YORYX® TRUST SASU

Politique de certification – cachet électronique

YT-PC-SEAL

OID : 1.3.6.1.4.1.[PEN].1.1.2

Version 0.1

5 septembre 2026

Projet — en préparation de la déclaration préalable

Diffusion publique

Identification du document

Champ	Valeur
Titre du document	Politique de certification – cachet électronique
Identifiant du document	YT-PC-SEAL
Identifiant d'objet (OID)	1.3.6.1.4.1.[PEN].1.1.2
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. INTRODUCTION....10
1.1. Présentation générale....10
1.2. Acronymes et Définitions....11
1.2.1. Acronymes....11
1.2.2. Terminologie....12
1.3. Niveaux de sécurité....13
1.4. PSCE et niveau de sécurité....14
1.5. Cachet électronique sécurisé et certificat sécurisé....15
1.6. Identification du document....16
1.7. Fonctionnalités minimales couvertes par une IGC....16
1.8. Interactions avec l'IGC....17
1.9. Responsabilités....17
1.9.1. De l'autorité de certification du prestataire....18
1.9.2. De l'autorité d'enregistrement du prestataire....19
1.9.3. Du titulaire du certificat....19
1.9.4. Du mandataire de certification....19
1.10. Usage des certificats....20
1.10.1. Domaines d'utilisation applicables....20
1.10.1.1. Bi-clés et certificats des titulaires....20
1.10.1.2. Bi-clés et certificats d'autorité et de composantes....20
1.11. Gestion de la PC....21
1.11.1. Entité gérant la PC....21
1.11.2. Point de contact....21
1.11.3. Entité déterminant la conformité d'une DPC avec cette PC....21
1.11.4. Procédures d'approbation de la conformité de la DPC....21
2. IDENTIFICATION ET AUTHENTIFICATION....23
2.1. Nommage....23
2.1.1. Types de noms....23
2.1.2. Nécessité d'utilisation de noms explicites....23
2.1.3. Unicité des noms....23
2.1.4. Identification, authentification et rôle des marques déposées....24
2.2. Validation initiale de l'identité....24
2.2.1. Méthode pour prouver la possession de la clé privée....24
2.2.2. Enregistrement d'un titulaire....24

2.2.3. Informations non vérifiées du titulaire....25
2.2.4. Validation de l'autorité du demandeur....25
2.2.5. Critères d'interopérabilité....25
2.3. Identification et validation d'une demande de renouvellement des clés....26
2.3.1. Identification et validation pour un renouvellement courant....26
2.3.2. Identification et validation pour un renouvellement après révocation....26
2.3.3. Identification et validation d'une demande de révocation....26
3. EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS....27
3.1. Demande de certificat....27
3.1.1. Origine d'une demande de certificat....27
3.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat....27
3.2. Traitement d'une demande de certificat....27
3.2.1. Exécution des processus d'identification et de validation de la demande....27
3.2.2. Acceptation ou rejet de la demande....27
3.2.3. Durée d'établissement du certificat....28
3.3. Délivrance du certificat....28
3.3.1. Actions de l'AC concernant la délivrance du certificat....28
3.3.2. Notification par l'AC de la délivrance du certificat au porteur....28
3.4. Acceptation du certificat....28
3.4.1. Démarche d'acceptation du certificat....28
3.4.2. Publication du certificat....29
3.4.3. Notification par l'AC aux autres entités de la délivrance du certificat....29
3.5. Usages de la bi-clé et du certificat....29
3.5.1. Utilisation de la clé privée et du certificat par le porteur....29
3.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat....29
3.6. Renouvellement d'un certificat....30
3.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé....30
3.7.1. Causes possibles de changement d'une bi-clé....30
3.7.2. Origine d'une demande d'un nouveau certificat....30
3.7.3. Procédure de traitement d'une demande d'un nouveau certificat....30
3.7.4. Notification au porteur de l'établissement du nouveau certificat....30
3.7.5. Démarche d'acceptation du nouveau certificat....30
3.7.6. Publication du nouveau certificat....31
3.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat....31
3.8. Modification du certificat....31

3.9. Révocation et suspension des certificats....31
3.9.1. Causes possibles d'une révocation....31
3.9.1.1. Certificats de titulaires....31
3.9.1.2. Certificats d'une composante de l'IGC....31
3.9.2. Origine d'une demande de révocation....32
3.9.2.1. Certificats de titulaires....32
3.9.2.2. Certificats d'une composante de l'IGC....32
3.9.3. Procédure de traitement d'une demande de révocation....32
3.9.3.1. Révocation d'un certificat de titulaire....32
3.9.3.2. Révocation d'un certificat d'une composante de l'IGC....32
3.9.4. Délai accordé au porteur pour formuler la demande de révocation....33
3.9.5. Délai de traitement par l'AC d'une demande de révocation....33
3.9.5.1. Révocation d'un certificat de titulaire....33
3.9.5.2. Révocation d'un certificat d'une composante de l'IGC....33
3.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats....33
3.9.7. Fréquence d'établissement des LCR....33
3.9.8. Délai maximum de publication d'une LCR....33
3.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats....33
3.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats....34
3.9.11. Autres moyens disponibles d'information sur les révocations....34
3.9.12. Exigences spécifiques en cas de compromission de la clé privée....34
3.9.13. Causes possibles d'une suspension....34
3.9.14. Origine d'une demande de suspension....34
3.9.15. Procédure de traitement d'une demande de suspension....34
3.9.16. Limites de la période de suspension d'un certificat....34
3.10. Fonction d'information sur l'état des certificats....34
3.10.1. Caractéristiques opérationnelles....34
3.10.2. Disponibilité de la fonction....35
3.10.3. Dispositifs optionnels....35
3.11. Fin de la relation entre le porteur et l'AC....35
3.12. Séquestre de clé et recouvrement....35
3.12.1. Politique et pratiques de recouvrement par séquestre des clés....35
3.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session....36
4. MESURES DE SÉCURITÉ NON TECHNIQUES....37

4.1. Mesures de sécurité physique....37
4.1.1. Situation géographique et construction des sites....37
4.1.2. Accès physique....37
4.1.3. Alimentation électrique et climatisation....37
4.1.4. Vulnérabilité aux dégâts des eaux....37
4.1.5. Prévention et protection incendie....38
4.1.6. Conservation des supports....38
4.1.7. Mise hors service des supports....38
4.1.8. Sauvegardes hors site....38
4.2. Mesures de sécurité procédurales....38
4.2.1. Rôles de confiance....38
4.2.2. Nombre de personnes requises par tâches....39
4.2.3. Identification et authentification pour chaque rôle....40
4.2.4. Rôles exigeant une séparation des attributions....40
4.3. Mesures de sécurité vis-à-vis du personnel....40
4.3.1. Qualifications, compétences et habilitations requises....40
4.3.2. Procédures de vérification des antécédents....40
4.3.3. Exigences en matière de formation initiale....40
4.3.4. Exigences et fréquence en matière de formation continue....40
4.3.5. Fréquence et séquence de rotation entre différentes attributions....41
4.3.6. Sanctions en cas d'actions non autorisées....41
4.3.7. Exigences vis-à-vis du personnel des prestataires externes....41
4.3.8. Documentation fournie au personnel....41
4.4. Procédures de constitution des données d'audit....41
4.4.1. Type d'évènements à enregistrer....41
4.4.2. Fréquence de traitement des journaux d'évènements....42
4.4.3. Période de conservation des journaux d'évènements....42
4.4.4. Protection des journaux d'évènements....42
4.4.5. Procédure de sauvegarde des journaux d'évènements....42
4.4.6. Système de collecte des journaux d'évènements....43
4.4.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement....43
4.4.8. Évaluation des vulnérabilités....43
4.5. Archivage des données....43
4.5.1. Types de données à archiver....43
4.5.2. Période de conservation des archives....43

4.5.3. Protection des archives....44
4.5.4. Procédure de sauvegarde des archives....44
4.5.5. Exigences d'horodatage des données....44
4.5.6. Système de collecte des archives....44
4.5.7. Procédures de récupération et de vérification des archives....44
4.6. Changement de clé d'AC....44
4.7. Reprise suite à compromission et sinistre....45
4.7.1. Procédures de remontée et de traitement des incidents et des compromissions....45
4.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)....45
4.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante 45
4.7.4. Capacités de continuité d'activité suite à un sinistre....45
4.8. Fin de vie de l'IGC....46
5. MESURES DE SÉCURITÉ TECHNIQUES....47
5.1. Génération et installation de bi-clés....47
5.1.1. Génération des bi-clés....47
5.1.1.1. Clés d'AC....47
5.1.1.2. Clés porteurs générées par l'AC....47
5.1.1.3. Clés porteurs générées par le porteur....47
5.1.1.4. Transmission de la clé privée à son propriétaire....47
5.1.2. Transmission de la clé publique à l'AC....48
5.1.3. Transmission de la clé publique de l'AC aux utilisateurs de certificats....48
5.1.4. Tailles des clés....48
5.1.5. Vérification de la génération des paramètres des bi-clés et de leur qualité....48
5.1.6. Objectifs d'usage de la clé....49
5.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques....49
5.2.1. Standards et mesures de sécurité pour les modules cryptographiques....49
5.2.1.1. Modules cryptographiques de l'AC....49
5.2.1.2. Dispositifs de création de cachet des titulaires....50
5.2.2. Contrôle de la clé privée par plusieurs personnes....50
5.2.3. Séquestre de la clé privée....50
5.2.4. Copie de secours de la clé privée....50
5.2.5. Archivage de la clé privée....50
5.2.6. Transfert de la clé privée vers/depuis le module cryptographique....50

5.2.7. Stockage de la clé privée dans un module cryptographique....50
5.2.8. Méthode d'activation de la clé privée....51
5.2.8.1. Clés privées d'AC....51
5.2.8.2. Clés privées des porteurs....51
5.2.9. Méthode de désactivation de la clé privée....51
5.2.9.1. Clés privées d'AC....51
5.2.9.2. Clés privées des porteurs....51
5.2.10. Méthode de destruction des clés privées....51
5.2.10.1. Clés privées d'AC....51
5.2.10.2. Clés privées des porteurs....51
5.2.11. Niveau d'évaluation sécurité du module cryptographique....51
5.3. Autres aspects de la gestion des bi-clés....52
5.3.1. Archivage des clés publiques....52
5.3.2. Durées de vie des bi-clés et des certificats....52
5.4. Données d'activation....52
5.4.1. Génération et installation des données d'activation....52
5.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC....52
5.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du porteur....52
5.4.2. Protection des données d'activation....53
5.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC....53
5.4.2.2. Protection des données d'activation correspondant aux clés privées des porteurs....53
5.4.3. Autres aspects liés aux données d'activation....53
5.5. Mesures de sécurité des systèmes informatiques....53
5.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques....53
5.5.2. Niveau d'évaluation sécurité des systèmes informatiques....54
5.6. Mesures de sécurité liées au développement des systèmes....54
5.7. Mesures de sécurité réseau....54
5.8. Horodatage / Système de datation....54
6. PROFIL DES CERTIFICATS ET DES LCR....55
6.1. Profil des certificats....55
6.2. Profil des LCR....56
7. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS....57
7.1. Fréquences et/ou circonstances des évaluations....57

7.2. Identités des auditeurs....57
7.3. Relations entre auditeur et entités évaluées....57
7.4. Sujets couverts par les évaluations....58
7.5. Actions prises suite aux conclusions des évaluations....58
7.6. Communication des résultats....58
8. AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES....59
8.1. Durée et fin anticipée de validité de la PC....59
8.1.1. Durée de validité....59
8.1.2. Fin anticipée de validité....59
9. ANNEXES....61
9.1. Exigences de sécurité....61
9.1.1. Exigences sur les objectifs de sécurité du module cryptographique....61
9.1.2. Exigences sur les objectifs de sécurité du dispositif de création de cachet....61
9.2. Variable de temps et niveaux de sécurité....62
9.3. Détails sur le gabarit d'un certificat racine....64
9.4. Détails sur le gabarit d'un certificat porteur....65
9.5. Algorithmes de signature et taille de clés des AC....67
9.6. Algorithmes et longueurs de clés des porteurs....67
9.7. Documents de références....68
9.8. Plan type détaillé d'une politique d'horodatage....70

1. INTRODUCTION

1.1. Présentation générale

La présente politique de certification (PC) définit les exigences que YORYX TRUST SASU, prestataire de services de confiance, s'impose et impose à ses composantes pour la délivrance et la gestion des certificats de cachet électronique. Elle décrit ce qui est fait ; la déclaration des pratiques de certification (YT-DPC) décrit comment cela est fait.

Elle s'applique à l'ensemble du cycle de vie des certificats de cachet électronique délivrés par l'autorité de certification émettrice YORYX TRUST Seal CA G1 : demande, vérification de l'identité, génération, délivrance, acceptation, usage, renouvellement, révocation et fin de vie, ainsi qu'aux données de création de cachet correspondantes.

YORYX TRUST SASU est une société par actions simplifiée à associé unique (SASU), immatriculée sous le RC Marrakech n° 184667 tenu par le tribunal de commerce de Marrakech, identifiant commun de l'entreprise 004013324000019, identifiant fiscal 73266987, dont le siège social est situé 57, rue Mauritania, BP 2609, Guéliz, 40000 Marrakech, Maroc. Son objet social comprend 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.

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.

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.

Le service couvert par la présente politique relève des services de confiance autres que qualifiés, au sens de l'article 3 de la loi n° 43-20. Il vise la conformité à la norme ETSI EN 319 411-1, comme l'exige l'exigence 3 du référentiel [Ref_Serv_Conf_NonQual] pour la délivrance de certificats destinés au cachet électronique avancé.

> **Statut réglementaire —** 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.

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.

La présente politique est publiée 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. 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.

1.2. Acronymes et Définitions

Les acronymes et les termes définis ci-dessous ont, dans l'ensemble du document, le sens qui leur est donné ici.

