YORYX® TRUST SASU

Déclaration des pratiques de certification (DPC)

YT-DPC

OID : 1.3.6.1.4.1.[PEN].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	Déclaration des pratiques de certification (DPC)
Identifiant du document	YT-DPC
Identifiant d'objet (OID)	1.3.6.1.4.1.[PEN].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. Signature électronique sécurisée et Certificat sécurisé....15
1.6. Identification du document....16
1.7. Fonctionnalités minimales couvertes par une IGC....17
1.8. Interactions avec l'IGC....17
1.9. Responsabilités....18
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 des certificats....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'AC et de composantes....20
1.11. Gestion de la PC....20
1.11.1. Entité gérant la PC....20
1.11.2. Point de contact....21
1.11.3. Entité déterminant la conformité d'une DPC avec cette PC....22
1.11.4. Procédures d'approbation de la conformité de la DPC....22
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....25

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....26
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....27
3. EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS....28
3.1. Demande de certificat....28
3.1.1. Origine d'une demande de certificat....28
3.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat....28
3.2. Traitement d'une demande de certificat....28
3.2.1. Exécution des processus d'identification et de validation de la demande....28
3.2.2. Acceptation ou rejet de la demande....29
3.2.3. Durée d'établissement du certificat....29
3.3. Délivrance du certificat....29
3.3.1. Actions de l'AC concernant la délivrance du certificat....29
3.3.2. Notification par l'AC de la délivrance du certificat au porteur....30
3.4. Acceptation du certificat....30
3.4.1. Démarche d'acceptation du certificat....30
3.4.2. Publication du certificat....30
3.4.3. Notification par l'AC aux autres entités de la délivrance du certificat....30
3.5. Usages de la bi-clé et du certificat....30
3.5.1. Utilisation de la clé privée et du certificat par le porteur....31
3.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat....31
3.6. Renouvellement d'un certificat....32
3.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé....32
3.7.1. Causes possibles de changement d'une bi-clé....32
3.7.2. Origine d'une demande d'un nouveau certificat....32
3.7.3. Procédure de traitement d'une demande d'un nouveau certificat....32
3.7.4. Notification au porteur de l'établissement du nouveau certificat....32
3.7.5. Démarche d'acceptation du nouveau certificat....32
3.7.6. Publication du nouveau certificat....32
3.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat....32
3.8. Modification du certificat....33

3.9. Révocation et suspension des certificats....33
3.9.1. Causes possibles d'une révocation....33
3.9.1.1. Certificats de porteurs....33
3.9.1.2. Certificats d'une composante de l'IGC....33
3.9.2. Origine d'une demande de révocation....34
3.9.2.1. Certificats de porteurs....34
3.9.2.2. Certificats d'une composante de l'IGC....34
3.9.3. Procédure de traitement d'une demande de révocation....34
3.9.3.1. Révocation d'un certificat de porteur....34
3.9.3.2. Révocation d'un certificat d'une composante de l'IGC....34
3.9.4. Délai accordé au porteur pour formuler la demande de révocation....34
3.9.5. Délai de traitement par l'AC d'une demande de révocation....35
3.9.5.1. Révocation d'un certificat de porteur....35
3.9.5.2. Révocation d'un certificat d'une composante de l'IGC....35
3.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats....35
3.9.7. Fréquence d'établissement des LCR....35
3.9.8. Délai maximum de publication d'une LCR....35
3.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats....35
3.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats....36
3.9.11. Autres moyens disponibles d'information sur les révocations....36
3.9.12. Exigences spécifiques en cas de compromission de la clé privée....36
3.9.13. Causes possibles d'une suspension....36
3.9.14. Origine d'une demande de suspension....36
3.9.15. Procédure de traitement d'une demande de suspension....36
3.9.16. Limites de la période de suspension d'un certificat....36
3.10. Fonction d'information sur l'état des certificats....37
3.10.1. Caractéristiques opérationnelles....37
3.10.2. Disponibilité de la fonction....37
3.10.3. Dispositifs optionnels....37
3.11. Fin de la relation entre le porteur et l'AC....37
3.12. Séquestre de clé et recouvrement....38
3.12.1. Politique et pratiques de recouvrement par séquestre des clés....38
3.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session....38
4. MESURES DE SÉCURITÉ NON TECHNIQUES....39

4.1. Mesures de sécurité physique....39
4.1.1. Situation géographique et construction des sites....39
4.1.2. Accès physique....39
4.1.3. Alimentation électrique et climatisation....40
4.1.4. Vulnérabilité aux dégâts des eaux....40
4.1.5. Prévention et protection incendie....40
4.1.6. Conservation des supports....40
4.1.7. Mise hors service des supports....40
4.1.8. Sauvegardes hors site....40
4.2. Mesures de sécurité procédurales....41
4.2.1. Rôles de confiance....41
4.2.2. Nombre de personnes requises par tâches....41
4.2.3. Identification et authentification pour chaque rôle....42
4.2.4. Rôles exigeant une séparation des attributions....42
4.3. Mesures de sécurité vis-à-vis du personnel....42
4.3.1. Qualifications, compétences et habilitations requises....42
4.3.2. Procédures de vérification des antécédents....43
4.3.3. Exigences en matière de formation initiale....43
4.3.4. Exigences et fréquence en matière de formation continue....43
4.3.5. Fréquence et séquence de rotation entre différentes attributions....43
4.3.6. Sanctions en cas d'actions non autorisées....43
4.3.7. Exigences vis-à-vis du personnel des prestataires externes....43
4.3.8. Documentation fournie au personnel....44
4.4. Procédures de constitution des données d'audit....44
4.4.1. Type d'évènements à enregistrer....44
4.4.2. Fréquence de traitement des journaux d'évènements....45
4.4.3. Période de conservation des journaux d'évènements....45
4.4.4. Protection des journaux d'évènements....45
4.4.5. Procédure de sauvegarde des journaux d'évènements....45
4.4.6. Système de collecte des journaux d'évènements....45
4.4.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement....45
4.4.8. Évaluation des vulnérabilités....46
4.5. Archivage des données....46
4.5.1. Types de données à archiver....46
4.5.2. Période de conservation des archives....47

4.5.3. Protection des archives....47
4.5.4. Procédure de sauvegarde des archives....47
4.5.5. Exigences d'horodatage des données....47
4.5.6. Système de collecte des archives....48
4.5.7. Procédures de récupération et de vérification des archives....48
4.6. Changement de clé d'AC....48
4.7. Reprise suite à compromission et sinistre....48
4.7.1. Procédures de remontée et de traitement des incidents et des compromissions....48
4.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)....49
4.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante 49
4.7.4. Capacités de continuité d'activité suite à un sinistre....49
4.8. Fin de vie de l'IGC....50
5. MESURES DE SÉCURITÉ TECHNIQUES....51
5.1. Génération et installation de bi-clés....51
5.1.1. Génération des bi-clés....51
5.1.1.1. Clés d'AC....51
5.1.1.2. Clés porteurs générées par l'AC....52
5.1.1.3. Clés porteurs générées par le porteur....52
5.1.1.4. Transmission de la clé privée à son propriétaire....52
5.1.2. Transmission de la clé publique à l'AC....52
5.1.3. Transmission de la clé publique de l'AC aux utilisateurs de certificats....52
5.1.4. Tailles des clés....53
5.1.5. Vérification de la génération des paramètres des bi-clés et de leur qualité....53
5.1.6. Objectifs d'usage de la clé....53
5.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques....54
5.2.1. Standards et mesures de sécurité pour les modules cryptographiques....54
5.2.1.1. Modules cryptographiques de l'AC....54
5.2.1.2. Dispositifs de création de signature des porteurs....54
5.2.2. Contrôle de la clé privée par plusieurs personnes....55
5.2.3. Séquestre de la clé privée....55
5.2.4. Copie de secours de la clé privée....55
5.2.5. Archivage de la clé privée....55
5.2.6. Transfert de la clé privée vers/depuis le module cryptographique....55

5.2.7. Stockage de la clé privée dans un module cryptographique....55
5.2.8. Méthode d'activation de la clé privée....56
5.2.8.1. Clés privées d'AC....56
5.2.8.2. Clés privées des porteurs....56
5.2.9. Méthode de désactivation de la clé privée....56
5.2.9.1. Clés privées d'AC....56
5.2.9.2. Clés privées des porteurs....56
5.2.10. Méthode de destruction des clés privées....56
5.2.10.1. Clés privées d'AC....56
5.2.10.2. Clés privées des porteurs....57
5.2.11. Niveau d'évaluation sécurité du module cryptographique....57
5.3. Autres aspects de la gestion des bi-clés....57
5.3.1. Archivage des clés publiques....57
5.3.2. Durées de vie des bi-clés et des certificats....57
5.4. Données d'activation....58
5.4.1. Génération et installation des données d'activation....58
5.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC....58
5.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du porteur....58
5.4.2. Protection des données d'activation....59
5.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC....59
5.4.2.2. Protection des données d'activation correspondant aux clés privées des porteurs....59
5.4.3. Autres aspects liés aux données d'activation....59
5.5. Mesures de sécurité des systèmes informatiques....59
5.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques....59
5.5.2. Niveau d'évaluation sécurité des systèmes informatiques....59
5.6. Mesures de sécurité liées au développement des systèmes....60
5.7. Mesures de sécurité réseau....60
5.8. Horodatage / Système de datation....61
6. PROFIL DES CERTIFICATS ET DES LCR....62
6.1. Profil des certificats....62
6.2. Profil des LCR....62
7. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS....64
7.1. Fréquences et/ou circonstances des évaluations....64

7.2. Identités des auditeurs....64
7.3. Relations entre auditeur et entités évaluées....65
7.4. Sujets couverts par les évaluations....65
7.5. Actions prises suite aux conclusions des évaluations....65
7.6. Communication des résultats....65
8. AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES....67
8.1. Durée et fin anticipée de validité de la PC....67
8.1.1. Durée de validité....67
8.1.2. Fin anticipée de validité....67
8.2. Protection des données à caractère personnel....67
8.3. Responsabilité, garanties et assurance....68
8.4. Réclamations, droit applicable et règlement des litiges....69
9. ANNEXES....70
9.1. Exigences de sécurité....70
9.1.1. Exigences sur les objectifs de sécurité du module cryptographique....70
9.1.2. Exigences sur les objectifs de sécurité du dispositif de création de signature....70
9.2. Variable de temps et niveaux de sécurité....71
9.3. Détails sur le gabarit d'un certificat racine....73
9.4. Détails sur le gabarit d'un certificat porteur....74
9.5. Algorithmes de signature et taille de clés des AC....74
9.6. Algorithmes et longueurs de clés des porteurs....75
9.7. Documents de références....76
9.8. Plan type détaillé d'une politique d'horodatage....78
9.9. Matrice de traçabilité [Ref_Serv_Conf_NonQual] — exigences 1 à 28....78

1. INTRODUCTION

1.1. Présentation générale

La présente déclaration des pratiques de certification, ci-après « la DPC », énonce les pratiques que YORYX TRUST SASU met en œuvre pour fournir ses services de confiance autres que qualifiés. Une politique de certification énonce ce qui est fait et ce à quoi le prestataire s'engage ; la présente déclaration énonce comment cela est fait : par quelle fonction, dans quel ordre, sous quel contrôle et avec quelle preuve.

