN].1.5.3). La révocation est définitive et irréversible : un certificat révoqué n’est jamais rétabli, et l’obtention d’un nouveau certificat suppose une nouvelle demande. 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.

7. Documents applicables, assistance et réclamations

7.1. Le registre de publication

Les documents ci-dessous sont publiés dans le registre de publication du site institutionnel de YORYX TRUST, 24 heures sur 24, 7 jours sur 7, sans contrôle d’accès ni frais. Vous pouvez les consulter avant de vous engager, et vous êtes invité à le faire.

- YT-PC-SIGN (OID 1.3.6.1.4.1.[PEN].1.1.1)
- YT-PC-SEAL (OID 1.3.6.1.4.1.[PEN].1.1.2)
- YT-PH-TSA (OID 1.3.6.1.4.1.[PEN].1.1.3)
- YT-DPC (OID 1.3.6.1.4.1.[PEN].1.2)
- YT-CGU-PP (OID 1.3.6.1.4.1.[PEN].1.4.1)
- YT-CGU-PM (OID 1.3.6.1.4.1.[PEN].1.4.2)
- YT-CGU-TSA (OID 1.3.6.1.4.1.[PEN].1.4.3)
- YT-PDS-CERT (OID 1.3.6.1.4.1.[PEN].1.3.1)
- YT-PDS-TSA (OID 1.3.6.1.4.1.[PEN].1.3.2)
- YT-FORM-REVOCATION (OID 1.3.6.1.4.1.[PEN].1.5.3)
- YT-FORM-MANDATE (OID 1.3.6.1.4.1.[PEN].1.5.4)
- YT-GUIDE-ENROLMENT (OID 1.3.6.1.4.1.[PEN].1.6.1)
- YT-GUIDE-IDENTITY (OID 1.3.6.1.4.1.[PEN].1.6.2)
- YT-PRICING (OID 1.3.6.1.4.1.[PEN].1.7.1)
- YT-COMPLAINTS (OID 1.3.6.1.4.1.[PEN].1.7.2)

Une nouvelle version d’un document y est publiée au plus tard le jour de sa prise d’effet. 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.

7.2. Assistance et réclamations

Pour une question sur votre demande, écrivez à trust@yoryx.com ou adressez un courrier au siège social indiqué au premier chapitre. Ces deux voies sont celles du prestataire ; pour une question commerciale, adressez-vous à la plateforme, qui est votre interlocuteur contractuel.

Si la réponse ne vous satisfait pas, vous pouvez déposer une réclamation. Sa réception vous est accusée dans un délai de 5 jours ouvrés et une réponse motivée vous est apportée dans un délai de 30 jours calendaires. La procédure complète, y compris l’escalade et les recours, figure dans YT-COMPLAINTS (OID 1.3.6.1.4.1.[PEN].1.7.2). Le traitement d’une réclamation est sans frais.

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.