1.2.1. Acronymes

Acronyme	Signification
AC	Autorité de certification
AE	Autorité d'enregistrement
ASiC	Associated Signature Containers (conteneur de signature associé)
CAdES	CMS Advanced Electronic Signatures
CEN	Comité européen de normalisation
CNDP	Commission Nationale de contrôle de la protection des Données à caractère Personnel
CNIE	Carte nationale d'identité électronique
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
DN	Distinguished Name (nom distinctif)
DPC	Déclaration des pratiques de certification
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de gestion de clés
LAR	Liste des autorités révoquées
LCP	Lightweight Certificate Policy (politique de certification allégée, ETSI EN 319 411-1)

Acronyme	Signification
LCR	Liste des certificats révoqués
MC	Mandataire de certification
NCP	Normalized Certificate Policy (politique de certification normalisée, ETSI EN 319 411-1)
NCP+	Politique normalisée exigeant un dispositif cryptographique sécurisé
OCSP	Online Certificate Status Protocol (protocole d'information en ligne sur l'état des certificats)
OID	Object Identifier (identifiant d'objet)
PAdES	PDF Advanced Electronic Signatures
PC	Politique de certification
PSCo	Prestataire de services de confiance
PSCE	Prestataire de services de certification électronique
RFC	Request for Comments (spécification publiée par l'IETF)
UTC	Temps universel coordonné
XAdES	XML Advanced Electronic Signatures

1.2.2. Terminologie

Terme	Définition retenue dans la présente politique
Autorité de certification	Composante qui, au nom et sous la responsabilité du prestataire, applique la présente politique et est identifiée comme émetteur dans les certificats délivrés à ce titre.
Autorité d'enregistrement	Fonction qui prend en compte et vérifie les informations d'identité du futur titulaire et constitue le dossier d'enregistrement correspondant.
Titulaire du certificat	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.
Mandataire de certification	Personne désignée par une entité et placée sous sa responsabilité, en relation directe avec l'autorité d'enregistrement, qui assure pour celle-ci une partie des vérifications d'identité.

Terme	Définition retenue dans la présente politique
Utilisateur de certificat	Personne ou entité qui reçoit un certificat et s'y fie pour vérifier le cachet électronique produit au moyen de ce certificat.
Personne autorisée	Personne, autre que le titulaire et le mandataire de certification, habilitée par la présente politique ou par contrat à accomplir certaines actions pour le compte du titulaire, notamment une demande de révocation.
module cryptographique matériel	Équipement matériel dédié aux opérations cryptographiques, à l'intérieur duquel les bi-clés d'autorité et les données de création de cachet des titulaires sont générées et conservées, et dont elles ne sortent jamais en clair.
Plateforme	La plateforme SELLO, canal d'enregistrement et de fourniture du service, agissant en qualité d'autorité d'enregistrement pour le compte du prestataire, dans le cadre du contrat écrit mentionné au chapitre 1.1.
Registre de publication	L'espace de publication documentaire du site institutionnel du prestataire, où sont mis à disposition les documents énumérés au chapitre 1.11.
Porteur	Terme employé par les intitulés du plan de référence de la DGSSI, reproduits tels quels ; il désigne le titulaire du certificat au sens du présent document. Le terme porteur de part de secret, employé au chapitre 5, désigne une notion distincte : le détenteur d’une part de secret d’activation d’une clé d’autorité.

1.3. Niveaux de sécurité

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. La présente politique couvre les deux premiers niveaux, qui relèvent du régime déclaratif des services de confiance autres que qualifiés.

Chaque niveau est associé à une politique distincte, portant son propre identifiant d'objet, et à une politique de référence de la norme ETSI EN 319 411-1 :

Niveau	OID de la politique	Politique ETSI de référence	Justification
Niveau simple	1.3.6.1.4.1.[PEN].1.1.2.1	LCP — Lightweight Certificate Policy 0.4.0.2042.1.3	Niveau destiné aux usages pour lesquels l’analyse de risque ne justifie pas l’ensemble des exigences de la politique normalisée, notamment la présence physique systématique.

Niveau	OID de la politique	Politique ETSI de référence	Justification
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	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 avancé se distingue du niveau simple par un point unique et déterminant : les données de création de cachet sont générées et conservées dans le module cryptographique matériel exploité par le prestataire et ne sont mises en œuvre qu'après une authentification forte du créateur du cachet. L'exigence 8 du référentiel [Ref_Serv_Conf_NonQual] impose cette garantie de contrôle exclusif pour le cachet électronique avancé.

> **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.

1.4. PSCE et niveau de sécurité

À chaque niveau correspondent des processus organisationnels, techniques et sécuritaires adaptés. Le tableau ci-dessous en donne la synthèse ; le détail figure aux chapitres 2 à 5.

Domaine	Niveau simple	Niveau avancé
Validation initiale de l'identité	Vérification de l'identité sur pièce officielle d'identité, contrôlée par l'autorité d'enregistrement selon les modalités du chapitre 2.2.	Contrôle d'identité en présence physique à titre de règle de base ; vérification à distance selon les modalités admises par le référentiel de la DGSSI.

Domaine	Niveau simple	Niveau avancé
Remise et acceptation du certificat	Notification au titulaire dans son espace sur la plateforme et acceptation explicite avant tout usage.	Notification et acceptation explicite, précédées d'une authentification forte du titulaire.
Protection des données de création de cachet	Génération et conservation dans le module cryptographique matériel exploité par le prestataire.	Génération et conservation dans le module cryptographique matériel, mise en œuvre subordonnée à une authentification forte du créateur du cachet.
Révocation	Demande authentifiée, canal disponible 24 heures sur 24, 7 jours sur 7, traitement en 24 heures au plus.	Identique, l'authentification de la demande reposant sur les mêmes facteurs que ceux du service.
Information sur l'état des certificats	Publication des listes de révocation et service en ligne, disponibles 24 heures sur 24, 7 jours sur 7.	Identique.
Protection des clés d'autorité	Génération et mise en œuvre dans le module cryptographique matériel, sous cérémonie de clés et double contrôle.	Identique.
Durée de validité du certificat	1 an	3 ans

Les valeurs ci-dessus ne sont pas des maxima déclaratifs : elles sont reprises, chiffrées, aux chapitres correspondants et à l'annexe 9.2, et toute évolution d'un de ces paramètres donne lieu à une révision de la présente politique dans les conditions du chapitre 8.

1.5. Cachet électronique sécurisé et certificat sécurisé

La loi n° 43-20 a remplacé le cadre antérieur : son article 83 abroge le chapitre préliminaire et le titre II de la loi n° 53-05, et son article 84 fixe son entrée en vigueur à la publication des textes pris pour son application. La notion de « certificat sécurisé » issue du cadre antérieur n'est donc plus le référentiel applicable, et la présente politique ne l'emploie pas.

Sous le cadre en vigueur, le cachet électronique qualifié est le niveau auquel la loi attache ses effets les plus forts. L'article 15 de la loi n° 43-20 subordonne ce niveau à un dispositif qualifié de création de cachet et à un certificat qualifié, et l'article 32 réserve la fourniture d'un service de confiance qualifié aux prestataires agréés.

> **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.

Les certificats de cachet électronique délivrés au titre de la présente politique ne sont donc pas des certificats qualifiés et ne sont jamais présentés comme tels, ni dans les certificats eux-mêmes, ni dans les documents du registre de publication, ni dans les interfaces de la plateforme.

1.6. Identification du document

La présente politique est identifiée par son identifiant d'objet, son titre, son numéro de version et sa date. Les identifiants d'objet des deux politiques qu'elle porte sont ceux inscrits dans l'extension certificatePolicies des certificats correspondants.

Élément	Valeur
Titre	Politique de certification – cachet électronique
Identifiant du document	YT-PC-SEAL
OID du document	1.3.6.1.4.1.[PEN].1.1.2
OID de la politique — niveau simple	1.3.6.1.4.1.[PEN].1.1.2.1
OID de la politique — niveau avancé	1.3.6.1.4.1.[PEN].1.1.2.2
Version	0.1
Statut	Projet — en préparation de la déclaration préalable
Classification	Diffusion publique
Langue	français

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

L'arc d'objet du prestataire est 1.3.6.1.4.1.[PEN].1, dérivé du numéro d'entreprise privée qui lui est attribué 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].

1.7. Fonctionnalités minimales couvertes par une IGC

L'autorité de certification a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie et s'appuie pour cela sur une infrastructure de gestion de clés. Les fonctions minimales mises en œuvre sont les suivantes.

- Autorité d'enregistrement — vérifie les informations d'identité du futur titulaire et, le cas échéant, les attributs demandés, avant de transmettre la demande à la fonction de génération ; elle procède également à la re-vérification lors du renouvellement.
- Fonction de génération des certificats — construit le certificat et le signe avec la clé privée de l'autorité émettrice, à partir des informations validées par l'autorité d'enregistrement et de la clé publique du titulaire.
- Fonction de génération des éléments secrets du titulaire — génère les données de création de cachet à l'intérieur du module cryptographique matériel ; aucun élément secret n'est remis

au titulaire sur un support, la mise en œuvre des données de création de cachet étant subordonnée aux facteurs d'authentification que celui-ci détient.

- Fonction de remise — met le certificat à disposition du titulaire dans son espace sur la plateforme et recueille son acceptation explicite.
- Fonction de publication — met à disposition les conditions générales, les politiques et pratiques publiées, les certificats d'autorité et toute autre information pertinente, hors informations d'état des certificats.
- Fonction de gestion des révocations — traite les demandes de révocation, en identifie et en authentifie l'origine, et détermine les actions à mener.
- Fonction d'information sur l'état des certificats — publie les listes de révocation et répond aux requêtes en ligne sur l'état d'un certificat.

La fonction de génération des éléments secrets du titulaire, optionnelle dans le plan de référence, est ici obligatoire : elle est la conséquence directe du modèle décrit au chapitre 5.1.1.2, dans lequel les données de création de cachet sont générées par le prestataire à l'intérieur du module cryptographique matériel.

1.8. Interactions avec l'IGC

Les entités et personnes suivantes interagissent avec l'infrastructure de gestion de clés.

- L'autorité de certification, qui applique la présente politique et figure comme émetteur dans les certificats délivrés à ce titre.
- L'autorité d'enregistrement, exercée par la plateforme SELLO pour le compte du prestataire dans le cadre du contrat écrit mentionné au chapitre 1.1.
- Le titulaire, personne morale identifiée dans le certificat, pour le compte de laquelle le cachet est apposé par ses systèmes à travers la plateforme.
- Le représentant légal de la personne morale, ou le mandataire qu’il désigne par écrit, qui présente la demande, accepte les conditions générales d’utilisation et exerce, pour le compte de la personne morale, les droits attachés au certificat.
- L'utilisateur de certificat, qui reçoit un certificat et s'y fie pour vérifier le cachet électronique produit au moyen de ce certificat.
- La personne autorisée, habilitée à accomplir certaines actions pour le compte du titulaire, notamment une demande de révocation.
- L'autorité nationale, qui exerce le contrôle a posteriori des prestataires non agréés en application de l'article 52 de la loi n° 43-20.

L'ordonnancement de ces fonctions relève du modèle adopté par le prestataire ; il est décrit dans la déclaration des pratiques de certification (YT-DPC). Les prestations effectivement fournies au titre de la présente politique sont la vérification d'identité par l'autorité d'enregistrement, la génération des données de création de cachet dans le module cryptographique matériel, la génération et la délivrance du certificat, la mise à disposition du service d’apposition de cachet électronique à travers la plateforme et la gestion des révocations.

1.9. Responsabilités

Les engagements ci-dessous s'ajoutent aux obligations légales et réglementaires ; ils sont repris, en des termes opposables à chaque partie, dans les conditions générales d'utilisation applicables.

1.9.1. De l'autorité de certification du prestataire

Quelle que soit l'organisation opérationnelle mise en œuvre, le prestataire demeure responsable, vis-à-vis de toute partie externe à l'infrastructure, des prestations fournies et du respect des engagements pris dans la présente politique et dans sa déclaration des pratiques. Le cadre contractuel qui le lie à chacune de ses composantes est documenté par écrit.

- Appliquer la présente politique et faire appliquer, par chaque composante, les procédures correspondantes de la déclaration des pratiques.
- Vérifier, avant toute délivrance, l'identité du futur titulaire dans les conditions du chapitre 2.2, 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 à l'annexe 9.4 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 le délai fixé au chapitre 4.8, avant toute cessation d'activité.
- Souscrire et maintenir une assurance de responsabilité professionnelle couvrant l'activité de services de confiance.

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.

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.

1.9.2. De l'autorité d'enregistrement du prestataire

L'autorité d'enregistrement, exercée par la plateforme pour le compte du prestataire, s'engage sur les points suivants.

- Recueillir la demande, vérifier l'identité du demandeur et, le cas échéant, la qualité et les pouvoirs de son représentant, selon les procédures du chapitre 2.2.
- 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.

1.9.3. Du titulaire du certificat

La personne morale titulaire du certificat de cachet électronique s’engage, par son représentant légal, sur les points suivants, repris en termes opposables dans les conditions générales d’utilisation YT-CGU-PM.

- 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 domaines d’utilisation du chapitre 1.10.1.1 et dans les limites de l’extension Key Usage.
- 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 conditions générales d’utilisation applicables et la présente politique.

1.9.4. Du mandataire de certification

Le représentant légal de la personne morale, et le cas échéant le mandataire qu’il désigne par écrit, s’engagent sur les points suivants.

- Vérifier l'identité des personnes dont il transmet les demandes et conserver les preuves de cette vérification.
- Attester auprès de l'autorité d'enregistrement de l'exactitude des informations transmises.
- Signaler sans délai toute cause de révocation dont il a connaissance.
- Restituer ses attributions dès la fin de son mandat, laquelle constitue elle-même une cause de révocation des certificats concernés.

1.10. Usage des certificats

Un certificat délivré au titre de la présente politique ne peut être utilisé que dans les domaines d'utilisation énoncés ci-dessous. Tout autre usage est exclu et exonère le prestataire dans les conditions du chapitre 1.9.1.

1.10.1. Domaines d'utilisation applicables

Les domaines d'utilisation se distinguent selon que la bi-clé et le certificat sont ceux d'un titulaire ou ceux d'une composante de l'infrastructure.

1.10.1.1. Bi-clés et certificats des titulaires

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, garantissant l’origine et l’intégrité des données cachetées.

- 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.

Les formats admis pour les cachets électroniques avancés et pour les conteneurs associés 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)

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, ainsi que tout usage pour lequel la réglementation exige un certificat qualifié.

1.10.1.2. Bi-clés et certificats d'autorité et de composantes

- La bi-clé de l'autorité racine YORYX TRUST Root CA G1 sert exclusivement à signer les certificats des autorités émettrices et les listes de révocation d'autorités.
- La bi-clé de l'autorité émettrice YORYX TRUST Seal CA G1 sert exclusivement à signer les certificats de cachet électronique délivrés au titre de la présente politique et les listes de révocation correspondantes.

- La bi-clé d'un répondeur d'information sur l'état des certificats sert exclusivement à signer les réponses de ce service.

Aucune de ces bi-clés n'est utilisée à d'autres fins, notamment ni pour le chiffrement, ni pour l'authentification de serveur, ni pour la signature de code.

1.11. Gestion de la PC

La présente politique est un document maîtrisé : elle est approuvée, versionnée, publiée et révisée selon les règles ci-dessous.