Elle couvre l'ensemble des services déclarés : la délivrance et la gestion des certificats de signature électronique régies par YT-PC-SIGN (1.3.6.1.4.1.[PEN].1.1.1), la délivrance et la gestion des certificats de cachet électronique régies par YT-PC-SEAL (1.3.6.1.4.1.[PEN].1.1.2), le service de création de signature électronique avancée à distance, et le service d'horodatage électronique simple régi par YT-PH-TSA (1.3.6.1.4.1.[PEN].1.1.3). Les pratiques propres à l'horodatage — acteurs, source de temps, exactitude déclarée, cycle de vie des clés d'unité d'horodatage, production et vérification des jetons — sont énoncées dans cette dernière et ne sont pas reprises ici ; la présente déclaration renvoie à elle chaque fois que la matière lui appartient.

La DPC ne répète pas les stipulations des politiques. Lorsqu'une exigence est énoncée par une politique, la présente déclaration cite celle-ci par son identifiant et son identifiant d'objet, puis décrit la procédure qui l'honore. Lorsqu'une divergence apparaît entre une politique et la présente déclaration, la politique prévaut et l'écart est corrigé dans la déclaration selon le chapitre 1.11.4.

YORYX TRUST SASU est une société par actions simplifiée à associé unique (SASU), immatriculée au tribunal de commerce de Marrakech sous le RC Marrakech n° 184667, 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 que la vérification de l'identité soit déléguée à une autorité d'enregistrement tierce 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 chapitre 2.2 décrit la chaîne d'enregistrement qui en résulte, et le chapitre 4.3.7 les obligations imposées au personnel du tiers.

Le prestataire prend connaissance de l'ensemble des textes qui composent le cadre juridique et normatif applicable à ses services, et tient à jour la liste de ces textes au chapitre 9.7. Les textes normatifs s'expliquent mutuellement ; en cas d'incohérence entre une spécification normative et une disposition de la loi n° 43-20 ou de son décret d'application, la loi et le décret prévalent. Une suspicion d'incohérence est remontée à l'autorité nationale avant toute mise en œuvre, afin que le point soit clarifié et, le cas échéant, rectifié : c'est ce que prescrit l'exigence 1 du référentiel [Ref_Serv_Conf_NonQual], et c'est la règle de lecture de la présente déclaration.

Les services couverts relèvent des services de confiance autres que qualifiés au sens de l'article 3 de la loi n° 43-20. Ils visent la conformité aux normes ETSI EN 319 401 pour les exigences générales applicables à tout prestataire, ETSI EN 319 411-1 pour la délivrance de certificats et ETSI EN 319 421 pour l'horodatage, comme l'exigent les exigences 2, 3 et 4 du référentiel [Ref_Serv_Conf_NonQual].

Aucun service d'envoi recommandé électronique n'est fourni ni déclaré : l'exigence 5 du référentiel [Ref_Serv_Conf_NonQual], qui impose la conformité à la norme ETSI EN 319 531 pour un tel service, est sans objet en l'état. Si ce service venait à être déclaré, il ferait l'objet d'une politique distincte et la présente déclaration serait complétée selon le chapitre 1.11.4 ; l'engagement de s'y conformer est pris ici, et la matrice de traçabilité du chapitre 9.9 en conserve la trace.

> **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.

> **Point ouvert —** Les mentions publiques du registre du commerce font l’objet d’une mise en conformité avec l’objet social avant le dépôt de la déclaration préalable.

1.2. Acronymes et Définitions

1.2.1. Acronymes

Acronyme	Signification
AC	Autorité de certification
AE	Autorité d'enregistrement
AH	Autorité d'horodatage
CNIE	Carte nationale d'identité électronique
CNDP	Commission Nationale de contrôle de la protection des Données à caractère Personnel

Acronyme	Signification
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
DPC	Déclaration des pratiques de certification
IGC	Infrastructure de gestion de clés
LCR	Liste des certificats révoqués
LDPAQ	Liste déclarative des prestataires fournissant des services autres que qualifiés
MC	Mandataire de certification
OID	Identifiant d'objet (object identifier)
PC	Politique de certification
PH	Politique d'horodatage
PSCo	Prestataire de services de confiance
UH	Unité d'horodatage
UTC	Temps universel coordonné

Les acronymes des normes et des référentiels cités sont reproduits tels que leurs auteurs les emploient ; ils figurent au chapitre 9.7 avec le titre complet du texte correspondant.

1.2.2. Terminologie

Terme	Définition retenue par la présente déclaration
Prestataire	YORYX TRUST SASU, personne morale qui fournit les services de confiance couverts par la présente déclaration et qui demeure responsable de leur exécution, quelle que soit l'organisation opérationnelle retenue.
Plateforme	SELLO, canal d'enregistrement et de fourniture du service, qui exerce les fonctions d'autorité d'enregistrement pour le compte du prestataire dans le cadre du contrat écrit mentionné au chapitre 1.1.
Composante	Un ensemble de moyens humains, techniques et organisationnels mis en œuvre pour assurer une des fonctions du chapitre 1.7, sous la responsabilité du prestataire.
Titulaire	La personne, physique ou morale, identifiée dans un certificat délivré au titre de l'une des politiques citées au chapitre 1.1.
Signataire	Le titulaire d'un certificat de signature électronique lorsqu'il autorise une opération de signature ; il est seul à pouvoir accomplir l'action qui déclenche cette opération.

Terme	Définition retenue par la présente déclaration
Créateur du cachet	La personne morale titulaire d'un certificat de cachet électronique, agissant par ses systèmes à travers la plateforme.
Mandataire de certification	La personne désignée par écrit par une entité de rattachement pour assurer auprès de l'autorité d'enregistrement une partie des vérifications relatives aux titulaires qui lui sont rattachés.
Personne autorisée	La personne habilitée à accomplir certaines actions pour le compte du titulaire, notamment une demande de révocation.
Utilisateur de certificat	Toute personne qui reçoit un certificat, une signature, un cachet ou un jeton d'horodatage et s'y fie.
Données d'activation	Les facteurs d'authentification que le titulaire détient et qui conditionnent la mise en œuvre de ses données de création de signature ou de cachet ; aucune donnée d'activation n'est un code remis par le prestataire.
module cryptographique matériel	Le dispositif matériel dans lequel les bi-clés d'autorité et les données de création des titulaires sont générées et conservées. Il n'est jamais désigné par sa marque, son modèle ni son numéro de série.
Dossier de preuve	L'ensemble constitué et scellé pour un titulaire ou pour une opération, réunissant les éléments qui établissent la vérification d'identité, l'acceptation, la délivrance et le cycle de vie du certificat.
Cérémonie de clés	L'opération encadrée par un script écrit et approuvé, exécutée sous double contrôle en présence de témoins, au terme de laquelle une bi-clé d'autorité est générée, sauvegardée ou détruite.
Registre de publication	le registre de publication du site institutionnel de YORYX TRUST, qui met à disposition les documents et les informations énumérés au chapitre 1.11.2.
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

Le plan de référence de la DGSSI gradue les exigences par niveau de sécurité. La loi n° 43-20 retient pour sa part, en son article 4, trois niveaux : une signature électronique est soit simple, soit avancée, soit qualifiée. Les mêmes niveaux valent pour le cachet électronique.

Les pratiques décrites ici servent deux niveaux commerciaux, déclinés à l'identique pour la signature et pour le cachet.

Niveau	Politique ETSI de référence	OID ETSI	Ce que la pratique en fait
simple	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.
avancé	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.

La distinction entre les deux niveaux n'est pas une distinction de moyens cryptographiques : les bi-clés sont générées et conservées dans le module cryptographique matériel dans les deux cas, avec les mêmes algorithmes et les mêmes tailles de clés. Elle porte sur la vérification de l'identité au chapitre 2.2.2 et sur les données d'activation au chapitre 5.4, dont l'exigence 7 du référentiel [Ref_Serv_Conf_NonQual] fixe le seuil pour le niveau 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.

Aucun service qualifié n'est fourni au titre de la présente déclaration. Les services suivants ne sont décrits nulle part comme offerts : services de confiance qualifiés au sens de la loi n° 43-20 (signature, cachet, horodatage qualifiés) ; validation qualifiée de signatures et de cachets électroniques ; conservation qualifiée de signatures, de cachets et de certificats ; authentification de site internet (article 30 de la loi n° 43-20, réservée aux prestataires agréés) ; envoi recommandé électronique.

1.4. PSCE et niveau de sécurité

Le prestataire fournit les services énumérés ci-dessous. La colonne « Norme visée » indique le texte normatif dont la conformité est recherchée, au sens des exigences 3 et 4 du référentiel [Ref_Serv_Conf_NonQual] ; la colonne « OID du service » indique l'identifiant que le prestataire déclare à l'autorité nationale pour publication sur la liste déclarative.

Service	Niveau	Sujet du certificat	Norme visée	OID du service
Délivrance de certificats de signature électronique — niveau simple	simple	personne physique	ETSI EN 319 411-1	1.3.6.1.4.1.[PEN].1.1.1.1
Délivrance de certificats de signature électronique — niveau avancé	avancée	personne physique	ETSI EN 319 411-1	1.3.6.1.4.1.[PEN].1.1.1.2
Délivrance de certificats de cachet électronique — niveau simple	simple	personne morale	ETSI EN 319 411-1	1.3.6.1.4.1.[PEN].1.1.2.1
Délivrance de certificats de cachet électronique — niveau avancé	avancé	personne morale	ETSI EN 319 411-1	1.3.6.1.4.1.[PEN].1.1.2.2
Horodatage électronique simple	simple	jeton d’horodatage	ETSI EN 319 421	1.3.6.1.4.1.[PEN].1.1.3.1
Service de création de signature électronique avancée (signature à distance)	avancée	personne physique	ETSI EN 319 411-1 (certificat) — CEN EN 419 241-1 / -2 en cible (service)	1.3.6.1.4.1.[PEN].1.1.1.2

Le service de création de signature électronique avancée à distance partage l'identifiant du certificat de niveau avancé qui le rend possible : il n'est pas un service de délivrance distinct mais la mise à disposition, au titulaire, de la fonction de signature exercée pour son compte à l'intérieur du module cryptographique matériel. Ses pratiques figurent aux chapitres 3.5.1, 5.1.1.2 et 5.4.

1.5. Signature électronique sécurisée et Certificat sécurisé

Le plan de référence, écrit sous l'empire de la loi n° 53-05, emploie les expressions « signature électronique sécurisée » et « certificat sécurisé ». La loi n° 43-20 leur a substitué la gradation de son article 4 et réserve, en ses articles 6 et 15, la qualification à la signature et au cachet produits par un dispositif qualifié de création et reposant sur un certificat qualifié.

La présente déclaration emploie donc exclusivement le vocabulaire de la loi n° 43-20 : simple, avancé, qualifié. Une correspondance de lecture est donnée ci-dessous pour le lecteur qui vient du plan de référence.

Expression du plan de référence	Lecture retenue
Signature électronique sécurisée	Signature électronique avancée au sens de l'article 5 de la loi n° 43-20, produite au moyen d'un certificat de niveau avancé délivré selon les pratiques du chapitre 3.
Certificat sécurisé	Certificat de niveau avancé au sens du chapitre 1.3, conforme à la politique ETSI NCP+.
Certificat qualifié	Certificat au sens des articles 9 et 18 de la loi n° 43-20, que seul un prestataire agréé peut délivrer en application de l'article 32 ; aucun certificat de cette nature n'est délivré au titre de la présente déclaration.

1.6. Identification du document

La présente déclaration est identifiée par son identifiant d'objet, son titre, son numéro de version et sa date.

Élément	Valeur
Titre	Déclaration des pratiques de certification (DPC)
Identifiant du document	YT-DPC
OID du document	1.3.6.1.4.1.[PEN].1.2
Version	0.1
Statut	Projet — en préparation de la déclaration préalable
Classification	Diffusion publique
Langue	français
Entité éditrice	YORYX TRUST SASU

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].

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

Les informations déclaratives transmises à l'autorité nationale en vue de leur publication sur la liste déclarative comprennent, pour le prestataire : dénomination officielle ou raison sociale du prestataire telle qu’enregistrée auprès des autorités compétentes ; numéro d’immatriculation officiel du prestataire (ICE, numéro d’inscription au registre du commerce) ; adresse postale du prestataire ; adresse électronique du prestataire ; URL du prestataire ; pour chaque service de confiance fourni : type de service, nom commercial, bref descriptif, OID du service et URI vers la

politique du service. Le prestataire s'engage à en garantir l'exactitude et le maintien à jour ; la procédure qui l'assure figure au chapitre 1.11.1.

1.7. Fonctionnalités minimales couvertes par une IGC

L'infrastructure de gestion de clés du prestataire met en œuvre les fonctions suivantes. Chaque fonction est rattachée à une composante, et chaque composante à un responsable désigné par sa fonction au sens du chapitre 4.2.1.

Fonction	Composante qui l'exerce	Chapitre des pratiques
Enregistrement	La plateforme SELLO, pour le compte du prestataire, sous le contrat écrit du chapitre 1.1	2.2, 3.1, 3.2
Génération des certificats	L'autorité de certification émettrice du service concerné	3.3, 5.1
Génération des éléments secrets du titulaire	Le module cryptographique matériel, sous le contrôle de la fonction de signature	5.1.1.2
Remise et acceptation	La plateforme, dans l'espace du titulaire	3.3.2, 3.4
Création de signature pour le compte du titulaire	Le service de signature, à l'intérieur du module cryptographique matériel	3.5.1, 5.4
Publication	Le registre de publication	1.11.2, 3.4.2
Gestion des révocations	La fonction de gestion des révocations	3.9
Information sur l'état des certificats	La fonction d'information sur l'état des certificats	3.10
Horodatage	L'unité d'horodatage YORYX TRUST TSU 1 G1, selon YT-PH-TSA (1.3.6.1.4.1.[PEN].1.1.3)	5.8

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 de signature décrit au chapitre 5.1.1.2, dans lequel les données de création sont générées par le prestataire à l'intérieur du module cryptographique matériel et n'en sortent jamais en clair.

1.8. Interactions avec l'IGC

Les entités et personnes suivantes interagissent avec l'infrastructure. La colonne de droite indique ce que la pratique attend de chacune.

Entité	Interaction attendue
Le prestataire	Applique les politiques citées au chapitre 1.1 et la présente déclaration ; demeure responsable vis-à-vis de toute partie externe des prestations fournies par ses composantes.
La plateforme	Recueille la demande, vérifie l'identité, constitue le dossier de preuve, remet le certificat et recueille l'acceptation ; rend compte au prestataire selon le contrat écrit.
Le titulaire	Fournit des informations exactes, enrôle ses facteurs d'authentification, accepte explicitement son certificat, en fait un usage conforme et demande sa révocation sans délai lorsqu'une cause survient.
Le mandataire de certification	Assure, pour l'entité de rattachement qui l'a désigné par écrit, une partie des vérifications relatives aux titulaires rattachés, et transmet les demandes correspondantes.
L'utilisateur de certificat	Vérifie la chaîne de certification, la période de validité, les limites d'usage et l'état de révocation avant de se fier à un certificat, à une signature, à un cachet ou à un jeton.
L'autorité nationale	Exerce le contrôle a posteriori des prestataires non agréés en application de l'article 52 de la loi n° 43-20 ; reçoit les notifications des chapitres 1.11.1 et 4.7.1.

1.9. Responsabilités

Les engagements opposables figurent dans les politiques et, en termes opposables au titulaire et à l'utilisateur de certificat, dans les conditions générales d'utilisation YT-CGU-PP, YT-CGU-PM et YT-CGU-TSA, dont l'annexe 9.7 donne les identifiants d'objet. Le présent chapitre décrit la manière dont le prestataire organise l'exécution de ces engagements.

1.9.1. De l'autorité de certification du prestataire

L'autorité de certification exerce ses responsabilités par les moyens suivants.

- Une revue documentaire annuelle qui confronte chaque engagement des politiques à la procédure correspondante de la présente déclaration, et qui produit la liste des écarts traités selon le chapitre 7.5.
- Un cadre contractuel écrit avec chacune de ses composantes, qui reprend les obligations de la présente déclaration et fixe les moyens de contrôle dont dispose le prestataire.
- Une séparation des attributions qui interdit qu'une même personne décide, exécute et contrôle une opération sensible, selon le chapitre 4.2.4.
- La conservation, pour chaque certificat délivré, du dossier de preuve constitué selon le chapitre 4.5.1, qui permet d'établir a posteriori ce qui a été vérifié et par quelle fonction.
- Le maintien de la fonction d'information sur l'état des certificats jusqu'à l'expiration du dernier certificat délivré, y compris après une cessation d'activité, selon le chapitre 4.8.

1.9.2. De l'autorité d'enregistrement du prestataire

Les fonctions d'autorité d'enregistrement sont exercées par la plateforme pour le compte du prestataire. Le contrat écrit qui les encadre comporte au moins les stipulations suivantes, conformes à l'exigence 10 du référentiel [Ref_Serv_Conf_NonQual].

- Il lie le tiers au prestataire et détermine les obligations, les rôles et les responsabilités de chacun.
- Il précise les moyens de contrôle dont dispose le prestataire sur l'exécution des vérifications déléguées, y compris un droit d'audit exercé selon le chapitre 7.
- Il fixe les modalités d'établissement, de transmission et de conservation des preuves de vérification de l'identité, qui rejoignent le dossier de preuve du chapitre 4.5.1.
- Il impose au personnel du tiers les obligations du chapitre 4.3.7, notamment l'engagement de confidentialité écrit et la formation.
- Il interdit toute sous-délégation qui n'aurait pas été préalablement autorisée par écrit par le prestataire.

La délégation ne transfère pas la responsabilité : le prestataire demeure responsable de la vérification d'identité vis-à-vis des titulaires, des utilisateurs de certificats et de l'autorité nationale.

1.9.3. Du titulaire des certificats

Les obligations du titulaire sont énoncées par la politique applicable et reprises en termes opposables dans les conditions générales d'utilisation. La pratique du prestataire consiste à les rendre effectives par les moyens suivants.

- L'acceptation explicite du certificat, tracée dans le dossier de preuve, conditionne la mise en service de celui-ci selon le chapitre 3.4.1.
- Les documents applicables — politique, déclaration de divulgation, conditions générales — sont présentés au titulaire avant l'acceptation et restent accessibles dans le registre de publication.
- Les canaux de demande de révocation sont ouverts sans interruption selon le chapitre 3.9.2.1, afin qu'aucune obligation de diligence ne se heurte à une indisponibilité.
- Le formulaire YT-FORM-REVOCATION et le guide YT-GUIDE-USE décrivent au titulaire, en termes non techniques, ce qu'il doit faire et dans quel délai.

1.9.4. Du mandataire de certification

Lorsqu'une entité de rattachement désigne un mandataire de certification, le prestataire vérifie la désignation écrite, l'étendue des attributions confiées et l'identité du mandataire selon le chapitre 2.2.4. Le formulaire YT-FORM-MANDATE consigne ces éléments et rejoint le dossier de preuve.

Le mandataire est informé de la délivrance et de la révocation des certificats des titulaires qui lui sont rattachés, à l'exclusion de toute donnée étrangère à sa mission. La fin de son mandat est une cause de révocation au sens du chapitre 3.9.1.1 lorsqu'elle affecte l'exactitude d'une information portée dans un certificat.