1.11.1. Entité gérant la PC

La politique est établie et maintenue par le prestataire. Elle est approuvée par la présidence de la société, sur proposition du responsable de sécurité et après examen du contrôleur ; l'approbation est formalisée par écrit et conservée au dossier d'audit. Aucune personne physique n'est désignée nominativement dans le présent document : seules les fonctions le sont.

1.11.2. Point de contact

Objet	Coordonnée
Adresse électronique	trust@yoryx.com
Adresse postale	57, rue Mauritania, BP 2609, Guéliz, 40000 Marrakech, Maroc
Registre de publication	le registre de publication du site institutionnel de YORYX TRUST
Réclamations	Procédure décrite dans le document YT-COMPLAINTS

Toute question relative à l'interprétation de la présente politique, toute demande de révocation et toute réclamation sont adressées à ce point de contact. Les délais d'accusé de réception et de réponse aux réclamations sont fixés par le document YT-COMPLAINTS.

1.11.3. Entité déterminant la conformité d'une DPC avec cette PC

La conformité de la déclaration des pratiques de certification (YT-DPC) à la présente politique est établie par le contrôleur, fonction distincte de celles d'opérateur, d'ingénieur système et de responsable d'application, conformément à la règle de séparation énoncée au chapitre 4.2.4. Son appréciation est portée à la connaissance de la présidence et versée au dossier d'audit.

1.11.4. Procédures d'approbation de la conformité de la DPC

1. Le responsable d'application soumet la déclaration des pratiques, ou sa révision, au contrôleur.
2. Le contrôleur vérifie, chapitre par chapitre, que chaque exigence de la présente politique trouve une pratique correspondante, et consigne les écarts.
3. 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.
4. La présidence approuve la déclaration des pratiques après clôture des écarts, ou en connaissance des écarts subsistants et de leur plan de traitement.

5. La version approuvée est publiée dans le registre de publication du site institutionnel de YORYX TRUST au plus tard le jour de sa prise d'effet.

2. IDENTIFICATION ET AUTHENTIFICATION

2.1. Nommage

Les règles de nommage ci-dessous s'appliquent aux certificats d'autorité, aux certificats de composantes et aux certificats de titulaires.

2.1.1. Types de noms

Les noms utilisés sont des noms distinctifs (DN) conformes à la norme X.501 et au profil de l'annexe 9.4. Les gabarits sont les suivants.

Certificat	Nom distinctif
Autorité racine	C=MA, O=YORYX TRUST SASU, organizationIdentifier=NTRMA-184667, CN=YORYX TRUST Root CA G1
Autorité émettrice	C=MA, O=YORYX TRUST SASU, organizationIdentifier=NTRMA-184667, CN=<nom de l’autorité émettrice>
Titulaire (personne morale)	C=MA, O=<dénomination de la personne morale>, organizationIdentifier=<NTRMA-|ICE- suivi de l’identifiant officiel>, CN=<nom du cachet>

L'attribut organizationIdentifier porte l'identifiant national d'immatriculation du prestataire sous la forme NTRMA-184667, et l'attribut serialNumber du certificat d'autorité porte l'identifiant commun de l'entreprise ICE 004013324000019, afin qu'un utilisateur de certificat puisse rattacher l'émetteur à une entité réelle.

2.1.2. Nécessité d'utilisation de noms explicites

Le nom distinctif d’un certificat de titulaire porte la dénomination de la personne morale telle qu’elle figure au registre du commerce, son identifiant officiel et le nom du cachet, de manière à identifier sans ambiguïté l’entité pour le compte de laquelle le cachet est apposé.

Les pseudonymes ne sont pas admis. Aucun nom distinctif ne comporte de mention susceptible d'induire en erreur sur l'identité du titulaire, sur son rattachement à une entité ou sur la nature du service.

2.1.3. Unicité des noms

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.

L'unicité est obtenue par l’identifiant officiel de la personne morale porté dans l’attribut organizationIdentifier, complété par le nom du cachet lorsqu’une même personne morale détient plusieurs certificats de cachet. Les champs Unique Identifiers de la norme X.509 ne sont pas utilisés, l'unicité du nom distinctif rendant leur emploi inutile.

2.1.4. Identification, authentification et rôle des marques déposées

Le prestataire ne vérifie pas la titularité des droits de propriété intellectuelle attachés à un signe figurant dans une demande et n'arbitre aucun litige relatif à une marque. Le nom du cachet peut reprendre un signe distinctif de la personne morale ; celle-ci garantit alors détenir les droits nécessaires à cet usage et fait son affaire de toute contestation élevée par un tiers.

YORYX® — marque utilisée sous licence : le signe « YORYX » est utilisé par la société en vertu d'un contrat de licence de marque, et cet usage ne lui confère aucun droit de propriété sur les marques correspondantes.

2.2. Validation initiale 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'enrôlement s'effectue par la plateforme, qui exerce les fonctions d'autorité d'enregistrement dans le cadre du contrat écrit préalable mentionné au chapitre 1.1 ; l'exigence 10 du référentiel [Ref_Serv_Conf_NonQual] constitue le fondement de cette organisation dans le référentiel applicable.

L'exigence 11 du référentiel [Ref_Serv_Conf_NonQual] précise que les dispositions de vérification de l'identité du référentiel [Ref_Deliv_Cert_Qual] demeurent applicables — suffisantes sans être nécessaires — pour la délivrance de certificats non qualifiés conformes à la norme ETSI EN 319 411-1, en particulier de type NCP et NCP+. La présente politique 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.

2.2.1. Méthode pour prouver la possession de la clé privée

Les données de création de cachet du titulaire sont générées à l'intérieur du module cryptographique matériel exploité par le prestataire, à la demande de l'autorité d'enregistrement et après validation du dossier d'enregistrement. La preuve de possession est donc établie par construction : la clé publique soumise à la fonction de génération des certificats est celle que le module vient de produire, et le module atteste de la correspondance entre la clé publique et la clé privée qu'il détient.

Aucune demande de certificat portant une clé publique produite hors du module cryptographique matériel n'est acceptée. Il n'existe par conséquent aucun cas dans lequel une preuve de possession devrait être apportée par une requête signée transmise par le titulaire.

2.2.2. Enregistrement d'un titulaire

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 par la présente politique, 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, lesquels constituent les données d’activation décrites au chapitre 5.4.1.2.
6. Il prend connaissance de la présente politique, de la déclaration de divulgation YT-PDS-CERT et des conditions générales d’utilisation YT-CGU-PM, et les accepte explicitement 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 d'identité produites et le résultat de leur contrôle, la date, le mode de vérification retenu et la fonction ayant procédé au contrôle, l'acceptation des conditions générales d'utilisation applicables, et le cas échéant les pièces établissant la qualité et les pouvoirs du représentant. Il est conservé pendant la durée fixée au chapitre 4.5.2.

2.2.3. Informations non vérifiées du titulaire

Aucune information non vérifiée n'est portée dans un certificat. Toute donnée inscrite dans un champ ou une extension du certificat a été contrôlée par l'autorité d'enregistrement au vu d'une pièce probante.

Les informations recueillies pour les seuls besoins de la relation de service et non portées dans le certificat — notamment l'adresse électronique de contact et les facteurs d'authentification — ne sont pas certifiées et n'engagent pas le prestataire à l'égard des tiers.

2.2.4. Validation de l'autorité du demandeur

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.

2.2.5. Critères d'interopérabilité

Les certificats délivrés sont conformes à la norme IETF RFC 5280 et au profil de l'annexe 9.4 ; les listes de révocation sont conformes au profil de l'annexe correspondante et au chapitre 6.2 ; le service d'information en ligne sur l'état des certificats met en œuvre le protocole IETF RFC 6960. Aucune extension propriétaire n'est employée.

Les certificats des autorités de certification sont publiés dans le registre de publication du site institutionnel de YORYX TRUST afin que tout utilisateur de certificat puisse construire et vérifier la chaîne de certification sans accord préalable ni frais.

2.3. Identification et validation d'une demande de renouvellement des clés

Le renouvellement au sens de la présente politique s'entend de la délivrance d'un nouveau certificat sur une nouvelle bi-clé : un certificat n'est jamais re-signé sur une bi-clé existante. Le chapitre 3.6 en tire les conséquences opérationnelles.

2.3.1. Identification et validation pour un renouvellement courant

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.

L'autorité d'enregistrement vérifie que les informations portées dans le certificat n'ont pas changé. En cas de changement de l'une d'entre elles, la demande est traitée comme un premier enregistrement, selon le chapitre 2.2, et le certificat en cours est révoqué pour inexactitude d'une information portée dans le certificat.

Une re-vérification complète de l'identité, dans les conditions du chapitre 2.2, 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.

2.3.2. Identification et validation pour un renouvellement après révocation

Un certificat révoqué n'est jamais rétabli. Une demande présentée après révocation constitue une nouvelle demande et suit intégralement la procédure d'enregistrement initial du chapitre 2.2, y compris la production des pièces d'identité et le contrôle correspondant.

Lorsque la révocation a pour cause une compromission ou une suspicion de compromission des données de création de cachet, la nouvelle bi-clé est générée dans le module cryptographique matériel et les facteurs d'authentification du titulaire sont réinitialisés avant toute délivrance.

2.3.3. Identification et validation d'une demande de révocation

L'origine d'une demande de révocation est authentifiée avant tout traitement. Sont admises : le représentant légal de la personne morale ; le mandataire habilité par écrit ; une personne autorisée au sens du chapitre 1.2.2 ; l’autorité d’enregistrement ; le prestataire, agissant de sa propre initiative lorsqu’une cause du chapitre 3.9.1.1 est constatée ; l’autorité nationale ou une autorité judiciaire dans l’exercice de leurs attributions.

Les canaux de demande sont disponibles 24 heures sur 24, 7 jours sur 7. 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.

Le formulaire de demande de révocation figure au registre de publication sous l'identifiant YT-FORM-REVOCATION.

3. EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

3.1. Demande de certificat

3.1.1. Origine d'une demande de certificat

Une demande de certificat émane du représentant légal de la personne morale, ou d'un mandataire qu'il a habilité par écrit, présentée par la plateforme.

Aucune demande n'est acceptée d'une origine autre que celles énumérées ci-dessus. Une demande présentée par un tiers non habilité est rejetée et le rejet est consigné.

3.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat

La demande est établie sur la plateforme, qui recueille les informations nécessaires, présente les documents applicables — la présente politique, la déclaration des pratiques (YT-DPC), les conditions générales d'utilisation applicables et la déclaration de divulgation YT-PDS-CERT — et enregistre leur acceptation explicite avant toute suite.

- Le demandeur fournit les informations et les pièces énumérées au chapitre 2.2.2 et atteste de leur exactitude ; le formulaire correspondant figure au registre de publication sous l'identifiant YT-FORM-LEGAL-REP.
- L'autorité d'enregistrement contrôle les pièces, procède à la vérification d'identité et constitue le dossier d'enregistrement.
- Le prestataire vérifie la complétude du dossier reçu et la cohérence des informations destinées à figurer dans le certificat.
- Le demandeur accepte les conditions générales d'utilisation applicables et prend connaissance des limites d'usage du certificat.

Les responsabilités respectives de ces intervenants sont celles énoncées au chapitre 1.9.

3.2. Traitement d'une demande de certificat

3.2.1. Exécution des processus d'identification et de validation de la demande

L'autorité d'enregistrement exécute les processus décrits au chapitre 2.2 : contrôle des pièces, vérification de l'identité de la personne morale et de son représentant selon le chapitre 2.2.2, et le cas échéant vérification de la qualité et des pouvoirs du représentant. Le résultat de chaque contrôle est horodaté, associé à la fonction qui l'a conduit et versé au dossier d'enregistrement.

La demande n'est transmise à la fonction de génération des certificats qu'après validation complète du dossier. Les informations destinées au certificat sont transmises par un canal dont l'intégrité et l'authenticité de l'origine sont assurées.

3.2.2. Acceptation ou rejet de la demande

La demande est acceptée lorsque l'identité a été vérifiée, que les pièces produites sont valides et cohérentes, que les informations destinées au certificat sont exactes et que les conditions générales d'utilisation ont été acceptées. Elle est rejetée dans le cas contraire.

- Le rejet est motivé et notifié au demandeur.
- Le motif du rejet est consigné et conservé selon le chapitre 4.5.

- Un rejet fondé sur un doute sur l'identité n'est jamais levé par une simple réitération de la demande : il exige la production de nouvelles pièces ou un contrôle en présence physique.

3.2.3. Durée d'établissement du certificat

Le certificat est établi dès la validation de la demande. La durée d'établissement n'est pas un engagement de délai commercial : elle est bornée par l'obligation de ne pas générer de certificat sur un dossier incomplet. Aucun certificat n'est généré par anticipation, avant validation.

Les délais opposables au prestataire au titre de la présente politique sont ceux de la révocation et de l'information sur l'état des certificats, fixés aux chapitres 3.9.5 et 3.10, ainsi que ceux de l'annexe 9.2.

3.3. Délivrance du certificat

3.3.1. Actions de l'AC concernant la délivrance du certificat

1. L'autorité émettrice YORYX TRUST Seal CA G1 vérifie que la demande provient de la fonction d'enregistrement habilitée et que son intégrité est intacte.
2. Elle vérifie que la clé publique soumise provient du module cryptographique matériel et qu'aucun certificat en cours de validité ne porte déjà le même nom distinctif pour un autre titulaire.
3. Elle construit le certificat conformément au profil de l'annexe 9.4, y inscrit l'identifiant de la politique applicable au niveau demandé et la période de validité correspondante.
4. Elle signe le certificat avec sa clé privée, mise en œuvre à l'intérieur du module cryptographique matériel.
5. Elle journalise l'opération conformément au chapitre 4.4.1.

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.

3.3.2. Notification par l'AC de la délivrance du certificat au porteur

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. La notification indique l'identifiant du certificat, sa période de validité, la politique sous laquelle il a été délivré et l'adresse du registre de publication où figurent les documents applicables.

Aucun élément secret n'accompagne cette notification : les données de création de cachet demeurent dans le module cryptographique matériel. 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.

3.4. Acceptation du certificat

3.4.1. Démarche d'acceptation du certificat

Le titulaire prend connaissance du contenu du certificat et l'accepte explicitement avant tout usage. L'acceptation est recueillie par la plateforme, horodatée et conservée ; elle 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, si le titulaire le demande, une nouvelle demande est instruite.

3.4.2. Publication du certificat

Les certificats de titulaires ne sont pas publiés. Cette abstention est délibérée : la publication d'un annuaire de certificats de personnes morales constituerait une diffusion de données non nécessaire à la vérification du cachet électronique, laquelle s'opère à partir du certificat transmis avec le cachet.