1.10. Usage des certificats

1.10.1. Domaines d'utilisation applicables

Les domaines d'utilisation sont fixés par les politiques. La présente déclaration décrit les moyens techniques et procéduraux par lesquels ces limites sont rendues effectives.

1.10.1.1. Bi-clés et certificats des titulaires

- L'extension Key Usage est renseignée à la génération selon le gabarit de la politique applicable et marquée critique, ce qui interdit techniquement tout usage autre que celui prévu.
- L'extension Certificate Policies porte l'identifiant de la politique du niveau délivré, ce qui permet à un utilisateur de certificat d'écarter un certificat dont le niveau ne convient pas à son usage.
- Le service de signature n'accepte, pour une bi-clé de titulaire, que les opérations de signature ; aucune opération de chiffrement ni d'authentification n'est exposée pour ces clés.
- Les formats de signature et de cachet acceptés sont ceux de l'exigence 25 du référentiel [Ref_Serv_Conf_NonQual], énumérés au chapitre 9.6.

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

- La clé privée de l'autorité racine ne sert qu'à signer les certificats des autorités émettrices et les listes de révocation qui les concernent ; elle n'est activée que le temps d'une cérémonie.
- La clé privée d'une autorité émettrice ne sert qu'à signer les certificats de titulaires du service correspondant, les listes de révocation et les certificats des répondeurs d'information sur l'état des certificats.
- La clé privée d'un répondeur ne sert qu'à signer des réponses d'état ; celle d'une unité d'horodatage ne sert qu'à signer des jetons, selon les pratiques de la politique d'horodatage.
- Aucune clé de composante n'est employée dans un environnement de recette ou de développement, la séparation étant assurée selon le chapitre 4.1.1.

1.11. Gestion de la PC

Le présent chapitre décrit la gouvernance documentaire du prestataire : qui gère les politiques et la présente déclaration, comment une évolution est décidée, publiée et notifiée, et à qui le lecteur s'adresse.

Aucun procédé alternatif au certificat électronique, au sens de l'article 22 du décret n° 2-22-687, n'est mis en œuvre : les services décrits reposent tous sur des certificats électroniques délivrés par les autorités du chapitre 1.4. L'exigence 12 du référentiel [Ref_Serv_Conf_NonQual] subordonne la mise en œuvre d'un tel procédé à l'accord préalable de l'autorité nationale et à la publication du procédé par arrêté ; le prestataire n'en emploierait aucun sans avoir obtenu cet accord et sans avoir modifié la présente déclaration selon le chapitre 1.11.4, la liste des procédés jugés équivalents étant fixée par arrêté de l'autorité gouvernementale compétente.

1.11.1. Entité gérant la PC

Les politiques et la présente déclaration sont gérées par le prestataire. La responsabilité éditoriale relève du responsable d'application au sens du chapitre 4.2.1 ; l'approbation relève de la direction de la société, exprimée par une décision écrite versée au dossier d'audit.

Le prestataire tient à jour les informations déclaratives publiées sur la liste déclarative de l'autorité nationale et en garantit l'exactitude, conformément à l'exigence 27 du référentiel [Ref_Serv_Conf_NonQual]. Une revue de ces informations est conduite à chaque publication d'une nouvelle version d'un document du registre, et en tout état de cause selon la fréquence de contrôle interne du chapitre 7.1.

Toute modification de l'un des éléments au vu desquels la déclaration préalable a été effectuée est notifiée à l'autorité nationale dans les meilleurs délais, en application de l'article 21 du décret n° 2-22-687 et de l'exigence 21 du référentiel [Ref_Serv_Conf_NonQual]. Les modifications concernées sont les suivantes :

- un changement dans la prise de participation du prestataire ou dans sa gouvernance
- un changement affectant un service déclaré
- un changement significatif des procédures d’enregistrement ou des procédures d’identification des utilisateurs
- une modification de l’une des informations déclaratives publiées sur la liste déclarative des prestataires fournissant des services de confiance autres que qualifiés
- un changement induit par une modification de la politique de service
- un changement induit par une modification des conditions générales d’utilisation d’un service
- un changement de sous-traitants
- un changement de composant technique, matériel ou logiciel, concourant à la fourniture du service de confiance, notamment les composants cryptographiques
- une modification des conditions d’hébergement des services
- une modification de l’architecture technique
- un changement de site d’exploitation
- un changement substantiel des documents du registre de publication

La notification est accompagnée d'un rapport d'analyse des impacts de la modification, conformément à l'exigence 23, et des versions à jour de tous les documents impactés. Elle est adressée par envoi recommandé, postal ou électronique, ou déposée contre récépissé auprès de l'autorité nationale, conformément à l'exigence 24 ; le prestataire conserve l'accusé de réception au dossier d'audit.

Le prestataire définit et tient à jour la liste des changements techniques ou paramétriques standards, au sens de l'exigence 22 : changements prédéfinis, à faible risque et à faible impact, qui ne donnent pas lieu à notification. Cette liste est revue lors de chaque contrôle interne et toute modification de son périmètre est elle-même documentée.

1.11.2. Point de contact

Le point de contact du prestataire pour toute question relative aux politiques, à la présente déclaration et aux notifications est l'adresse électronique trust@yoryx.com, et l'adresse postale du siège social 57, rue Mauritania, BP 2609, Guéliz, 40000 Marrakech, Maroc.

Le registre de publication met à disposition, 24 heures sur 24, 7 jours sur 7, sans contrôle d’accès ni frais : les politiques de certification et la politique d’horodatage ; la déclaration des pratiques de certification ; les déclarations de divulgation PKI ; les conditions générales d’utilisation de chaque service ; les formulaires d’enregistrement, de mandat et de révocation ; les guides d’inscription, de contrôle d’identité et d’utilisation ; les tarifs et la procédure de réclamation ; les certificats des

autorités de certification ; les listes de révocation et le point d’accès au service d’information sur l’état des certificats.

Toute nouvelle version d’un document du registre y est publiée au plus tard le jour de sa prise d’effet ; les versions antérieures restent accessibles pendant la durée de conservation des archives. La consultation est libre ; seule l’écriture est restreinte aux fonctions habilitées, et toute modification est journalisée.

Une réclamation est traitée selon la procédure publiée sous l'identifiant YT-COMPLAINTS, dont les délais d'accusé de réception et de réponse sont rappelés au chapitre 8.4.

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

La conformité de la présente déclaration aux politiques citées au chapitre 1.1 est déterminée par le prestataire lui-même, par le contrôle interne du chapitre 7.1, et vérifiée par l'audit externe du chapitre 7.2. Aucune tierce partie n'est habilitée à modifier la présente déclaration.

L'autorité nationale exerce le contrôle a posteriori prévu par l'article 52 de la loi n° 43-20 ; ses constats sont traités comme des écarts au sens du chapitre 7.5.

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

Une évolution de la présente déclaration suit la procédure suivante.

1. Le responsable d'application établit le projet de version et l'analyse d'impact correspondante, qui identifie les politiques, les procédures et les documents du registre affectés.
2. Le responsable de sécurité et le contrôleur émettent un avis écrit sur le projet, portant respectivement sur la sécurité et sur la conformité aux politiques.
3. La direction approuve la version par une décision écrite datée, versée au dossier d'audit.
4. La version approuvée est publiée dans le registre de publication ; une modification substantielle est annoncée 30 jours avant sa prise d'effet, sauf lorsqu'une exigence légale ou de sécurité impose un délai plus court.
5. Lorsque l'évolution modifie le niveau d'exigence ou le champ d'application, un nouvel identifiant d'objet est attribué et l'autorité nationale est notifiée selon le chapitre 1.11.1.
6. Les versions antérieures restent accessibles pendant la durée de conservation des archives fixée au chapitre 4.5.2.

Une correction purement rédactionnelle, qui ne modifie ni une exigence ni une valeur, est publiée sans préavis et signalée dans le tableau des révisions du document.

2. IDENTIFICATION ET AUTHENTIFICATION

2.1. Nommage

Les noms portés dans les certificats sont composés par l'autorité d'enregistrement à partir des seules informations vérifiées, puis contrôlés par la fonction de génération avant signature. Le présent chapitre décrit la composition, l'exigence d'explicitation, le mécanisme d'unicité et le traitement des signes distinctifs.

2.1.1. Types de noms

Les noms portés dans les certificats sont des noms distinctifs au format X.501, conformes à la norme IETF RFC 5280. Les gabarits sont fixés par les politiques ; la pratique consiste à les composer à partir des seules informations vérifiées au chapitre 2.2.

Certificat	Nom distinctif composé
YORYX TRUST Root CA G1	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 physique	C=MA, CN=<prénom et nom du titulaire>, serialNumber=<identifiant unique attribué par le prestataire>
Titulaire personne morale	C=MA, O=<dénomination de la personne morale>, organizationIdentifier=<NTRMA-|ICE- suivi de l’identifiant officiel>, CN=<nom du cachet>

Les attributs d'organisation portés dans les certificats d'autorité sont ceux de la société : organizationIdentifier NTRMA-184667, serialNumber ICE 004013324000019, pays MA. Ils sont repris de l'extrait du registre du commerce et ne sont jamais saisis à la main lors d'une cérémonie : ils figurent dans le script approuvé au préalable.

2.1.2. Nécessité d'utilisation de noms explicites

Aucune abréviation, aucun pseudonyme et aucune forme qui ne permettrait pas d'identifier la personne ne sont acceptés. L'autorité d'enregistrement compose le nom distinctif à partir de la pièce d'identité produite pour une personne physique, ou de l'extrait du registre du commerce pour une personne morale ; elle rejette la demande lorsque l'orthographe déclarée ne correspond pas à la pièce.

La transcription des caractères non latins et des signes diacritiques suit celle de la pièce d'identité produite ; lorsque la pièce comporte deux transcriptions, celle qui figure dans la zone lisible par machine est retenue et l'autre est consignée dans le dossier de preuve.

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.

La pratique qui l'assure est la suivante : avant toute génération, la fonction de génération des certificats interroge le registre des noms distinctifs déjà attribués par l'autorité émettrice concernée. Lorsqu'un nom identique existe, la demande est suspendue et l'autorité d'enregistrement complète le nom par l'identifiant unique attribué par le prestataire, deux titulaires pouvant légitimement porter les mêmes prénom et nom. Un nom distinctif libéré par l'expiration ou la révocation d'un certificat n'est jamais réattribué à un autre titulaire.

2.1.4. Identification, authentification et rôle des marques déposées

Aucun signe distinctif ni aucune marque ne figure dans le nom distinctif d'un certificat de titulaire personne physique, celui-ci ne portant que l'identité du signataire.

Pour un certificat de cachet, le nom distinctif porte la dénomination de la personne morale telle qu'elle est enregistrée auprès des autorités compétentes ; aucune dénomination commerciale ou marque n'y est substituée. Lorsqu'un demandeur sollicite l'inscription d'un signe distinctif, l'autorité d'enregistrement refuse la demande sans instruire la question de la titularité du signe : le prestataire n'arbitre aucun litige de propriété intellectuelle et n'engage aucune vérification à ce titre.

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. La vérification d’identité à distance est conduite selon les modalités admises par le référentiel de la DGSSI.

> **Point ouvert —** L’article 20 du décret n° 2-22-687 nomme la carte nationale d’identité électronique parmi les moyens d’identification électronique permettant de prouver l’identité à distance, et Ref_Serv_Conf_NonQual_Exig 11 rend suffisantes les dispositions de [Ref_Deliv_Cert_Qual] ; la liste des modalités concrètement admises pour le régime déclaratif reste néanmoins à confirmer auprès de l’autorité nationale, et aucune intégration de la carte n’existe à ce jour.

Les dispositions de vérification de l'identité du référentiel [Ref_Deliv_Cert_Qual] demeurent applicables — suffisantes mais non nécessaires — pour la délivrance de certificats non qualifiés conformes à la norme ETSI EN 319 411-1, en particulier de type NCP et NCP+, comme le rappelle l'exigence 11 du référentiel [Ref_Serv_Conf_NonQual]. La pratique décrite ci-dessous s'aligne sur elles.

2.2.1. Méthode pour prouver la possession de la clé privée

La bi-clé du titulaire est générée à l'intérieur du module cryptographique matériel, sur demande de la fonction de génération des certificats et pour le compte d'un titulaire déjà identifié. La preuve de possession résulte de la génération elle-même : la clé publique certifiée est celle que le module a produite dans la même opération, sous le contrôle de la fonction, et la clé privée correspondante n'a jamais quitté le module.

Aucune requête de certification transmise par un tiers n'est acceptée pour un certificat de titulaire ; la fonction de génération n'expose pas d'interface qui permettrait de soumettre une clé publique d'origine externe. La correspondance entre la clé privée et la clé publique est vérifiée par le module lui-même, selon l'objectif de sécurité énoncé à l'annexe 9.1.2 des politiques.

2.2.2. Enregistrement d'un titulaire

L'enregistrement se déroule à travers la plateforme, qui exerce les fonctions d'autorité d'enregistrement. La chaîne est la suivante.

1. Le demandeur ouvre une demande dans son espace sur la plateforme et déclare les informations destinées à figurer dans le certificat.
2. Il produit sa carte nationale d'identité électronique, référence d'identité retenue, ou une autre pièce officielle d'identité en cours de validité lorsque la première ne peut être produite ; pour une personne morale, l'extrait du registre du commerce et la pièce d'identité du représentant légal sont produits en outre.
3. L'autorité d'enregistrement contrôle la validité de la pièce, la cohérence de ses mentions avec les informations déclarées, et l'identité du demandeur, en présence physique à titre de règle de base.
4. Elle vérifie, le cas échéant, les pouvoirs du demandeur selon le chapitre 2.2.4.
5. Le demandeur enrôle ses facteurs d'authentification, qui constituent les données d'activation décrites au chapitre 5.4.1.2.
6. Il prend connaissance de la politique applicable, de la déclaration de divulgation et des conditions générales d'utilisation, et les accepte explicitement.
7. L'autorité d'enregistrement clôt le dossier, constitue le dossier de preuve du chapitre 4.5.1 et transmet la demande validée à la fonction de génération des certificats.

La vérification en présence physique est conduite selon le guide YT-GUIDE-IDENTITY, qui décrit les contrôles opérés sur la pièce produite : validité, intégrité du support, cohérence de la zone lisible par machine, concordance de la photographie avec le porteur, et concordance des mentions avec les informations déclarées. Le résultat de chaque contrôle est consigné, ainsi que la fonction qui l'a opéré et la date.

Aucune copie de pièce d'identité n'est conservée au-delà de ce que la constitution du dossier de preuve exige, et les données à caractère personnel recueillies sont limitées à celles qui sont nécessaires à la vérification et à la composition du nom distinctif, selon le chapitre 8.2.

Le niveau simple et le niveau avancé se distinguent ici : au niveau avancé, la vérification en présence physique est la règle et le recours à une modalité admise à distance est tracé et motivé dans le dossier de preuve ; au niveau simple, l'analyse de risque admet une vérification allégée dès lors que l'identité reste établie sur une pièce officielle en cours de validité.

2.2.3. Informations non vérifiées du titulaire

Aucune information non vérifiée ne figure dans un certificat. Une information déclarée par le demandeur et non contrôlable par l'autorité d'enregistrement est soit écartée du certificat, soit vérifiée avant délivrance ; il n'existe pas de troisième voie.

Les informations recueillies pour les besoins de la relation et qui ne figurent pas dans le certificat — adresse de contact, préférences de notification — sont traitées selon le chapitre 8.2 et ne sont jamais certifiées.

2.2.4. Validation de l'autorité du demandeur

Lorsque le demandeur agit pour son propre compte, l'identité vérifiée au chapitre 2.2.2 suffit et aucune vérification de pouvoirs n'est requise.

Lorsque la demande porte sur un certificat de cachet, l'autorité d'enregistrement vérifie l'existence de la personne morale sur l'extrait du registre du commerce, la qualité du représentant légal et, le cas échéant, la délégation écrite dont se prévaut le demandeur. Ces éléments sont consignés au formulaire YT-FORM-LEGAL-REP, versé au dossier de preuve.

Lorsque la demande est présentée par un mandataire de certification pour le compte d'une entité de rattachement, l'autorité d'enregistrement vérifie la désignation écrite du mandataire par cette entité, l'étendue de ses attributions et l'accord exprès du futur titulaire ; ces éléments sont consignés au formulaire YT-FORM-MANDATE, versé au dossier de preuve.

2.2.5. Critères d'interopérabilité

Les certificats délivrés respectent la norme IETF RFC 5280 et les gabarits publiés en annexe des politiques ; aucune extension propriétaire n'est employée. Cette pratique est ce qui rend les certificats exploitables par les logiciels de vérification du marché sans configuration particulière.

Aucune reconnaissance croisée, aucune certification croisée et aucune hiérarchie externe ne sont mises en œuvre : l'autorité racine YORYX TRUST Root CA G1 n'est certifiée par aucune autre autorité et ne certifie aucune autorité qui ne soit une composante du prestataire. La confiance repose sur l'installation du certificat racine par l'utilisateur de certificat, décrite dans le guide YT-GUIDE-USE.

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

L'intensité de la vérification dépend de la situation : allégée lorsque rien n'a changé et que le certificat en cours n'a pas été révoqué, intégrale dans tous les autres cas. Une demande de révocation obéit à une règle distincte, énoncée au chapitre 2.3.3, parce qu'elle doit pouvoir aboutir vite sans jamais aboutir sur une origine non authentifiée.

2.3.1. Identification et validation pour un renouvellement courant

Un renouvellement courant intervient avant l'expiration d'un certificat non révoqué, dont les informations n'ont pas changé. La pratique est la suivante.

1. Le titulaire est avisé de l'échéance dans son espace sur la plateforme, avec un préavis suffisant pour éviter toute interruption d'usage.
2. Il présente sa demande après authentification forte au moyen des facteurs d'authentification enrôlés lors de l'enregistrement.
3. L'autorité d'enregistrement confirme que les informations destinées à figurer dans le nouveau certificat sont inchangées et que la pièce d'identité produite à l'enregistrement est toujours en cours de validité.
4. Une nouvelle bi-clé est générée selon le chapitre 5.1.1.2 ; l'ancienne n'est jamais recertifiée.

Lorsqu'une information a changé, ou lorsque la pièce d'identité initialement produite a expiré, la demande est traitée comme un enregistrement initial et la vérification d'identité du chapitre 2.2.2 est reconduite intégralement.

2.3.2. Identification et validation pour un renouvellement après révocation

Un certificat révoqué n'est jamais rétabli. Une nouvelle demande consécutive à une révocation est traitée comme un enregistrement initial : la vérification d'identité du chapitre 2.2.2 est reconduite dans son intégralité, et le dossier de preuve du nouveau certificat référence la révocation qui l'a précédé.

Lorsque la révocation est intervenue pour compromission ou suspicion de compromission des données de création, l'autorité d'enregistrement vérifie en outre que la cause a cessé, et les facteurs d'authentification du titulaire sont réenrôlés 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, selon le canal employé.

Canal	Authentification de l'origine
Espace du titulaire sur la plateforme	Authentification forte au moyen des facteurs enrôlés ; la demande est imputée au titulaire lui-même.
Formulaire de demande de révocation transmis par un canal écrit	Vérification de l'identité du demandeur et de sa qualité — titulaire, personne autorisée, mandataire de certification, représentant légal — sur pièce ; la fonction de gestion des révocations rappelle le demandeur par un moyen de contact enregistré avant l'enregistrement.
Demande émanant d'une composante du prestataire	Décision consignée par une fonction habilitée au sens du chapitre 4.2.1, sous double contrôle lorsqu'elle porte sur un certificat de composante.
Demande émanant de l'autorité nationale ou d'une autorité judiciaire	Vérification de l'authenticité de l'acte reçu ; la demande est exécutée sans délai et consignée.

Une demande dont l'origine ne peut être authentifiée n'est pas exécutée ; elle est consignée et, lorsqu'elle porte des indices de compromission, elle déclenche l'analyse du chapitre 4.7.1. Le délai de traitement du chapitre 3.9.5.1 court à compter de l'authentification de l'origine, et non de la réception d'une demande non authentifiée.

3. EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

3.1. Demande de certificat

Une demande n'est instruite que si son origine est identifiée et si le dossier qui l'accompagne permet la vérification. Le présent chapitre énonce qui peut demander et ce que le dossier contient.