Sont en revanche 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 : les certificats des autorités de certification, les listes de révocation et le point d'accès au service d'information sur l'état des certificats.

3.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

L'autorité d'enregistrement est informée de la délivrance afin de clore le dossier d'enregistrement. Le représentant légal de la personne morale est informé de la délivrance, y compris lorsque la demande a été présentée par un mandataire habilité.

Aucune autre entité n'est notifiée : la délivrance d'un certificat n'est pas rendue publique.

3.5. Usages de la bi-clé et du certificat

3.5.1. Utilisation de la clé privée et du certificat par le porteur

La personne morale met en œuvre ses données de création de cachet exclusivement pour apposer des cachets électroniques, à l’intérieur du module cryptographique matériel et par l’intermédiaire de la plateforme.

- L'usage est limité aux domaines d'utilisation du chapitre 1.10.1.1 et à la valeur de l'extension Key Usage inscrite dans le certificat.
- L'usage cesse à l'expiration ou à la révocation du certificat ; aucune opération n'est produite après l'un de ces deux évènements.
- L'usage est subordonné, à chaque opération, à une authentification forte du créateur du cachet.

3.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat

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.

- Construire la chaîne de certification jusqu'à un certificat d'autorité racine dont l'authenticité a été établie à partir du registre de publication.
- Vérifier que la date de l'opération se situe dans la période de validité du certificat.
- Vérifier l'état du certificat, soit auprès de la liste de révocation en vigueur, soit auprès du service d'information en ligne, dans les conditions du chapitre 3.9.6.
- Vérifier que l'usage effectif du certificat entre dans les domaines d'utilisation déclarés et dans la valeur de l'extension Key Usage.
- Vérifier l'identifiant de politique inscrit dans l'extension certificatePolicies, afin de connaître le niveau sous lequel le certificat a été délivré.

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

3.6. Renouvellement d'un certificat

Le renouvellement d'un certificat sur la même bi-clé n'est pas pratiqué. Un nouveau certificat est délivré sur une nouvelle bi-clé, selon le chapitre 3.7, ce qui borne la durée d'exposition d'une même clé privée à la durée de vie d'un seul certificat.

Cette règle est plus stricte que le plan de référence, qui admet le renouvellement à clé constante. Elle est retenue parce que la bi-clé est générée dans le module cryptographique matériel et que sa régénération n'impose au titulaire ni manipulation, ni support, ni coût.

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 le guide YT-GUIDE-USE.

3.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé

3.7.1. Causes possibles de changement d'une bi-clé

- L'échéance du certificat en cours de validité.
- La révocation du certificat, quelle qu'en soit la cause.
- La compromission, la suspicion de compromission, la perte ou le vol des données de création de cachet.
- L'évolution des exigences cryptographiques, notamment un changement de taille de clé ou d'algorithme rendu nécessaire par le chapitre 5.1.4.
- Le changement d'une information portée dans le certificat.

3.7.2. Origine d'une demande d'un nouveau certificat

Une demande de certificat émane du représentant légal de la personne morale, ou d’un mandataire qu’il a habilité par écrit, présentée par la plateforme.

3.7.3. Procédure de traitement d'une demande d'un nouveau certificat

La demande suit la procédure des chapitres 3.1 à 3.3. La vérification d'identité est celle du chapitre 2.3.1 lorsque le certificat en cours est valide et que les informations n'ont pas changé, et celle du chapitre 2.2 dans tous les autres cas.

Une nouvelle bi-clé est générée dans le module cryptographique matériel ; la bi-clé précédente est désactivée puis détruite selon le chapitre 5.2.10.2.

3.7.4. Notification au porteur de l'établissement du nouveau certificat

La notification suit les modalités du chapitre 3.3.2. Elle rappelle la période de validité du nouveau certificat et, le cas échéant, la date à laquelle le certificat précédent cesse d'être utilisable.

3.7.5. Démarche d'acceptation du nouveau certificat

L'acceptation suit les modalités du chapitre 3.4.1. Le nouveau certificat n'est utilisable qu'après acceptation explicite.

3.7.6. Publication du nouveau certificat

Les règles du chapitre 3.4.2 s'appliquent sans changement : le certificat de titulaire n'est pas publié.

3.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Les règles du chapitre 3.4.3 s'appliquent sans changement.

3.8. Modification du certificat

La modification d'un certificat en cours de validité n'est pas pratiquée : un certificat est immuable une fois signé.

Tout changement d'une information portée dans le certificat entraîne la révocation de celui-ci et la délivrance d'un nouveau certificat, après vérification de l'information modifiée dans les conditions du chapitre 2.2.

3.9. Révocation et suspension des certificats

La fonction de gestion des révocations et la fonction d'information sur l'état des certificats sont opérées dès la première délivrance de certificat : elles ne sont pas différées et ne sont subordonnées à aucune étape ultérieure. Seule la publication, dans le registre du site institutionnel, des certificats des autorités de certification suit le calendrier de publication du registre.

3.9.1. Causes possibles d'une révocation

3.9.1.1. Certificats de titulaires

- 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. La compromission d’un moyen d’authentification des systèmes de la personne morale n’est pas, à elle seule, une cause de révocation du certificat : elle entraîne la révocation de ce moyen et un nouvel enrôlement, les données de création de cachet demeurant dans le module cryptographique matériel. Elle devient une cause de révocation dès lors qu’elle laisse craindre qu’un cachet ait pu être apposé sans l’accord de la personne morale.

3.9.1.2. Certificats d'une composante de l'IGC

- Compromission, suspicion de compromission, perte ou vol de la clé privée de la composante.
- Cessation d'exploitation de la composante ou de son service.

- Inexactitude ou changement d'une information portée dans le certificat de la composante.
- Décision de l'autorité nationale ou décision de justice.
- Non-conformité constatée de la composante à la présente politique ou à la déclaration des pratiques, non corrigée dans le délai du plan d'action.

La révocation du certificat d'une autorité émettrice entraîne la révocation de l'ensemble des certificats qu'elle a délivrés et qui sont encore en cours de validité, ainsi que l'information sans délai des titulaires concernés et de l'autorité nationale.

3.9.2. Origine d'une demande de révocation

3.9.2.1. Certificats de titulaires

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 du chapitre 1.2.2 ; l’autorité d’enregistrement ; le prestataire, agissant de sa propre initiative lorsqu’une cause du chapitre 3.9.1.1 est constatée ; l’autorité nationale ou une autorité judiciaire dans l’exercice de leurs attributions.

3.9.2.2. Certificats d'une composante de l'IGC

Sont habilités à demander la révocation du certificat d'une composante : le responsable de sécurité, le responsable d'application dont relève la composante, le contrôleur, la présidence de la société, ainsi que l'autorité nationale dans l'exercice de ses attributions.

3.9.3. Procédure de traitement d'une demande de révocation

3.9.3.1. Révocation d'un certificat de titulaire

1. La demande est reçue par l'un des canaux disponibles 24 heures sur 24, 7 jours sur 7.
2. L'origine de la demande est authentifiée selon le chapitre 2.3.3.
3. La cause invoquée est rattachée à l'une des causes du chapitre 3.9.1.1 ; en cas de doute sur une compromission, la révocation est prononcée.
4. La révocation est inscrite dans la base de révocation, puis diffusée par la liste de révocation et par le service d'information en ligne, dans le délai du chapitre 3.9.5.1.
5. Le titulaire, et le cas échéant le demandeur, sont informés de la suite donnée.
6. L'opération est journalisée conformément au chapitre 4.4.1 et versée aux archives.

Une révocation est définitive et irréversible. Une demande présentée par erreur n'est pas annulée : un nouveau certificat est délivré selon le chapitre 3.7.

3.9.3.2. Révocation d'un certificat d'une composante de l'IGC

La décision est prise par le responsable de sécurité, sous double contrôle avec le responsable d'application ou la présidence. Elle donne lieu à un procès-verbal versé au dossier d'audit, à la mise à jour de la liste des autorités révoquées, à l'information des titulaires concernés et, lorsque l'incident relève de l'article 40 de la loi n° 43-20, à la notification prévue au chapitre 4.7.1.

3.9.4. Délai accordé au porteur pour formuler la demande de révocation

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 est opposable au titulaire dans les conditions du chapitre 1.9.3.

3.9.5. Délai de traitement par l'AC d'une demande de révocation

3.9.5.1. Révocation d'un certificat de 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.

3.9.5.2. Révocation d'un certificat d'une composante de l'IGC

La révocation du certificat d'une composante est traitée sans délai et l'information d'état correspondante est publiée immédiatement après la décision, sans attendre l'échéance périodique de la liste de révocation.

3.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat vérifie l'état de révocation au moment où il se fie au cachet électronique. Cette vérification s'opère soit auprès de la liste de révocation en vigueur, dont la fréquence de publication est fixée au chapitre 3.9.7, soit auprès du service d'information en ligne du chapitre 3.10.

Une vérification fondée sur une liste de révocation dont la date de prochaine mise à jour est dépassée n'est pas une vérification : l'utilisateur obtient une liste à jour ou interroge le service en ligne.

3.9.7. Fréquence d'établissement des LCR

La liste de révocation des certificats de titulaires est établie au moins toutes les 24 heures, et immédiatement après toute révocation. Le champ nextUpdate est positionné à 72 heures après la date de production, de sorte qu'une interruption temporaire de la fonction de publication ne rende pas la liste inexploitable.

La liste des autorités révoquées, produite par l'autorité racine, est établie tous les 6 mois, et à chaque révocation d’un certificat d’autorité émettrice.

3.9.8. Délai maximum de publication d'une LCR

Chaque liste de révocation est publiée dans les 30 minutes suivant sa génération et reste accessible sans contrôle d’accès ni frais.

3.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Un service d'information en ligne sur l'état des certificats, conforme au protocole IETF RFC 6960, est mis en œuvre et disponible 24 heures sur 24, 7 jours sur 7 ; il est accessible publiquement, sans contrôle d’accès ni frais.

Les réponses sont signées par un répondeur délégué, certifié par l’autorité émettrice concernée, dont le certificat est délivré par l'autorité émettrice concernée et dont la période de validité est fixée au chapitre 5.3.2.

3.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

L'utilisateur qui interroge le service en ligne vérifie la signature de la réponse, l'identité du répondeur et la fraîcheur de la réponse. Une réponse dont la date de production est antérieure de plus de 24 heures à l'instant de la vérification n'est pas exploitée.

Le point d'accès au service est inscrit dans l'extension Authority Information Access des certificats délivrés, conformément au profil de l'annexe 9.4.

3.9.11. Autres moyens disponibles d'information sur les révocations

Aucun autre moyen d'information sur l'état des certificats n'est mis en œuvre. Sans objet : les listes de révocation delta ne sont pas mises en œuvre. La liste de révocation complète est publiée au moins toutes les 24 heures, ce qui rend l’incrément sans effet utile au volume d’émission déclaré.

3.9.12. Exigences spécifiques en cas de compromission de la clé privée

En cas de compromission ou de suspicion de compromission des données de création de cachet d'un titulaire, la révocation est prononcée sans attendre l'issue de l'analyse, l'information d'état est publiée immédiatement, les facteurs d'authentification du titulaire sont réinitialisés et les journaux correspondants sont conservés pour l'analyse.

En cas de compromission de la clé privée d'une autorité de certification, les mesures du chapitre 4.7.3 s'appliquent : révocation du certificat de l'autorité, information des titulaires et des utilisateurs de certificats par le registre de publication, notification à l'autorité nationale au titre de l'article 40 de la loi n° 43-20, et génération d'une nouvelle bi-clé en cérémonie.

3.9.13. Causes possibles d'une 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.

3.9.14. Origine d'une demande de suspension

Sans objet : la suspension n'étant pas proposée, aucune demande de suspension n'est recevable. Une demande formulée en ce sens est instruite comme une demande de révocation, selon le chapitre 3.9.3.1.

3.9.15. Procédure de traitement d'une demande de suspension

Sans objet : aucune procédure de suspension n'est mise en œuvre. Le choix de ne pas proposer la suspension 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.

3.9.16. Limites de la période de suspension d'un certificat

Sans objet : la suspension n'étant pas proposée, aucune période de suspension n'existe.

3.10. Fonction d'information sur l'état des certificats

3.10.1. Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats est assurée par deux moyens complémentaires : la publication de listes de révocation signées, dans les conditions des chapitres 3.9.7 et 3.9.8, et un service de requête en ligne conforme au protocole IETF RFC 6960, dans les conditions du chapitre 3.9.9.

Les deux moyens reposent sur la même base de révocation et délivrent donc la même information ; en cas d'écart apparent, l'information la plus récente prévaut.

Ces deux moyens sont opérés dès la première délivrance de certificat sous la présente politique.

3.10.2. Disponibilité de la fonction

Fonction	Disponibilité	Indisponibilité maximale par interruption	Indisponibilité maximale par mois
Information sur l'état des certificats	24 heures sur 24, 7 jours sur 7	1 heure	4 heures
Gestion des révocations	24 heures sur 24, 7 jours sur 7	30 minutes	2 heures
Publication des certificats d'autorité	24 heures sur 24, 7 jours sur 7	1 heure	4 heures
Publication des autres informations	jours ouvrés	8 heures (jours ouvrés)	32 heures (jours ouvrés)

Ces valeurs sont reprises à l'annexe 9.2. Elles sont mesurées et vérifiées lors du contrôle de conformité annuel du chapitre 7.1.

3.10.3. Dispositifs optionnels

Aucun dispositif optionnel d'information sur l'état des certificats n'est mis en œuvre au-delà des deux moyens décrits au chapitre 3.10.1. Sans objet : les listes de révocation delta ne sont pas mises en œuvre. La liste de révocation complète est publiée au moins toutes les 24 heures, ce qui rend l’incrément sans effet utile au volume d’émission déclaré.

3.11. Fin de la relation entre le porteur et l'AC

La fin de la relation entre le titulaire et le prestataire entraîne la révocation des certificats en cours de validité, la désactivation puis la destruction des données de création de cachet correspondantes selon le chapitre 5.2.10.2, et la conservation du dossier de preuve pendant la durée fixée au chapitre 4.5.2.

La fin de la relation n'efface pas les opérations déjà produites : les éléments permettant de vérifier les cachets électroniques produits pendant la période de validité du certificat demeurent conservés, ce qui est la condition même de la valeur probante de ces opérations.

Les conditions dans lesquelles cette fin de relation intervient et ses conséquences pour le titulaire sont énoncées dans les conditions générales d'utilisation applicables.