3.1.1. Origine d'une demande de certificat

Une demande de certificat de titulaire émane du futur titulaire lui-même, présentée par la plateforme, du mandataire de certification de l'entité à laquelle il est rattaché agissant avec son accord exprès, ou du représentant légal de la personne morale lorsque la demande porte sur un certificat de cachet.

Une demande de certificat de composante — autorité émettrice, répondeur d'information sur l'état des certificats, unité d'horodatage — émane du responsable d'application de la composante concernée et n'est instruite que dans le cadre d'une cérémonie de clés au sens du chapitre 5.1.1.1.

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

La demande est établie dans l'espace du demandeur sur la plateforme. Le dossier constitué comporte au moins les éléments suivants, dont l'autorité d'enregistrement répond.

- Les informations destinées à figurer dans le certificat, telles que déclarées puis telles que vérifiées.
- La référence de la pièce d'identité produite et le résultat de chaque contrôle opéré sur elle, sans conservation d'une donnée qui ne serait pas nécessaire.
- Pour une personne morale, les pièces établissant son existence et la qualité de son représentant.
- L'acceptation explicite de la politique applicable, de la déclaration de divulgation et des conditions générales d'utilisation, horodatée.
- L'identification de la fonction qui a opéré chaque vérification et la date de celle-ci.

Le demandeur répond de l'exactitude et de la complétude des informations qu'il fournit ; l'autorité d'enregistrement répond de la vérification et de la traçabilité de celle-ci ; le prestataire répond de l'ensemble vis-à-vis des tiers.

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 vérifications du chapitre 2.2 avant toute transmission à la fonction de génération. La transmission est elle-même authentifiée : la fonction de génération n'accepte une demande que d'une origine identifiée et n'accepte aucune demande dont le dossier de preuve serait incomplet.

Aucune vérification n'est réputée acquise du fait d'une vérification antérieure portant sur une autre demande, sauf lorsqu'il s'agit d'un renouvellement courant relevant du chapitre 2.3.1.

3.2.2. Acceptation ou rejet de la demande

La demande est acceptée lorsque toutes les vérifications ont abouti et que le dossier de preuve est complet. Elle est rejetée dans les cas suivants.

- La pièce d'identité produite n'est pas en cours de validité, ou ses mentions ne concordent pas avec les informations déclarées.
- Les pouvoirs du demandeur ne sont pas établis alors que la demande est présentée pour le compte d'un tiers ou d'une personne morale.
- Une information destinée au certificat ne peut être vérifiée.
- Le demandeur n'accepte pas la politique applicable ou les conditions générales d'utilisation.
- Le prestataire est fondé à considérer que la délivrance servirait un usage contraire à la loi ou aux limites d'usage de la politique applicable.

Le rejet est motivé et notifié au demandeur dans son espace sur la plateforme ; le motif et sa date sont consignés. Un rejet ne fait pas obstacle à une nouvelle demande dès lors que la cause a disparu.

3.2.3. Durée d'établissement du certificat

Aucun engagement de délai n'est pris entre l'acceptation de la demande et la délivrance : la durée dépend de la disponibilité du demandeur pour la vérification d'identité, qui n'est pas maîtrisée par le prestataire. Le prestataire s'engage en revanche sur la disponibilité des fonctions qui concourent à la délivrance, énoncée au chapitre 3.10.2, et sur les délais opposables du chapitre 3.9.5.1 pour la révocation.

Une demande acceptée dont la génération ne peut aboutir pour une cause technique est signalée au demandeur et rejointe par un enregistrement d'incident au sens du chapitre 4.7.1 lorsque la cause affecte une fonction de l'infrastructure.

3.3. Délivrance du certificat

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

La fonction de génération des certificats exécute la séquence suivante, sans intervention manuelle sur le contenu du certificat.

1. Elle demande au module cryptographique matériel la génération de la bi-clé du titulaire, selon les algorithmes et les tailles du chapitre 9.6.
2. Elle compose le certificat à partir des seules informations validées par l'autorité d'enregistrement et de la clé publique produite, selon le gabarit de la politique applicable.
3. Elle attribue un numéro de série non prévisible et unique au sein du domaine de l'autorité émettrice.
4. Elle soumet le certificat à la signature de la clé privée de l'autorité émettrice, à l'intérieur du module.
5. Elle enregistre l'opération dans le journal d'évènements du chapitre 4.4.1 et verse le certificat délivré au dossier de preuve.

Aucun certificat n'est délivré dont la fin de validité dépasserait celle du certificat de l'autorité émettrice ; la fonction de génération refuse une telle demande, ce qui rend effective la règle énoncée au chapitre 5.3.2.

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

Le titulaire est avisé de la délivrance dans son espace sur la plateforme. La notification comporte le certificat, ses dates de validité, l'identifiant de la politique sous laquelle il a été délivré, le rappel des limites d'usage et le moyen d'en demander la révocation.

Aucun support matériel n'est expédié et aucun secret n'est transmis par un canal de notification : les données de création demeurent dans le module et les données d'activation sont les facteurs d'authentification que le titulaire détient déjà.

3.4. Acceptation du certificat

3.4.1. Démarche d'acceptation du certificat

Le titulaire prend connaissance du certificat délivré, vérifie l'exactitude des informations qu'il porte et l'accepte explicitement dans son espace. L'acceptation est horodatée et versée au dossier de preuve.

Tant que l'acceptation n'est pas recueillie, le service de signature refuse toute opération au moyen du certificat. Un certificat non accepté au terme d'un délai raisonnable est révoqué selon le chapitre 3.9.1.1, sans frais pour le titulaire.

Une contestation formulée à ce stade sur l'exactitude d'une information entraîne la révocation du certificat et la reprise de la demande à partir du chapitre 2.2.2, la correction d'un certificat délivré étant impossible.

3.4.2. Publication du certificat

Les certificats de titulaires ne sont pas publiés : aucun annuaire public de certificats de titulaires n'est exploité, ce qui limite l'exposition des données à caractère personnel qu'ils portent. Le certificat est mis à la disposition du titulaire dans son espace, et se diffuse par ailleurs avec les signatures et les cachets qu'il permet de vérifier.

Les certificats des autorités de certification sont publiés dans le registre de publication et diffusés 24 heures au moins avant toute délivrance sous la clé correspondante.

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

Aucune notification n'est adressée à un tiers, à deux exceptions près : le mandataire de certification est informé de la délivrance des certificats des titulaires qui lui sont rattachés, à l'exclusion de toute donnée étrangère à sa mission ; le représentant légal est informé de la délivrance d'un certificat de cachet à sa personne morale.

3.5. Usages de la bi-clé et du certificat

L'usage d'une bi-clé et du certificat qui la couvre est borné par la politique applicable, rendu contraignant par l'extension Key Usage selon le chapitre 1.10.1.1, et exercé selon les pratiques ci-dessous.

Toute signature et tout cachet produits par le service sont liés aux données associées de telle sorte que toute modification ultérieure de celles-ci soit détectable : le lien est obtenu par l'application d'une fonction d'empreinte conforme au chapitre 9.5, dans un format de l'exigence 25 du référentiel [Ref_Serv_Conf_NonQual] énuméré au chapitre 9.6. C'est ce que requiert l'exigence 9 du même référentiel, et c'est ce qui donne à l'utilisateur de certificat le moyen de constater une altération sans se fier à une déclaration.

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

Les données de création du titulaire sont mises en œuvre exclusivement à l'intérieur du module cryptographique matériel, par l'intermédiaire du service du prestataire, et seulement après l'action d'autorisation du titulaire.

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

L’utilisation des données de création de signature du titulaire est subordonnée à une authentification forte multifacteur mettant en œuvre au moins deux facteurs d’authentification, propre à chaque opération de signature. L'exigence 7 du référentiel [Ref_Serv_Conf_NonQual] impose ce niveau pour la signature électronique avancée : les clés de signature doivent être utilisées sous le contrôle exclusif du signataire avec un niveau de confiance élevé, garanti par une authentification forte multifacteur propre à l'usage des clés. 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. L'exigence 8 pose la règle correspondante pour le cachet.

La pratique qui rend ce contrôle effectif comporte quatre éléments.

- Le service de signature n'expose aucune interface permettant de déclencher une opération sans l'action d'autorisation du titulaire ; il n'existe pas de mode d'exploitation dans lequel une fonction interne signerait pour le compte d'un titulaire.
- L'autorisation est liée à l'opération : elle porte sur les données à signer présentées au titulaire, et ne vaut pas pour une autre opération ni pour une opération ultérieure.
- Les données présentées au titulaire avant l'autorisation sont celles qui sont effectivement signées ; leur empreinte est consignée dans le journal d'évènements avec la référence de l'opération.
- Chaque opération de signature ou de cachet donne lieu à un enregistrement qui identifie le certificat employé, la date, l'empreinte des données et le résultat, et qui rejoint les archives du chapitre 4.5.1.

La signature ou le cachet produits sont liés aux données associées de telle sorte que toute modification ultérieure de celles-ci soit détectable, par l'emploi d'une fonction d'empreinte conforme au chapitre 9.5 : c'est ce que requiert l'exigence 9 du référentiel [Ref_Serv_Conf_NonQual].

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.

Le prestataire met à disposition les moyens de cette vérification sans contrôle d'accès ni frais : les certificats d'autorité et les listes de révocation dans le registre de publication, et le service d'information en ligne sur l'état des certificats décrit au chapitre 3.10. Le guide YT-GUIDE-USE décrit la démarche pour un utilisateur non technicien.

Un utilisateur de certificat qui se fie à un certificat sans procéder à ces vérifications ne peut se prévaloir des engagements des politiques ; cette limite figure dans les conditions générales d'utilisation et dans les déclarations de divulgation.

3.6. Renouvellement d'un certificat

Le renouvellement d'un certificat sans changement de bi-clé n'est pas pratiqué. Une bi-clé n'est jamais recertifiée : toute prolongation de service donne lieu à une nouvelle bi-clé générée dans le module et à un nouveau certificat, selon le chapitre 3.7.

Ce choix supprime une catégorie entière de risque — l'usage prolongé d'une même clé au-delà de la durée pour laquelle sa robustesse a été évaluée — et il ne coûte rien au titulaire, la génération de la bi-clé se déroulant à l'intérieur du module sans manipulation de sa part.