3.12. Séquestre de clé et recouvrement

3.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet : aucun séquestre des données de création de cachet des titulaires n'est mis en œuvre, et aucune procédure de recouvrement n'existe. Les données de création de cachet servent exclusivement à apposer un cachet électronique ; elles ne servent jamais au chiffrement, de sorte

que leur perte n'entraîne la perte d'aucune donnée. La clé est régénérée dans le module cryptographique matériel et un nouveau certificat est délivré selon le chapitre 3.7.

Les sauvegardes chiffrées des clés d'autorité mentionnées au chapitre 5.2.4 ne constituent pas un séquestre : elles portent sur les clés du prestataire, non sur celles des titulaires, et leur restauration est soumise au même quorum que les opérations sur les clés.

3.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet : aucun service de chiffrement n'est fourni au titre de la présente politique, et aucune clé de session n'est encapsulée ni recouvrée.

4. MESURES DE SÉCURITÉ NON TECHNIQUES

Les mesures décrites dans le présent chapitre s'appliquent à toutes les composantes de l'infrastructure de gestion de clés. Leur mise en œuvre opérationnelle est décrite dans la déclaration des pratiques de certification (YT-DPC). Conformément à la règle de non-divulgation du chapitre 7.6, la description détaillée des dispositifs de sécurité n'est pas publiée.

4.1. Mesures de sécurité physique

4.1.1. Situation géographique et construction des sites

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.

Les deux sites sont distants l'un de l'autre et ne partagent ni alimentation électrique, ni arrivée de télécommunication, ni zone de risque naturel. Leur localisation n'est pas publiée : la publier reviendrait à désigner la cible.

> **Point ouvert —** L’exploitation repose sur un site principal et un site secondaire ; les exigences physiques minimales opposables sont celles du référentiel applicable.

4.1.2. Accès physique

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.

- L'accès à la zone sensible, qui abrite les équipements cryptographiques, est nominatif, limité aux rôles de confiance du chapitre 4.2.1 et soumis au double contrôle.
- Toute entrée et toute sortie sont enregistrées, avec la date, l'heure, l'identifiant de la personne et le motif.
- Tout visiteur est accompagné en permanence par une personne habilitée et inscrit au registre des visites.
- Les droits d'accès sont revus périodiquement et retirés immédiatement à la fin de l'affectation.

4.1.3. Alimentation électrique et climatisation

Chaque site dispose d'une alimentation électrique secourue, d'une source autonome de relève et d'une climatisation redondée. La capacité de la source autonome permet soit la poursuite du service, soit un arrêt ordonné des équipements sans perte d'intégrité. Les dispositifs sont testés périodiquement et chaque test donne lieu à un compte rendu.

4.1.4. Vulnérabilité aux dégâts des eaux

Les équipements sensibles ne sont pas installés au niveau le plus bas des bâtiments ni sous des canalisations. Une détection de présence d'eau est installée dans les zones techniques et sensibles, et son déclenchement est reporté vers la fonction de surveillance.

4.1.5. Prévention et protection incendie

Chaque site est équipé d'une détection automatique d'incendie et d'un dispositif d'extinction adapté aux équipements informatiques, sans agent susceptible d'endommager les supports. Les consignes d'évacuation et d'intervention sont affichées et exercées périodiquement.

4.1.6. Conservation des supports

Les supports contenant des données sensibles — sauvegardes, journaux, archives, parts de secret — sont conservés dans des contenants scellés, dans des coffres, en zone sensible, avec un registre daté des remises et des restitutions. Les copies conservées hors site le sont dans des conditions équivalentes.

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.

4.1.7. Mise hors service des supports

Un support arrivé en fin de vie est effacé de manière irréversible ou détruit physiquement, selon la sensibilité des données qu'il a portées. L'opération est consignée dans un procès-verbal indiquant la date, la nature du support, la méthode employée et la fonction qui y a procédé.

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

4.1.8. Sauvegardes hors site

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

Les sauvegardes sont conservées sur le site secondaire dans des conditions de sécurité physique équivalentes à celles du site principal. Leur restauration est testée 1 fois par an, au minimum. 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.

4.2. Mesures de sécurité procédurales

4.2.1. Rôles de confiance

Les rôles de confiance suivants sont institués. Ils désignent des fonctions ; aucune personne physique n'est nommée dans le présent document.

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.

Rôle	Attributions
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.

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.

4.2.2. Nombre de personnes requises par tâches

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.

Tâche	Nombre minimal de personnes
Génération d'une bi-clé d'autorité	Cérémonie sous double contrôle, en présence de témoins, avec le quorum de 3 porteurs de parts de secret sur 5
Activation d'une clé privée d'autorité	Quorum de 3 sur 5, sous double contrôle
Sauvegarde ou restauration d'une clé d'autorité	Double contrôle et quorum identique
Révocation du certificat d'une composante	Deux personnes, dont le responsable de sécurité
Accès physique à la zone sensible	Deux personnes habilitées
Mise en production d'une évolution des systèmes	Deux personnes, dont le responsable d'application
Traitement d'une demande de révocation d'un certificat de titulaire	Une personne habilitée, l'opération étant journalisée et contrôlée a posteriori

4.2.3. Identification et authentification pour chaque rôle

Chaque titulaire d'un rôle de confiance dispose d'un compte nominatif ; les comptes partagés sont proscrits. L'accès aux systèmes de l'infrastructure est subordonné à une authentification à plusieurs facteurs, et les droits attribués sont strictement ceux du rôle exercé.

Les habilitations sont notifiées par écrit, revues périodiquement et retirées immédiatement à la fin de l'affectation. Toute action accomplie au titre d'un rôle de confiance est journalisée avec l'identifiant du compte, conformément au chapitre 4.4.1.

4.2.4. Rôles exigeant une séparation des attributions

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.

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.

4.3. Mesures de sécurité vis-à-vis du personnel

4.3.1. Qualifications, compétences et habilitations requises

Chaque rôle de confiance est tenu par une personne dont les compétences techniques et l'expérience sont adaptées aux attributions correspondantes, et qui a été formée à la présente politique, à la déclaration des pratiques et à la politique de sécurité. L'habilitation est prononcée par écrit, pour un rôle déterminé, et versée au dossier d'audit.

4.3.2. Procédures de vérification des antécédents

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.

La vérification est conduite avant l'affectation au rôle et renouvelée en cas de changement d'attributions. Les éléments recueillis sont conservés dans les conditions prévues par la loi n° 09-08 et ne figurent dans aucun document public.

4.3.3. Exigences en matière de formation initiale

Toute personne affectée à un rôle de confiance reçoit, avant sa prise de fonction, une formation portant sur les principes de l'infrastructure de gestion de clés, la présente politique, les procédures qui la concernent, la protection des données à caractère personnel et la conduite à tenir en cas d'incident. La formation est sanctionnée par une attestation versée au dossier.

4.3.4. Exigences et fréquence en matière de formation continue

Une formation continue est dispensée au moins une fois par an, ainsi qu'à chaque évolution significative des procédures, des systèmes ou du cadre réglementaire applicable. Le suivi de ces formations est enregistré.

4.3.5. Fréquence et séquence de rotation entre différentes attributions

Aucune rotation systématique n'est imposée : la taille de l'organisation en ferait une mesure de façade. La garantie recherchée est obtenue autrement, par la séparation des attributions du chapitre 4.2.4, par le double contrôle des opérations sensibles et par le contrôle indépendant du chapitre 7.

Tout changement d'attribution donne lieu au retrait immédiat des droits attachés au rôle quitté et à une nouvelle habilitation écrite pour le rôle pris.

4.3.6. Sanctions en cas d'actions non autorisées

Toute action non autorisée accomplie sur une composante de l'infrastructure entraîne la suspension immédiate des droits d'accès de la personne concernée, une analyse de l'incident selon le chapitre 4.7.1 et, le cas échéant, les suites disciplinaires et judiciaires prévues par la loi et par le contrat de travail ou de prestation.

Les faits établis sont consignés et conservés au dossier d'audit, et l'incident est traité comme tel s'il a une incidence sur le service ou sur les données conservées.

4.3.7. Exigences vis-à-vis du personnel des prestataires externes

Le personnel d'un prestataire externe intervenant sur une composante est soumis aux mêmes exigences de vérification, de formation, d'habilitation, de confidentialité et de journalisation que le personnel du prestataire. Ces exigences sont stipulées dans le contrat écrit qui lie le prestataire au tiers, lequel prévoit également les moyens de contrôle et les modalités d'établissement des preuves.

Une intervention en zone sensible s'effectue sous accompagnement permanent et sous double contrôle.

4.3.8. Documentation fournie au personnel

Chaque personne titulaire d'un rôle de confiance dispose de la présente politique, de la déclaration des pratiques de certification, des procédures opérationnelles de son rôle, de la politique de sécurité et de la procédure de gestion des incidents. La documentation est maîtrisée, versionnée, et sa diffusion est enregistrée.

4.4. Procédures de constitution des données d'audit

4.4.1. Type d'évènements à enregistrer

Les évènements suivants sont journalisés, avec la date et l'heure issues du système de datation du chapitre 5.8, l'identifiant de l'auteur et le résultat de l'opération.

- Cérémonies de clés : génération, sauvegarde, restauration, activation, désactivation et destruction d'une clé d'autorité.
- Réception, validation ou rejet d'une demande de certificat, avec le motif du rejet.
- Génération, délivrance, notification et acceptation d'un certificat.
- Génération, activation, désactivation et destruction des données de création de cachet d'un titulaire à l'intérieur du module cryptographique matériel.
- Réception, authentification et traitement d'une demande de révocation, et publication de l'information d'état correspondante.

- Production et publication de chaque liste de révocation, et fonctionnement du service d'information en ligne.
- Création, modification et suppression d'un compte, attribution et retrait d'une habilitation.
- Tentatives d'accès ou d'opération en échec, sur les systèmes comme sur les locaux.
- Démarrage, arrêt, alarme et anomalie des équipements de l'infrastructure, y compris les alarmes physiques du module cryptographique.
- Mise en production d'une évolution des systèmes, application d'un correctif, changement de configuration.
- Accès physique aux zones techniques et sensibles.

Un évènement journalisé porte l'information nécessaire à la reconstitution du fait ; il ne porte aucune donnée à caractère personnel non nécessaire, ni aucun élément secret.

4.4.2. Fréquence de traitement des journaux d'évènements

Traitement	Fréquence
Analyse complète des journaux d'évènements	1 fois par jour ouvré, et dès la détection d’une anomalie
Contrôle des tentatives en échec d'accès ou d'opération	toutes les 24 heures
Rapprochement des journaux entre composantes	1 fois par semaine

Toute anomalie détectée lors de ces traitements est traitée comme un incident selon le chapitre 4.7.1.

4.4.3. Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur le site pendant 1 mois, puis versés aux archives et conservés dans les conditions du chapitre 4.5.2.

4.4.4. Protection des journaux d'évènements

Les journaux sont protégés en intégrité et en confidentialité. Ils sont scellés, horodatés, et leur accès est restreint aux fonctions de responsable de sécurité et de contrôleur. Aucune fonction d'exploitation ne dispose du droit de les modifier ou de les supprimer.

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

4.4.5. Procédure de sauvegarde des journaux d'évènements

Les journaux sont sauvegardés selon la même périodicité que les autres données sensibles, chiffrés et conservés hors site. La restauration d'une sauvegarde de journaux est testée dans le cadre du test annuel du chapitre 4.7.4.

4.4.6. Système de collecte des journaux d'évènements

La collecte est automatique pour les évènements produits par les systèmes, et manuelle, sous la forme d'un procès-verbal signé, pour les évènements physiques et pour les cérémonies de clés. Les deux sources sont rapprochées selon la fréquence du chapitre 4.4.2.

4.4.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement

L'auteur d'une opération n'est pas notifié individuellement de son enregistrement : la journalisation est systématique et connue de tous, et son caractère exhaustif est porté à la connaissance du personnel lors de la formation initiale et par l'engagement de confidentialité signé.

Le titulaire est informé, dans les conditions générales d'utilisation applicables et dans la déclaration de divulgation YT-PDS-CERT, de la nature des données enregistrées à l'occasion du service et de leur durée de conservation.

4.4.8. Évaluation des vulnérabilités

Les journaux sont exploités pour détecter les tentatives d'atteinte à la sécurité. Une évaluation des vulnérabilités des composantes est conduite périodiquement et après toute évolution significative des systèmes ; les correctifs de sécurité sont appliqués selon un délai proportionné à la criticité de la vulnérabilité.

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.

4.5. Archivage des données

4.5.1. Types de données à archiver

- Les dossiers d'enregistrement, y compris les pièces produites, le résultat des contrôles d'identité et l'acceptation des conditions générales d'utilisation.
- Les certificats délivrés, les demandes de certificat et leur suite, ainsi que les acceptations recueillies.
- Les demandes de révocation, leur traitement et les listes de révocation produites.
- Les journaux d'évènements de l'ensemble des composantes.
- Les procès-verbaux de cérémonie de clés, de test de restauration et de destruction de support.
- Les versions successives de la présente politique, de la déclaration des pratiques et des conditions générales d'utilisation.
- Les rapports de contrôle et d'audit et les plans d'action correspondants.

4.5.2. Période de conservation des archives

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.

Cette durée procède des articles 18 et 23 du décret n° 2-22-687, l'article 23 rendant l'obligation de l'article 18 applicable aux prestataires fournissant des services de confiance autres que qualifiés.

4.5.3. Protection des archives

Les archives sont protégées en intégrité, en confidentialité et en disponibilité, pendant toute la durée de conservation. L'accès est restreint aux fonctions habilitées, nominatif et journalisé. Aucune archive n'est modifiable après versement.

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

4.5.4. Procédure de sauvegarde des archives

Les archives sont sauvegardées, chiffrées et conservées hors site selon le chapitre 4.1.8. Les supports d'archives sont contrôlés périodiquement et leur contenu est migré avant toute obsolescence du support ou du format, la migration étant elle-même journalisée.

4.5.5. Exigences d'horodatage des données

Chaque évènement archivé porte une date et une heure issues du système de datation du chapitre 5.8. Les dossiers de preuve dont la valeur probante doit être opposable sont en outre horodatés par le service d'horodatage électronique du prestataire, décrit par la politique d'horodatage YT-PH-TSA (1.3.6.1.4.1.[PEN].1.1.3).

4.5.6. Système de collecte des archives

Le versement aux archives est automatique pour les données produites par les systèmes et procède d'un dépôt contrôlé pour les pièces sur support matériel. Chaque versement est enregistré avec sa date, son origine et son empreinte d'intégrité.