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'approche du terme de la période de validité du certificat en cours.
- La révocation du certificat en cours, quelle qu'en soit la cause.
- La modification d'une information portée dans le certificat.
- L'évolution des algorithmes ou des tailles de clés retenus au chapitre 9.6, qui rend souhaitable le remplacement anticipé des bi-clés en service.
- Le changement de clé de l'autorité émettrice selon le chapitre 4.6, lorsqu'il impose la reprise des certificats délivrés sous l'ancienne clé.

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

Les origines admises sont celles du chapitre 3.1.1. Une demande consécutive à une révocation ne peut émaner que du titulaire ou de son représentant légal, à l'exclusion de toute origine automatique.

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

La procédure est celle du chapitre 3.2, avec l'intensité de vérification fixée par le chapitre 2.3 : allégée pour un renouvellement courant, intégrale après une révocation ou lorsqu'une information a changé.

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

La notification est celle du chapitre 3.3.2. Elle rappelle en outre la date à laquelle le certificat précédent cesse de produire effet, afin que le titulaire n'emploie pas simultanément deux certificats pour un même usage.

3.7.5. Démarche d'acceptation du nouveau certificat

L'acceptation est celle du chapitre 3.4.1 ; elle est requise pour le nouveau certificat comme pour le premier, sans reprise automatique de l'acceptation antérieure.

3.7.6. Publication du nouveau certificat

La règle du chapitre 3.4.2 s'applique sans changement.

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

La règle du chapitre 3.4.3 s'applique sans changement.

3.8. Modification du certificat

Sans objet : un certificat délivré n'est jamais modifié. Toute évolution d'une information qu'il porte entraîne sa révocation selon le chapitre 3.9 et la délivrance d'un nouveau certificat selon le chapitre 3.7, la signature de l'autorité émettrice ne pouvant couvrir qu'un contenu figé.

3.9. Révocation et suspension des certificats

La révocation est la fonction la plus sensible du service : elle est le seul moyen dont dispose un titulaire pour faire cesser l'effet d'un certificat, et le seul moyen dont dispose un utilisateur de certificat pour savoir qu'il ne doit plus s'y fier. Les canaux de demande sont ouverts sans interruption, le traitement est borné par un délai maximum opposable, et la révocation est irréversible.

3.9.1. Causes possibles d'une révocation

3.9.1.1. Certificats de porteurs

- 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

Sont assimilées à ces causes, dans la pratique du prestataire, l'absence d'acceptation du certificat au terme du délai mentionné au chapitre 3.4.1, et la constatation qu'une information vérifiée à l'enregistrement était inexacte.

La perte ou la compromission d'un facteur d'authentification n'est pas, à elle seule, une cause de révocation du certificat : elle entraîne la révocation de ce facteur et un nouvel enrôlement, les données de création demeurant dans le module. Elle devient une cause de révocation dès lors qu'elle laisse craindre qu'une opération ait pu être autorisée sans l'accord du titulaire.

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.
- Décision de mettre fin à l'exploitation de la composante avant le terme de son certificat.
- Inexactitude ou changement d'une information portée dans le certificat de la composante.
- Non-conformité constatée de la composante aux politiques ou à la présente déclaration, lorsque l'écart ne peut être corrigé sans remplacement de la clé.
- Évolution des algorithmes ou des tailles de clés rendant la clé de la composante insuffisamment robuste.
- Cessation d'activité du prestataire sans reprise par un autre prestataire.

3.9.2. Origine d'une demande de révocation

3.9.2.1. Certificats de porteurs

Une demande peut émaner du titulaire lui-même, d'une personne autorisée, du mandataire de certification dont relève le titulaire, du représentant légal de la personne morale pour un certificat de cachet, de l'autorité d'enregistrement, du prestataire agissant de sa propre initiative lorsqu'une cause du chapitre 3.9.1.1 est constatée, ou de l'autorité nationale ou d'une autorité judiciaire dans l'exercice de leurs attributions.

Les canaux de demande sont ouverts 24 heures sur 24, 7 jours sur 7. L'origine de la demande est authentifiée selon le chapitre 2.3.3 avant tout traitement.

3.9.2.2. Certificats d'une composante de l'IGC

Une demande portant sur un certificat de composante émane du responsable d'application de la composante, du responsable de sécurité, ou de la direction ; elle est décidée sous double contrôle et consignée. L'autorité nationale peut en outre en former une 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 porteur

1. La fonction de gestion des révocations authentifie l'origine de la demande selon le chapitre 2.3.3 et enregistre l'heure de cette authentification.
2. Elle vérifie que le certificat visé existe, qu'il n'est pas déjà révoqué et qu'il n'est pas expiré.
3. Elle qualifie la cause au regard du chapitre 3.9.1.1 et la consigne.
4. Elle inscrit la révocation, qui prend effet immédiatement et interdit toute nouvelle opération au moyen du certificat.
5. Elle publie l'information d'état selon les chapitres 3.9.7 et 3.10.1.
6. Elle notifie le titulaire et, le cas échéant, le mandataire de certification ou le représentant légal.
7. Elle verse au dossier de preuve la demande, son authentification, la cause retenue, l'heure d'effet et l'heure de publication.

Une révocation est irréversible : aucun mécanisme ne permet de rétablir un certificat révoqué, y compris lorsque la cause se révèle ultérieurement infondée. Une révocation prononcée à tort donne lieu à la délivrance d'un nouveau certificat sans frais, selon le chapitre 3.7.

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

La révocation d'un certificat de composante est décidée sous double contrôle et exécutée en cérémonie lorsqu'elle porte sur un certificat signé par l'autorité racine. Elle donne lieu à la publication d'une liste de révocation d'autorités selon le chapitre 3.9.7, à l'information des titulaires concernés et à l'application du chapitre 4.7.3 lorsque la cause est une compromission.

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

Le titulaire formule sa demande sans délai, dès la connaissance de la cause de révocation. Cette obligation figure dans les conditions générales d'utilisation ; la pratique du prestataire consiste à la rendre praticable en maintenant les canaux ouverts 24 heures sur 24, 7 jours sur 7 et sans frais.

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

3.9.5.1. Révocation d'un certificat de porteur

Le délai maximum de traitement d'une demande de révocation authentifiée est de 24 heures. L'information d'état correspondante est publiée dans un délai maximum de 24 heures à compter du traitement.

Ces deux délais sont des maxima opposables et non des objectifs de fonctionnement : le traitement est engagé dès l'authentification de l'origine, et la publication suit la génération de la liste de révocation dans le délai fixé au chapitre 3.9.8.

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

Une demande portant sur un certificat de composante est traitée sans délai dès sa décision, la compromission d'une clé de composante affectant l'ensemble des certificats délivrés sous cette clé. La liste de révocation d'autorités est régénérée et publiée immédiatement après la révocation, sans attendre l'échéance périodique du chapitre 3.9.7.

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

L'utilisateur de certificat vérifie l'état de révocation au moment où il se fie au certificat, par la liste de révocation ou par le service d'information en ligne. Une vérification antérieure ne vaut pas pour un usage postérieur : c'est l'état au moment de l'usage qui est opposable.

Le prestataire ne peut imposer cette vérification ; il la rend possible en tout temps et sans frais, et il en rappelle la nécessité dans les conditions générales d'utilisation, dans les déclarations de divulgation et dans le guide YT-GUIDE-USE.

3.9.7. Fréquence d'établissement des LCR

Une liste de révocation est générée par chaque autorité émettrice au moins toutes les 24 heures, et immédiatement après toute révocation. Le champ nextUpdate est positionné à 72 heures, ce qui laisse une marge suffisante pour qu'une indisponibilité de publication n'expose pas les utilisateurs de certificats à une liste périmée.

La liste de révocation des certificats d'autorités émettrices est générée par l'autorité racine 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 est exploité selon le protocole IETF RFC 6960. Il est disponible 24 heures sur 24, 7 jours sur 7 et accessible publiquement, sans contrôle d’accès ni frais. Les réponses sont signées par un répondeur délégué, certifié par l’autorité émettrice concernée.

Le délai maximum entre une révocation et sa prise en compte par ce service est de 24 heures.

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

L'emploi du service en ligne n'est pas imposé : un utilisateur de certificat peut se fier à la liste de révocation. Le service en ligne est en revanche le seul moyen d'obtenir un état plus récent que la dernière liste publiée, et il est recommandé pour tout usage dont l'enjeu justifie une information à jour.

3.9.11. Autres moyens disponibles d'information sur les révocations

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.

Aucun autre moyen d'information sur les révocations n'est exploité : une notification par message ou par flux de diffusion créerait une source d'état concurrente de la liste et du service en ligne, et un utilisateur de certificat ne saurait plus laquelle fait foi.

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

Une compromission ou une suspicion de compromission des données de création d'un titulaire entraîne la révocation immédiate du certificat, sans attendre l'établissement de la réalité de la compromission : le doute suffit, et le coût d'une révocation infondée est supporté par le prestataire selon le chapitre 3.9.3.1.

Une compromission ou une suspicion de compromission d'une clé de composante déclenche en outre la procédure du chapitre 4.7.3 : information de l'autorité nationale selon le chapitre 4.7.1, information des titulaires et des utilisateurs de certificats par le registre de publication, révocation de tous les certificats délivrés sous la clé compromise, 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 ces termes est instruite comme une demande de révocation selon le chapitre 3.9.3.1, après information du demandeur du caractère irréversible de celle-ci.

3.9.15. Procédure de traitement d'une demande de suspension

Sans objet : aucune procédure de suspension n'existe. Le renvoi du chapitre 3.9.14 vers la procédure de révocation est la seule voie ouverte.

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

Sans objet : aucun certificat ne peut être suspendu ; la question d'une durée maximale de suspension ne se pose donc pas.

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

Cette fonction est celle sur laquelle repose la confiance d'un utilisateur de certificat qui n'a aucune relation avec le prestataire. Elle est donc traitée comme la fonction la plus critique du service en matière de disponibilité, avant même la délivrance.

3.10.1. Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats est assurée par deux moyens complémentaires : la publication des listes de révocation dans le registre de publication, et le service d'information en ligne du chapitre 3.9.9.

Les deux moyens sont alimentés par la même source : l'inscription de la révocation opérée par la fonction de gestion des révocations. Aucun état n'est saisi séparément dans l'un ou l'autre, ce qui exclut qu'ils divergent.