4.5.7. Procédures de récupération et de vérification des archives

Une archive est restituée sur demande motivée d'une fonction habilitée, d'un titulaire justifiant de son identité pour ce qui le concerne, ou de l'autorité nationale dans l'exercice de ses attributions. Le délai maximal de récupération est de 2 jours ouvrés.

La vérification d'une archive porte sur son intégrité, sur son horodatage et sur la continuité de la chaîne de conservation ; le résultat de la vérification est consigné.

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.

4.6. Changement de clé d'AC

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.

Une nouvelle bi-clé d'autorité est générée en cérémonie, selon le chapitre 5.1.1.1, et le nouveau certificat d'autorité est publié dans le registre de publication du site institutionnel de YORYX TRUST au moins 24 heures avant sa première utilisation.

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

L'ancienne clé demeure utilisée, jusqu'à l'expiration du dernier certificat qu'elle a délivré, pour signer les listes de révocation correspondantes ; elle n'est détruite qu'après cette échéance, selon le chapitre 5.2.10.1.

4.7. Reprise suite à compromission et sinistre

4.7.1. Procédures de remontée et de traitement des incidents et des compromissions

Tout évènement susceptible de porter atteinte à la sécurité du service est signalé sans délai au responsable de sécurité, qualifié, tracé et traité selon une procédure écrite. La qualification détermine les mesures conservatoires immédiates, dont la révocation lorsqu'un doute pèse sur une clé.

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.

Chaque incident donne lieu à une analyse des causes, à un plan d'action daté et à une vérification de clôture, versés au dossier d'audit.

4.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)

La reprise s'appuie sur les sauvegardes chiffrées conservées hors site. La séquence de reprise est écrite, priorise le rétablissement de la fonction de gestion des révocations et de la fonction d'information sur l'état des certificats, et n'autorise la reprise de la délivrance qu'après vérification de l'intégrité des systèmes concernés.

Aucune donnée restaurée n'est mise en production sans vérification de son intégrité au regard des empreintes conservées.

4.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante

1. Le certificat de la composante est révoqué sans délai et l'information d'état est publiée immédiatement.
2. Les certificats délivrés par la composante compromise, encore en cours de validité, sont révoqués.
3. Les titulaires et les utilisateurs de certificats sont informés par le registre de publication du site institutionnel de YORYX TRUST.
4. L'autorité nationale est notifiée au titre de l'article 40 de la loi n° 43-20.
5. Une nouvelle bi-clé est générée en cérémonie et le nouveau certificat d'autorité est publié selon le chapitre 4.6.
6. Les titulaires concernés obtiennent un nouveau certificat selon le chapitre 3.7, sans frais.

4.7.4. Capacités de continuité d'activité suite à un sinistre

Un plan de continuité et de reprise d'activité est établi et testé 1 fois par an. 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.

La continuité repose sur les deux sites décrits au chapitre 4.1.1 : les fonctions de gestion des révocations et d'information sur l'état des certificats sont rétablies en priorité, dans les limites d'indisponibilité du chapitre 3.10.2.

4.8. Fin de vie de l'IGC

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 met en œuvre les mesures suivantes.

1. Informer préalablement l'autorité nationale, dans le délai fixé ci-dessus, ainsi que les titulaires et les utilisateurs de certificats par le registre de publication.
2. Cesser toute délivrance de nouveaux certificats à compter de la date annoncée.
3. Révoquer les certificats encore en cours de validité et publier l'information d'état correspondante, sauf reprise de l'activité par un autre prestataire.
4. Maintenir la fonction d'information sur l'état des certificats jusqu'à l'expiration du dernier certificat délivré.
5. Détruire les clés privées d'autorité selon le chapitre 5.2.10.1, sous procès-verbal.
6. Transférer ou conserver les archives pour la durée restant à courir au titre du chapitre 4.5.2, la conservation demeurant due après la cessation d'activité.

Le plan de cessation d'activité, qui détaille ces opérations et les moyens financiers qui leur sont affectés, est un document interne ; sa substance opposable au titulaire figure dans les conditions générales d'utilisation applicables.

5. MESURES DE SÉCURITÉ TECHNIQUES

5.1. Génération et installation de bi-clés

5.1.1. Génération des bi-clés

Toute bi-clé mise en œuvre au titre de la présente politique — bi-clé d'autorité comme bi-clé de titulaire — est générée à l'intérieur du module cryptographique matériel. Aucune bi-clé n'est générée sur un poste de travail, dans un environnement d'usage général ni par un composant logiciel non dédié.

5.1.1.1. Clés d'AC

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

La bi-clé de l'autorité racine YORYX TRUST Root CA G1 est générée puis conservée hors ligne ; activée uniquement le temps d’une cérémonie de clés, selon un script écrit et approuvé au préalable, sous double contrôle et en présence de témoins. Les bi-clés des autorités émettrices sont générées dans les mêmes conditions.

5.1.1.2. Clés porteurs générées par l'AC

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.

La génération intervient après validation du dossier d'enregistrement et sur ordre de la fonction de génération des certificats. Le module cryptographique matériel garantit que la génération est réalisée exclusivement par des utilisateurs autorisés et atteste de la robustesse cryptographique de la bi-clé produite.

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

5.1.1.3. Clés porteurs générées par le porteur

Sans objet : aucune bi-clé de titulaire n'est générée par le titulaire lui-même. Le modèle de service exclut la remise d'un support matériel et l'installation d'un logiciel de création de cachet sur le poste du titulaire ; la bi-clé est générée dans le module cryptographique matériel selon le chapitre 5.1.1.2.

5.1.1.4. Transmission de la clé privée à son propriétaire

Sans objet : aucune clé privée de titulaire n'est transmise, ni en clair, ni sous forme protégée. Les données de création de cachet demeurent à l'intérieur du module cryptographique matériel pendant tout leur cycle de vie ; le titulaire en dispose par l'exercice du contrôle exclusif décrit au chapitre 5.4, non par leur détention matérielle.

5.1.2. Transmission de la clé publique à l'AC

La clé publique du titulaire est produite par le module cryptographique matériel et transmise à la fonction de génération des certificats par un canal interne dont l'intégrité et l'authenticité de l'origine sont assurées. Aucune clé publique d'origine externe n'est acceptée.

5.1.3. Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les certificats des autorités de certification 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, et sont diffusés au moins 24 heures avant leur première utilisation.

L'utilisateur de certificat vérifie l'authenticité d'un certificat d'autorité par son empreinte, publiée dans le même registre, avant de l'installer comme ancre de confiance. Le guide YT-GUIDE-USE décrit cette vérification.

5.1.4. Tailles des clés

Bi-clé	Algorithme et taille	Algorithme de signature
Autorité racine YORYX TRUST Root CA G1	RSA 4096 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
Autorité émettrice YORYX TRUST Seal CA G1	RSA 4096 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
Répondeur d'information sur l'état des certificats	RSA 3072 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
Bi-clé de cachet d’un titulaire	RSA 3072 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)

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.

Ces tailles sont supérieures aux minima du plan de référence, rappelés aux annexes 9.5 et 9.6 ; la valeur la plus exigeante est retenue.

5.1.5. Vérification de la génération des paramètres des bi-clés et de leur qualité

La qualité des bi-clés repose sur le générateur d'aléa du module cryptographique matériel, qui met en œuvre les tests d'auto-vérification prévus par son profil de protection et entre dans un état sûr s'il détecte une erreur. Aucune bi-clé n'est utilisée si le module signale une anomalie lors de sa génération.

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.

5.1.6. Objectifs d'usage de la clé

L'usage de chaque bi-clé est borné par l'extension Key Usage du certificat correspondant, marquée critique, et par les domaines d'utilisation du chapitre 1.10. Une bi-clé de titulaire sert exclusivement à l’apposition d’un cachet électronique et n’est employée ni pour le chiffrement, ni pour l’authentification de serveur.

- Certificat d'autorité racine et d'autorité émettrice : keyCertSign et cRLSign.
- Certificat de répondeur d'information sur l'état des certificats : digitalSignature, avec le rôle étendu de signature de réponses d'état.
- Certificat de titulaire : contentCommitment, à l’exclusion de tout autre bit.

5.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

5.2.1. Standards et mesures de sécurité pour les modules cryptographiques

5.2.1.1. Modules cryptographiques de l'AC

Le module cryptographique matériel employé pour générer et mettre en œuvre les clés d'autorité présente les propriétés suivantes.

- les bi-clés d’autorité et les données de création de cachet des titulaires 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

Il vise la conformité aux textes suivants.

- 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.

> **Point ouvert —** 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.

5.2.1.2. Dispositifs de création de cachet des titulaires

Aucun dispositif matériel n'est remis à la personne morale : la fonction de création de cachet est assurée, pour son compte et sous son contrôle, par le module cryptographique matériel exploité par le prestataire. Les objectifs de sécurité auxquels ce dispositif répond sont énoncés à l'annexe 9.1.2.

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.

5.2.2. Contrôle de la clé privée par plusieurs personnes

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.

Ce contrôle multiple porte sur les clés d'autorité. Il ne s'applique pas aux données de création de cachet des titulaires, dont la mise en œuvre relève au contraire du contrôle exclusif du seul titulaire, décrit au chapitre 5.4.

5.2.3. Séquestre de la clé privée

Sans objet : aucune clé privée, d'autorité ou de titulaire, n'est mise sous séquestre. Le chapitre 3.12.1 en énonce le motif : les données de création de cachet ne servent jamais au chiffrement, de sorte que leur perte n'entraîne la perte d'aucune donnée.

5.2.4. Copie de secours de la clé privée

Les clés privées d'autorité font l'objet d'une sauvegarde chiffrée, conservée dans les conditions du chapitre 4.1.6 ; leur restauration est soumise au quorum du chapitre 4.2.2 et donne lieu à un procès-verbal.

Les données de création de cachet des titulaires font l'objet, à l'intérieur du dispositif de sauvegarde du module cryptographique matériel, d'une sauvegarde chiffrée dont la restauration s'effectue exclusivement vers un module du même type et sous le même quorum. À aucun moment ces données n'existent en clair hors du module.

5.2.5. Archivage de la clé privée

Sans objet : aucune clé privée n'est archivée. Une clé privée arrivée en fin de vie est détruite selon le chapitre 5.2.10 ; seules sont archivées les clés publiques et les certificats, selon le chapitre 5.3.1.

5.2.6. Transfert de la clé privée vers/depuis le module cryptographique

Aucune clé privée n'est transférée en clair vers le module cryptographique matériel ni depuis celui-ci. Les clés y sont générées et y demeurent ; elles sont non exportables et non extractibles.

Le seul transfert admis est celui d'une sauvegarde chiffrée entre modules de même type, dans le cadre du chapitre 5.2.4, sous double contrôle et sous quorum.

5.2.7. Stockage de la clé privée dans un module cryptographique

Toute clé privée mise en œuvre au titre de la présente politique est stockée à l'intérieur du module cryptographique matériel. Celui-ci détecte les tentatives d'altération physique et entre dans un état sûr lorsqu'une tentative est détectée.

5.2.8. Méthode d'activation de la clé privée

5.2.8.1. Clés privées d'AC

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.

L'activation intervient au commencement d'une session d'exploitation ou d'une cérémonie et est journalisée ; la clé de l'autorité racine n'est activée que le temps de la cérémonie.

5.2.8.2. Clés privées des porteurs

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.

5.2.9. Méthode de désactivation de la clé privée

5.2.9.1. Clés privées d'AC

La clé privée d'une autorité est désactivée à la fin de la session d'exploitation ou de la cérémonie, ainsi qu'à l'arrêt du module ou sur détection d'une anomalie. La désactivation est journalisée.

5.2.9.2. Clés privées des porteurs

La capacité d'usage des données de création de cachet cesse à la fin de chaque opération : elle n'est pas maintenue d'une opération à l'autre. Elle cesse également, définitivement, à l'expiration ou à la révocation du certificat correspondant, ainsi qu'à la fin de la relation avec le titulaire.

5.2.10. Méthode de destruction des clés privées

5.2.10.1. Clés privées d'AC

Une clé privée d'autorité est détruite à l'intérieur du module cryptographique matériel, sous le quorum du chapitre 4.2.2 et en présence de témoins, après expiration du dernier certificat ou de la dernière liste de révocation qu'elle avait à signer. La destruction porte également sur les sauvegardes chiffrées correspondantes et donne lieu à un procès-verbal signé versé au dossier d'audit.

5.2.10.2. Clés privées des porteurs

Les données de création de cachet d'un titulaire sont détruites à l'intérieur du module cryptographique matériel, ainsi que leurs sauvegardes chiffrées, à l'expiration ou à la révocation du certificat correspondant, ou à la fin de la relation avec le titulaire. L'opération est journalisée selon le chapitre 4.4.1.

5.2.11. Niveau d'évaluation sécurité du module cryptographique

Le niveau d'évaluation visé est celui énoncé au chapitre 5.2.1.1 et rappelé à l'annexe 9.1.1.

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.

5.3. Autres aspects de la gestion des bi-clés

5.3.1. Archivage des clés publiques

Les clés publiques et les certificats correspondants sont archivés selon le chapitre 4.5 et conservés pendant 7 ans au moins après l'expiration du certificat. Cette conservation est la condition de la vérification différée des cachets électroniques produits pendant la période de validité.

5.3.2. Durées de vie des bi-clés et des certificats

Bi-clé et certificat	Durée de vie
Autorité racine YORYX TRUST Root CA G1	10 ans
Autorité émettrice YORYX TRUST Seal CA G1	6 ans
Répondeur d'information sur l'état des certificats	1 an
Certificat de titulaire — niveau simple	1 an
Certificat de titulaire — niveau avancé	3 ans

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.

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.

La durée de vie d'une bi-clé de titulaire est celle du certificat qui la porte : la bi-clé n'est jamais réutilisée pour un certificat postérieur, conformément au chapitre 3.6.

5.4. Données d'activation

5.4.1. Génération et installation des données d'activation

5.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC

Les parts de secret servant à l'activation des clés d'autorité sont générées au cours de la cérémonie de clés, à l'intérieur du module cryptographique matériel, et remises individuellement aux porteurs de parts de secret désignés par leur fonction. 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.

5.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du porteur

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.

Les moyens d’authentification des systèmes de la personne morale sont enrôlés par le représentant légal ou par le mandataire habilité, après vérification de leur identité et de leurs pouvoirs ; leur administration au sein de la personne morale relève de celle-ci, le prestataire n’en conservant que les éléments de vérification.

5.4.2. Protection des données d'activation

5.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC

Chaque part de secret est protégée par son porteur dans les conditions du chapitre 4.1.6 ; un porteur ne détient qu'une seule part, et la reconstitution du secret exige la réunion du quorum. La perte d'une part donne lieu à une nouvelle répartition du secret, sous cérémonie.

5.4.2.2. Protection des données d'activation correspondant aux clés privées des porteurs

Les facteurs d'authentification du titulaire ne sont connus que de lui ; le prestataire n'en conserve que les éléments de vérification, sous une forme qui ne permet pas de les reconstituer. Un facteur perdu ou compromis est révoqué et remplacé par un nouvel enrôlement, sans que les données de création de cachet en soient affectées.

Perdre un moyen d’authentification ne fait perdre aucune donnée de création de cachet : cela révoque ce moyen, que la personne morale titulaire réenrôle.

5.4.3. Autres aspects liés aux données d'activation

Le nombre de tentatives d'authentification en échec est limité ; leur dépassement bloque temporairement l'accès au service, produit un évènement journalisé et déclenche le contrôle prévu au chapitre 4.4.2.

Aucune donnée d'activation n'est transmise par un canal non protégé, ni consignée dans un journal, ni communiquée à un tiers.

5.5. Mesures de sécurité des systèmes informatiques

5.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

- Les systèmes de l'infrastructure sont dédiés à cette fonction et ne portent aucun service étranger à celle-ci.
- Les comptes sont nominatifs, les droits attribués selon le rôle exercé, et l'accès est subordonné à une authentification à plusieurs facteurs.
- Les flux entre composantes sont authentifiés et protégés en intégrité et en confidentialité.
- Les configurations sont maîtrisées, versionnées et vérifiées ; toute évolution est validée avant mise en production selon le chapitre 4.2.2.
- Les correctifs de sécurité sont appliqués selon un délai proportionné à la criticité de la vulnérabilité corrigée.
- La journalisation du chapitre 4.4.1 est activée sur l'ensemble des systèmes et son intégrité est protégée.

5.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Aucune évaluation certifiée n'est revendiquée pour les systèmes informatiques autres que le module cryptographique. Le niveau de sécurité de ces systèmes est établi par les mesures du chapitre 5.5.1 et vérifié par les contrôles du chapitre 7.

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.

5.6. Mesures de sécurité liées au développement des systèmes

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.

Les développements et les paramétrages sont maîtrisés : gestion de versions, revue par une seconde personne, jeux d'essai dépourvus de données réelles, validation en environnement de recette et mise en production sous double contrôle. La traçabilité entre une évolution demandée, sa validation et sa mise en production est conservée.

Les composants tiers employés sont inventoriés et suivis en vulnérabilité ; leur mise à jour suit la règle du chapitre 5.5.1.

5.7. Mesures de sécurité réseau

Les composantes de l'infrastructure sont isolées des réseaux d'usage général. Les zones réseau sont segmentées selon le zonage physique du chapitre 4.1.2, et les flux autorisés sont limités à ceux nécessaires au service, filtrés et journalisés.

Le module cryptographique matériel n'est accessible qu'aux composantes qui en ont l'usage, par des interfaces dédiées et authentifiées. Les fonctions publiques — publication, information sur l'état des certificats — sont exposées par des composantes distinctes de celles qui mettent en œuvre les clés d'autorité.

Les accès d'administration à distance sont proscrits depuis un réseau non maîtrisé ; toute intervention distante s'effectue par un canal authentifié, chiffré et journalisé, sous double contrôle pour les opérations sensibles.

5.8. Horodatage / Système de datation

Les évènements journalisés et les certificats délivrés portent une date et une heure issues d'une source de temps de confiance, synchronisée sur le temps universel coordonné et surveillée ; une perte de synchronisation est détectée et traitée comme un incident selon le chapitre 4.7.1.

Le système de datation interne ne produit pas de jetons d'horodatage opposables aux tiers. Lorsqu'une preuve horodatée opposable est nécessaire, notamment pour les dossiers de preuve du chapitre 4.5.5, le service d'horodatage électronique du prestataire est employé ; il fait l'objet de la politique d'horodatage YT-PH-TSA (1.3.6.1.4.1.[PEN].1.1.3), dont les exigences propres — exactitude, source de temps, profil du jeton — ne sont pas reprises ici.

6. PROFIL DES CERTIFICATS ET DES LCR

6.1. Profil des certificats

Les certificats délivrés sont des certificats X.509 version 3 conformes à la norme IETF RFC 5280. Le détail des champs de base et des extensions figure aux annexes 9.3, pour les certificats d'autorité, et 9.4, pour les certificats de titulaires ; le présent chapitre en donne la synthèse.

Certificat et sujet	Nom distinctif	Clé	Validité	Key Usage
YORYX TRUST Root CA G1 Autorité de certification racine, hors ligne	C=MA, O=YORYX TRUST SASU, organizationIdentifier=NTRMA-184667, CN=YORYX TRUST Root CA G1	RSA 4096 bits	10 ans	keyCertSign, cRLSign (critique)
YORYX TRUST Seal CA G1 autorité de certification émettrice des certificats de cachet électronique	C=MA, O=YORYX TRUST SASU, organizationIdentifier=NTRMA-184667, CN=<nom de l’autorité émettrice>	RSA 4096 bits	6 ans	keyCertSign, cRLSign (critique)
Certificat de titulaire — niveau simple Sujet : personne morale	C=MA, O=<dénomination de la personne morale>, organizationIdentifier=<NTRMA-|ICE- suivi de l’identifiant officiel>, CN=<nom du cachet>	RSA 3072 bits	1 an	contentCommitment (critique)
Certificat de titulaire — niveau avancé Sujet : personne morale	C=MA, O=<dénomination de la personne morale>, organizationIdentifier=<NTRMA-|ICE- suivi de l’identifiant officiel>, CN=<nom du cachet>	RSA 3072 bits	3 ans	contentCommitment (critique)

L'extension certificatePolicies d'un certificat de titulaire porte l'identifiant de la politique correspondant au niveau sous lequel il a été délivré — 1.3.6.1.4.1.[PEN].1.1.2.1 pour le niveau simple, 1.3.6.1.4.1.[PEN].1.1.2.2 pour le niveau avancé — ainsi que l'identifiant de la politique de référence ETSI correspondante, 0.4.0.2042.1.3 pour le niveau simple et 0.4.0.2042.1.2 pour le niveau avancé.

L'exigence 6 du référentiel [Ref_Serv_Conf_NonQual] rappelle que le certificat sur lequel repose le cachet électronique avancé doit être conforme à la norme ETSI EN 319 411-1 ou ETSI EN 319 411-2, et qu'il doit reposer au minimum sur un certificat de type LCP, un certificat de type NCP,

NCP+ ou QCP demeurant admis. Le niveau avancé de la présente politique se place au niveau NCP+.

Les extensions CRL Distribution Points et Authority Information Access sont présentes dans tout certificat délivré et désignent respectivement le point de publication de la liste de révocation applicable et le point d'accès au service d'information en ligne sur l'état des certificats. 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.

Aucune extension propriétaire n'est employée, et aucune extension non prévue par le profil de l'annexe 9.4 n'est ajoutée sans révision de la présente politique.

6.2. Profil des LCR

Les listes de révocation sont conformes à la norme IETF RFC 5280, version 2. Elles portent les champs suivants.

Champ	Valeur
Version	v2
Signature	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
Issuer	Le nom distinctif de l'autorité qui produit la liste, identique à celui de son certificat
thisUpdate	Date et heure de production de la liste
nextUpdate	Date de production augmentée de 72 heures
revokedCertificates	Numéro de série, date de révocation et, le cas échéant, code de motif de chaque certificat révoqué
Extension CRL Number	Numéro d'ordre strictement croissant, sans réutilisation
Extension Authority Key Identifier	Identifiant de la clé publique de l'autorité qui signe la liste

La liste des certificats révoqués délivrés par YORYX TRUST Seal CA G1 est produite selon la fréquence du chapitre 3.9.7 ; la liste des autorités révoquées, produite par l'autorité racine, l'est tous les 6 mois, et à chaque révocation d’un certificat d’autorité émettrice.

Chaque liste de révocation est publiée dans les 30 minutes suivant sa génération et reste accessible sans contrôle d’accès ni frais. Sans objet : les listes de révocation delta ne sont pas mises en œuvre. La liste de révocation complète est publiée au moins toutes les 24 heures, ce qui rend l’incrément sans effet utile au volume d’émission déclaré.

Une entrée n'est jamais retirée d'une liste de révocation avant l'expiration du certificat qu'elle concerne : le retrait anticipé reviendrait à faire réapparaître comme valide un certificat révoqué.

7. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

7.1. Fréquences et/ou circonstances des évaluations

Évaluation	Fréquence ou circonstance
Contrôle de conformité interne	1 fois par an
Audit externe indépendant	tous les 2 ans
Test du plan de continuité et de reprise	1 fois par an
Test de restauration des sauvegardes	1 fois par an, au minimum
Évaluation préalable à une demande d'agrément	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.
Évaluation exceptionnelle	Après tout incident de sécurité majeur, toute compromission d'une clé d'autorité, toute évolution substantielle de l'architecture ou des procédures, et sur demande de l'autorité nationale

Le contrôle interne porte 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. L'audit externe consiste en un 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.

7.2. Identités des auditeurs

Le contrôle interne est conduit par le contrôleur, fonction instituée au chapitre 4.2.1, dont la compétence et l'indépendance à l'égard des composantes contrôlées sont établies avant sa désignation.

L'audit externe est conduit par un organisme disposant d'une compétence établie en matière d'infrastructures de gestion de clés et de services de confiance. Aucun auditeur n'est désigné nominativement dans le présent document, la désignation relevant d'une décision documentée versée au dossier d'audit.

L’évaluation de conformité est réalisée, aux frais du demandeur, par un organisme désigné à cet effet par l’autorité nationale (article 14 du décret n° 2-22-687).

7.3. Relations entre auditeur et entités évaluées

L'auditeur externe n'a pris part ni à la conception, ni à la réalisation, ni à l'exploitation des composantes qu'il évalue, et n'entretient avec le prestataire aucune relation de nature à compromettre son jugement. Le contrôleur interne relève de la règle de séparation des attributions du chapitre 4.2.4.

L'auditeur dispose d'un accès à l'ensemble des documents, journaux, archives et locaux nécessaires à sa mission, dans le respect des obligations de confidentialité auxquelles il est lui-même tenu par écrit.

7.4. Sujets couverts par les évaluations

- La conformité de la déclaration des pratiques de certification à la présente politique.
- La conformité des opérations effectivement conduites à la déclaration des pratiques.
- Les mesures de sécurité physiques, procédurales et techniques des chapitres 4 et 5.
- La gestion du cycle de vie des clés d'autorité et des clés de titulaires.
- Le respect des délais de traitement des révocations et des engagements de disponibilité du chapitre 3.10.2.
- La complétude, l'intégrité et la protection des journaux d'évènements et des archives.
- L'exercice des fonctions d'autorité d'enregistrement par la plateforme et le respect du contrat écrit qui l'encadre.
- Le traitement des données à caractère personnel au regard de la loi n° 09-08.
- Le suivi des plans d'action issus des évaluations précédentes.

7.5. Actions prises suite aux conclusions des évaluations

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.

Un écart affectant la vérification d'identité, la protection des clés ou la fonction de révocation est traité en priorité et fait l'objet d'une mesure conservatoire immédiate lorsque la sécurité des titulaires ou des utilisateurs de certificats l'exige.

7.6. Communication des résultats

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.

Un titulaire ou un utilisateur de certificat qui justifie d'un intérêt peut obtenir communication d'une synthèse attestant de la tenue et de la portée des contrôles, à l'exclusion de tout élément dont la divulgation affaiblirait les mesures de sécurité.

8. AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

Les stipulations opposables au titulaire et à l'utilisateur de certificat — obligations, limites d'usage, responsabilité, protection des données à caractère personnel, réclamations, droit applicable et juridiction — figurent dans les conditions générales d'utilisation applicables (YT-CGU-PM) et dans la déclaration de divulgation YT-PDS-CERT. Le présent chapitre traite de la vie de la politique elle-même.

Le droit applicable est le droit marocain ; tout litige relève des tribunaux compétents de Marrakech. 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.

Le traitement des données à caractère personnel opéré à l'occasion du service est soumis à la loi n° 09-08 ; le prestataire s'astreint aux obligations rappelées par l'exigence 17 du référentiel [Ref_Serv_Conf_NonQual] et met en œuvre les moyens permettant l'exercice des droits d'accès, de rectification et d'opposition.

> **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.

Toute réclamation relative à l'application de la présente politique est traitée selon la procédure publiée sous l'identifiant YT-COMPLAINTS ; les tarifs des services couverts figurent sous l'identifiant YT-PRICING.

8.1. Durée et fin anticipée de validité de la PC

8.1.1. Durée de validité

La présente politique entre en vigueur à la date de sa publication dans le registre de publication du site institutionnel de YORYX TRUST et demeure applicable jusqu'à la publication d'une version postérieure ou jusqu'à sa fin anticipée. 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).

Elle demeure opposable, pour chaque certificat, dans la version en vigueur à la date de délivrance de celui-ci ; les versions antérieures restent accessibles pendant la durée de conservation des archives fixée au chapitre 4.5.2.

8.1.2. Fin anticipée de validité

La présente politique prend fin par anticipation dans trois cas : la cessation du service qu'elle régit, une évolution réglementaire qui la rendrait contraire au droit applicable, ou une décision de l'autorité nationale.

Dans chacun de ces cas, l'information est publiée dans le registre de publication du site institutionnel de YORYX TRUST, les titulaires en sont avisés, et les certificats en cours de validité sont soit maintenus jusqu'à leur terme sous la politique en vigueur à leur délivrance, soit révoqués selon le chapitre 4.8 lorsque la cause de la fin anticipée l'impose.

La fin de la politique n'éteint ni l'obligation de conservation du chapitre 4.5.2, ni l'obligation de maintenir la fonction d'information sur l'état des certificats jusqu'à l'expiration du dernier certificat délivré.

9. ANNEXES

9.1. Exigences de sécurité

9.1.1. Exigences sur les objectifs de sécurité du module cryptographique

Le module cryptographique matériel employé par l'autorité de certification pour générer et mettre en œuvre ses clés de signature, ainsi que pour générer les données de création de cachet des titulaires, répond aux objectifs de sécurité suivants.

- Garantir que la génération des bi-clés des titulaires est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés produites.
- Assurer la confidentialité des données de création de cachet des titulaires et l'intégrité de leurs bi-clés pendant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie.
- Assurer la confidentialité et l'intégrité des clés privées de signature des autorités durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie.
- Être capable d'identifier et d'authentifier ses utilisateurs.
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné.
- Être capable de mener une série de tests pour vérifier son bon fonctionnement et entrer dans un état sûr s'il détecte une erreur.
- Permettre de produire une signature qui ne révèle pas la clé privée et qui ne peut être falsifiée sans la connaissance de celle-ci.
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité.
- Garantir, lorsqu'une fonction de sauvegarde et de restauration des clés privées est offerte, la confidentialité et l'intégrité des données sauvegardées, et exiger au minimum un double contrôle des opérations de sauvegarde et de restauration.
- Détecter les tentatives d'altération physique et entrer dans un état sûr lorsqu'une tentative est détectée.

Textes visés en cible pour ces objectifs :

- 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.

9.1.2. Exigences sur les objectifs de sécurité du dispositif de création de cachet

Le dispositif de création de cachet, mis en œuvre pour le compte de la personne morale titulaire à l’intérieur du module cryptographique matériel, répond aux objectifs de sécurité suivants.

- Garantir que la génération de la bi-clé est réalisée exclusivement par des utilisateurs autorisés et garantir sa robustesse cryptographique.

- Détecter les défauts lors des phases d'initialisation, de personnalisation et d'exploitation, et disposer de techniques sûres de destruction de la clé privée.
- Garantir la confidentialité et l'intégrité des données de création de cachet.
- Assurer la correspondance entre la clé privée et la clé publique.
- Produire un cachet électronique qui ne peut être falsifié sans la connaissance de la clé privée.
- Assurer la fonction de cachet pour la seule personne morale titulaire, après une authentification forte de ses systèmes, et protéger la clé privée contre toute utilisation par un tiers.
- Garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

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.

9.2. Variable de temps et niveaux de sécurité

Les exigences temporelles de la présente politique sont récapitulées ci-dessous. La colonne « Chapitre » renvoie à la disposition qui les énonce ; en cas d'écart apparent, la disposition prévaut sur le récapitulatif.

Variable	Description	Valeur	Chapitre
F_CONFORM	Fréquence de contrôle de conformité de l'ensemble de l'infrastructure	1 fois par an	7.1
F_JOUR_ANA	Fréquence d'analyse complète des journaux d'évènements	1 fois par jour ouvré, et dès la détection d’une anomalie	4.4.2
F_JOUR_ECH	Fréquence de contrôle des journaux pour identification des tentatives en échec	toutes les 24 heures	4.4.2
F_JOUR_RAP	Fréquence de rapprochement des journaux d'évènements	1 fois par semaine	4.4.2
F_PUB_LCR	Fréquence de publication des listes de révocation	24 heures	3.9.7
F_PUB_dLCR	Fréquence de publication des listes de révocation delta	non mise en œuvre	3.9.11
F_TEST_PLAN	Fréquence de test du plan de continuité	1 fois par an	4.7.4
T_AC_DISP	Disponibilité des systèmes publiant les certificats d'autorité	24 heures sur 24, 7 jours sur 7	3.10.2
T_AC_INDISP	Indisponibilité maximale par interruption de ces systèmes	1 heure	3.10.2

Variable	Description	Valeur	Chapitre
T_AC_MAX	Indisponibilité maximale mensuelle de ces systèmes	4 heures	3.10.2
T_C_AC_MAX	Durée de vie maximale d'un certificat d'autorité	10 ans	5.3.2
T_CESS	Délai minimum d'information en cas de cessation d'activité programmée	2 mois	4.8
T_DIFF_AC	Délai de diffusion préalable des certificats d'autorité	24 heures	5.1.3
T_ETAT_DISP	Disponibilité de la fonction d'information sur l'état des certificats	24 heures sur 24, 7 jours sur 7	3.10.2
T_ETAT_INDISP	Indisponibilité maximale par interruption de cette fonction	1 heure	3.10.2
T_ETAT_MAX	Indisponibilité maximale mensuelle de cette fonction	4 heures	3.10.2
T_INF_DISP	Disponibilité de la fonction de publication des autres informations	jours ouvrés	3.10.2
T_INF_INDISP	Indisponibilité maximale par interruption de cette fonction	8 heures (jours ouvrés)	3.10.2
T_INF_MAX	Indisponibilité maximale mensuelle de cette fonction	32 heures (jours ouvrés)	3.10.2
T_JOUR_SITE	Délai de conservation des journaux d'évènements sur site avant archivage	1 mois	4.4.3
T_PORT_MAX	Durée de vie maximale d'une bi-clé et d'un certificat de titulaire	3 ans	5.3.2
T_PORT_MIN	Durée de vie minimale, hors révocation, d'une bi-clé et d'un certificat de titulaire	1 an	5.3.2
T_PUB_LCR	Délai maximum de publication d'une liste de révocation après sa génération	30 minutes	3.9.8
T_REC_ARCH	Délai maximum de récupération des archives	2 jours ouvrés	4.5.7
T_REV_DISP	Disponibilité de la fonction de gestion des révocations	24 heures sur 24, 7 jours sur 7	3.10.2
T_REV_INDISP	Indisponibilité maximale par interruption de cette fonction	30 minutes	3.10.2

Variable	Description	Valeur	Chapitre
T_REV_MAX	Indisponibilité maximale mensuelle de cette fonction	2 heures	3.10.2
T_TRAIT_REV	Délai maximum de traitement d'une demande de révocation	24 heures	3.9.5.1
T_ARCH	Durée de conservation des données relatives à la fourniture du service	7 ans	4.5.2

Lorsqu'une valeur ci-dessus est plus exigeante que celle du plan de référence de la DGSSI, c'est la valeur la plus exigeante qui est retenue ; l'écart et sa justification figurent dans le registre des décisions de conception du prestataire.

9.3. Détails sur le gabarit d'un certificat racine

Le tableau ci-dessous précise les champs de base d'un certificat d'autorité de certification, qui respecte par ailleurs les exigences de la norme IETF RFC 5280.

Champ	Exigence
Version	La valeur de ce champ est « 2 », indiquant un certificat de version 3.
Serial number	Numéro de série non prévisible et unique au sein du domaine de l'autorité émettrice.
Signature	Voir l'annexe 9.5 : sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256).
Issuer	Nom distinctif de l'autorité émettrice ; pour l'autorité racine, identique au champ Subject, le certificat étant auto-signé.
Validity	10 ans pour l'autorité racine, 6 ans pour une autorité émettrice.
Subject	C=MA, O=YORYX TRUST SASU, organizationIdentifier=NTRMA-184667, CN=YORYX TRUST Root CA G1
Subject Public Key Info	Voir l'annexe 9.5 : RSA 4096 bits.
Unique Identifiers	Non utilisés, l'unicité des noms distinctifs étant imposée par le chapitre 2.1.3.

Extensions d'un certificat d'autorité :

Extension	Obligatoire	Critique	Exigence
Basic Constraints	Oui	Oui	cA à vrai ; le champ pathLenConstraint borne la profondeur de la hiérarchie.

Extension	Obligatoire	Critique	Exigence
Key Usage	Oui	Oui	keyCertSign et cRLSign ; les autres bits sont à zéro.
Subject Key Identifier	Oui	Non	Identifiant de la clé publique du certificat.
Authority Key Identifier	Oui pour tout certificat non auto-signé	Non	Identifiant de la clé publique de l'autorité émettrice.
Certificate Policies	Oui pour une autorité émettrice	Non	Identifiants des politiques sous lesquelles l'autorité délivre, soit 1.3.6.1.4.1.[PEN].1.1.2.1 et 1.3.6.1.4.1.[PEN].1.1.2.2.
CRL Distribution Points	Oui pour tout certificat non auto-signé	Non	Point de publication de la liste des autorités révoquées.
Authority Information Access	Oui pour une autorité émettrice	Non	Point d'accès au service d'information en ligne sur l'état des certificats.
Subject Alternative Name, Issuer Alternative Name	Non	Non	Peuvent être présents ; marqués non critiques.

Les extensions traitées par la norme IETF RFC 5280 et non reprises ci-dessus respectent strictement les exigences de cette norme.

9.4. Détails sur le gabarit d'un certificat porteur

Le tableau ci-dessous précise les champs de base d'un certificat de cachet électronique, qui respecte par ailleurs les exigences de la norme IETF RFC 5280.

Champ	Exigence
Version	La valeur de ce champ est « 2 », indiquant un certificat de version 3.
Serial number	Numéro de série non prévisible et unique au sein du domaine de l'autorité émettrice.
Signature	Voir l'annexe 9.6 : sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256).
Issuer	Nom distinctif de YORYX TRUST Seal CA G1, identique à celui porté par le champ Subject de son certificat.
Validity	1 an au niveau simple, 3 ans au niveau avancé.

Champ	Exigence
Subject	C=MA, O=<dénomination de la personne morale>, organizationIdentifier=<NTRMA-|ICE- suivi de l'identifiant officiel>, CN=<nom du cachet>
Subject Public Key Info	Voir l'annexe 9.6 : RSA 3072 bits.
Unique Identifiers	Non utilisés, l'unicité des noms distinctifs étant imposée par le chapitre 2.1.3.

Extensions d'un certificat de cachet électronique :

Extension	Obligatoire	Critique	Exigence
Key Usage	Oui	Oui	Le bit contentCommitment est à « 1 » ; tous les autres bits sont à « 0 », ce qui interdit techniquement tout usage autre que l'apposition d'un cachet.
Certificate Policies	Oui	Non	Identifiant de la politique du niveau délivré (1.3.6.1.4.1.[PEN].1.1.2.1 ou 1.3.6.1.4.1.[PEN].1.1.2.2) et identifiant de la politique ETSI de référence correspondante (0.4.0.2042.1.3 ou 0.4.0.2042.1.2).
Authority Key Identifier	Oui	Non	Identifiant de la clé publique de l'autorité émettrice.
Subject Key Identifier	Oui	Non	Identifiant de la clé publique du certificat.
Basic Constraints	Oui	Oui	cA à faux : un certificat de titulaire ne certifie aucun autre certificat.
CRL Distribution Points	Oui	Non	Point de publication de la liste de révocation applicable.
Authority Information Access	Oui	Non	Point d'accès au service d'information en ligne sur l'état des certificats.
Extended Key Usage	Non	Non	Non employée : la limitation d'usage résulte de l'extension Key Usage et du chapitre 1.10.
Subject Alternative Name	Non	Non	Peut être présent et marqué non critique ; il ne porte aucune information relative à la personne morale qui n'aurait pas été vérifiée par l'autorité d'enregistrement.

Le champ Subject porte la dénomination de la personne morale, son identifiant officiel et le nom du cachet. Aucune donnée à caractère personnel relative à une personne physique n'y figure : ni le nom du représentant légal, ni celui d'un administrateur des systèmes.

Les extensions traitées par la norme IETF RFC 5280 et non reprises ci-dessus respectent strictement les exigences de cette norme ; aucune extension propriétaire n'est employée.

9.5. Algorithmes de signature et taille de clés des AC

Autorité	Algorithme et taille de clé	Algorithme de signature	Empreinte
YORYX TRUST Root CA G1	RSA 4096 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)	SHA-256
YORYX TRUST Seal CA G1	RSA 4096 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)	SHA-256
Répondeur d'information sur l'état des certificats	RSA 3072 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)	SHA-256

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.

Le plan de référence de la DGSSI fixe pour les autorités un minimum de RSA 2048 bits et une empreinte SHA-224 ou SHA-256 ; les valeurs retenues ci-dessus sont supérieures à ce minimum, une clé de 2048 bits protégeant une autorité pendant 10 ans étant en deçà de ce que recommande la norme ETSI TS 119 312 pour des clés en service au-delà de 2030.

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.

9.6. Algorithmes et longueurs de clés des porteurs

Élément	Valeur
Algorithme et taille de clé	RSA 3072 bits
Algorithme de signature	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
Fonction d'empreinte minimale	SHA-256
Algorithmes proscrits	MD5, SHA-1 et toute longueur de clé RSA inférieure à 2048 bits sont proscrits.

Élément	Valeur
Formats admis pour les cachets électroniques avancés	PAdES (ETSI EN 319 142-1) ; XAdES (ETSI EN 319 132-1) ; CAdES (ETSI EN 319 122-1)
Conteneurs associés	ASiC (ETSI EN 319 162-1)

Le plan de référence fixe pour les titulaires un minimum de RSA 2048 bits ; la valeur retenue lui est supérieure et ne coûte rien au titulaire, la bi-clé étant générée à l'intérieur du module cryptographique matériel et n'étant manipulée par lui à aucun moment.

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

9.7. Documents de références

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.

[DECRET 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.

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

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.

Normes et spécifications visées.

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

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

ETSI EN 319 411-2, version V2.6.1 — Policy and security requirements for Trust Service Providers issuing certificates — Part 2: Requirements for trust service providers issuing EU qualified certificates.

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

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

ETSI TS 119 431-1, version V1.2.1 — Policy and security requirements for trust service providers — Part 1: TSP service components operating a remote QSCD / SCDev.

ETSI TS 119 431-2, version V1.2.1 — Policy and security requirements for trust service providers — Part 2: TSP service components supporting AdES digital signature creation.

ETSI TS 119 432, version V1.3.1 — Protocols for remote digital signature creation.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Documents du registre de publication cités par la présente politique.

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

YT-PH-TSA (1.3.6.1.4.1.[PEN].1.1.3) — Politique d'horodatage.

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

YT-CGU-PP (1.3.6.1.4.1.[PEN].1.4.1) — Conditions générales d'utilisation, personne physique.

YT-CGU-PM (1.3.6.1.4.1.[PEN].1.4.2) — Conditions générales d'utilisation, personne morale.

YT-FORM-LEGAL-REP — Formulaire d’enregistrement du représentant légal.

YT-FORM-REVOCATION — Formulaire de demande de révocation.

YT-FORM-MANDATE — Mandat et autorisation de retrait.

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.

YT-COMPLAINTS — Procédure de réclamation.

YT-PRICING — Tarifs.

9.8. Plan type détaillé d'une politique d'horodatage

Le plan de référence de la DGSSI place en annexe le plan type détaillé d'une politique d'horodatage. Cette matière ne relève pas de la présente politique : le service d'horodatage électronique du prestataire fait l'objet d'un document distinct, la politique d'horodatage YT-PH-TSA (1.3.6.1.4.1.[PEN].1.1.3), qui suit ce plan type et le complète par le chapitre 6 de la norme ETSI EN 319 421. Les exigences propres à l'horodatage — acteurs, exactitude déclarée, source de temps, profil du jeton, cycle de vie des clés d'unité d'horodatage, disponibilité du service et administration de la politique — y sont énoncées et ne sont pas reprises ici ; le seul point de contact entre les deux documents est l'horodatage des dossiers de preuve mentionné au chapitre 4.5.5 et le système de datation du chapitre 5.8.