Le point d'accès à chacun de ces moyens figure dans les certificats délivrés, respectivement dans les extensions CRL Distribution Points et Authority Information Access, de sorte qu'un utilisateur de certificat n'ait pas à le connaître par avance.

3.10.2. Disponibilité de la fonction

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

Ces engagements sont mesurés par une supervision continue dont les relevés rejoignent les journaux d'évènements du chapitre 4.4.1. Un dépassement est traité comme un incident au sens du chapitre 4.7.1 et donne lieu à une analyse de cause versée au dossier d'audit.

3.10.3. Dispositifs optionnels

Aucun dispositif optionnel d'information sur l'état des certificats n'est exploité. En particulier, aucune agrafe de réponse d'état n'est produite par le prestataire pour le compte d'un tiers, et aucun service d'annuaire n'expose les certificats de titulaires.

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

La relation prend fin par l'expiration du dernier certificat du titulaire sans renouvellement, par la révocation à sa demande, ou par la résiliation des conditions générales d'utilisation applicables.

À la fin de la relation, les certificats en cours sont révoqués, les facteurs d'authentification sont désactivés, et les données de création du titulaire sont détruites à l'intérieur du module selon le chapitre 5.2.10.2. Le dossier de preuve est conservé pendant la durée du chapitre 4.5.2 : la fin de la relation n'éteint pas l'obligation de conservation, qui est ce qui permet de vérifier a posteriori une signature produite pendant la relation.

Le titulaire est informé de ce que ses signatures et cachets antérieurs restent vérifiables après la fin de la relation, la vérification reposant sur le certificat et sur l'information d'état à la date de l'opération, et non sur l'existence d'un compte.

3.12. Séquestre de clé et recouvrement

Les deux chapitres qui suivent énoncent des absences. Elles sont documentées plutôt que passées sous silence, parce que l'absence de séquestre est ce qui rend le contrôle exclusif du signataire vérifiable.

3.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet : aucun séquestre de clé n'est pratiqué. Les données de création de signature et de cachet ne sont ni copiées, ni confiées à un tiers, ni recouvrables : elles sont générées dans le module cryptographique matériel et n'en sortent jamais en clair. Un séquestre serait au surplus contraire au contrôle exclusif exigé pour la signature électronique avancée par l'exigence 7 du référentiel [Ref_Serv_Conf_NonQual], puisqu'il ferait exister, hors du contrôle du signataire, un moyen de produire une signature à son nom.

Les sauvegardes chiffrées de clés d'autorité mentionnées au chapitre 5.2.4 ne constituent pas un séquestre : elles ne portent que sur des clés de composante, jamais sur des clés de titulaires, elles ne sortent pas du domaine du module cryptographique matériel sous forme utilisable, et leur restauration est soumise au quorum du chapitre 5.2.2.

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

Sans objet : aucun service de chiffrement n'est fourni et aucune clé de session n'est encapsulée. Les bi-clés délivrées servent exclusivement à la signature et au cachet, ce que l'extension Key Usage rend techniquement contraignant selon le chapitre 1.10.1.1.

4. MESURES DE SÉCURITÉ NON TECHNIQUES

Les mesures décrites dans ce chapitre et dans le chapitre 5 mettent en œuvre les exigences d'organisation, de ressources humaines, de gestion des biens, de contrôle d'accès, de sécurité physique et environnementale, de sécurité d'exploitation, de gestion des incidents, de collecte des preuves, de continuité d'activité et de cessation d'activité que la norme ETSI EN 319 401 impose à tout prestataire de services de confiance, comme le rappelle l'exigence 2 du référentiel [Ref_Serv_Conf_NonQual]. Elles reposent sur une analyse de risque documentée, revue au moins à la fréquence du contrôle interne du chapitre 7.1 et après tout incident majeur.

La politique de sécurité de l'information du prestataire est un document interne approuvé par la direction ; elle n'est pas publiée, la description détaillée des mesures de sécurité ne pouvant être rendue publique sans affaiblir celles-ci. Le présent chapitre en publie ce qui est nécessaire à la compréhension du service, sans élément de localisation ni de configuration : ni adresse, ni identité d'équipement, ni paramètre d'exploitation.

4.1. Mesures de sécurité physique

Les mesures physiques protègent le matériel qui porte les clés, les supports qui portent les archives et les parts de secret, et l'environnement qui conditionne la disponibilité des fonctions. Elles sont décrites ici sans aucun élément permettant de localiser un site ou d'identifier un équipement.

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.

Le site principal héberge l'exploitation courante ; le site secondaire héberge les moyens de reprise et une copie des sauvegardes. Les deux sites sont distincts et ne partagent ni leur alimentation, ni leur accès physique.

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.

> **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.

La pratique du contrôle d'accès comporte les éléments suivants.

- L'accès à la zone sensible est nominatif, limité aux fonctions qui en ont besoin, et révoqué le jour où la fonction cesse d'être exercée.
- Chaque entrée et chaque sortie de la zone sensible sont enregistrées ; le registre est revu selon la fréquence du chapitre 4.4.2.
- Toute intervention d'un tiers en zone sensible est accompagnée par une personne tenant un rôle de confiance, et consignée.

- Aucune opération sur une clé d'autorité n'est possible en dehors de la zone sensible et hors de la présence des porteurs de part de secret requis par le quorum du chapitre 5.2.2.
- Les droits d'accès sont revus à chaque contrôle interne et après tout changement d'attribution.

4.1.3. Alimentation électrique et climatisation

Chaque site dispose d'une alimentation électrique et d'une climatisation redondées, dimensionnées pour maintenir les fonctions du chapitre 1.7 pendant une coupure de la fourniture principale, et testées selon la fréquence du chapitre 4.7.4. Un défaut d'alimentation ou de climatisation est remonté comme un incident au sens du chapitre 4.7.1.

4.1.4. Vulnérabilité aux dégâts des eaux

Les zones sensibles ne comportent aucune canalisation qui ne leur soit nécessaire, sont équipées d'une détection de présence d'eau raccordée à la supervision, et sont implantées de manière à ne pas subir un écoulement provenant d'un niveau supérieur. Le déclenchement de la détection est traité comme un incident.

4.1.5. Prévention et protection incendie

Chaque site est équipé d'une détection incendie raccordée à la supervision et d'un moyen d'extinction adapté à des équipements électroniques. Les consignes d'évacuation et d'intervention sont écrites, affichées et exercées ; l'exercice est consigné au dossier d'audit.

4.1.6. Conservation des supports

Les supports portant des données sensibles — sauvegardes, parts de secret, archives — sont conservés dans des contenants scellés, dans des coffres distincts en zone sensible, avec un registre daté de chaque remise et de chaque restitution.

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

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

4.1.7. Mise hors service des supports

Un support qui a porté des données sensibles est effacé de manière irréversible ou détruit physiquement avant toute sortie de la zone sensible. L'opération est exécutée sous double contrôle et donne lieu à un procès-verbal conservé au dossier d'audit ; aucun support n'est réemployé hors du périmètre sans cette opération.

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 et une copie est conservée hors du site principal. Leur restauration est soumise au même quorum que les opérations sur les clés, et elle est exercée 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

Les mesures procédurales reposent sur trois principes : les rôles sont des fonctions et non des personnes ; une opération sensible exige plus d'une personne ; celui qui contrôle n'exécute pas.

4.2.1. Rôles de confiance

Les rôles de confiance sont des FONCTIONS. Une personne peut tenir plusieurs rôles dans les limites du chapitre 4.2.4, et un rôle peut être tenu successivement par plusieurs personnes ; ce sont les attributions qui sont fixées ici, jamais une personne.

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

Chaque attribution de rôle est notifiée par écrit, acceptée par écrit, et retirée par écrit. La liste des rôles effectivement attribués est tenue à jour et revue à chaque contrôle interne.

4.2.2. Nombre de personnes requises par tâches

Tâche	Nombre de personnes et rôles requis
Génération d'une bi-clé d'autorité	Cérémonie : quorum de 3 porteurs de part de secret parmi 5, un opérateur, un témoin et un contrôleur, sous double contrôle
Activation d'une clé privée d'autorité	Quorum de 3 porteurs de part de secret parmi 5, sous double contrôle
Sauvegarde ou restauration d'une clé d'autorité	Double contrôle au minimum, et le même quorum que l'activation pour la restauration

Tâche	Nombre de personnes et rôles requis
Destruction d'une clé privée d'autorité	Double contrôle, en présence d'un témoin, avec procès-verbal
Révocation d'un certificat de composante	Double contrôle, décision consignée
Révocation d'un certificat de titulaire	Une personne tenant un rôle habilité, après authentification de l'origine selon le chapitre 2.3.3
Délivrance d'un certificat de titulaire	Aucune intervention manuelle : la chaîne du chapitre 3.3.1 est automatique et tracée
Mise en production d'une évolution des systèmes	Séparation du demandeur, de l'exécutant et du valideur, selon le chapitre 5.6

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.

4.2.3. Identification et authentification pour chaque rôle

Chaque personne tenant un rôle de confiance dispose d'une identité nominative distincte ; aucun compte partagé n'est employé pour une opération sensible. L'accès aux fonctions correspondantes est subordonné à une authentification forte et n'est ouvert qu'aux rôles qui en ont besoin.

L'identification est ce qui rend les journaux d'évènements du chapitre 4.4.1 exploitables : un enregistrement qui ne désignerait qu'un compte technique ne permettrait pas d'établir qui a agi, et la traçabilité serait perdue.

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.

Le respect de cette règle est vérifié à chaque attribution de rôle et à chaque contrôle interne ; un cumul constaté est un écart traité selon le chapitre 7.5 et corrigé avant toute nouvelle opération sensible par la personne concernée.

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

Les mesures décrites ci-dessous portent sur des fonctions et sur des pratiques ; aucune personne n'est nommée dans le présent document, et aucune donnée à caractère personnel relative au personnel n'y figure.

4.3.1. Qualifications, compétences et habilitations requises

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.

Les compétences attendues sont définies par rôle et vérifiées avant l'affectation : connaissance des politiques et de la présente déclaration, maîtrise des procédures du rôle, et compréhension des conséquences d'un écart. Aucune personne n'est affectée à un rôle de confiance sur la seule base d'une compétence technique.

4.3.2. Procédures de vérification des antécédents

La vérification des antécédents professionnels est conduite avant l'affectation, dans les limites permises par la loi et avec l'information de la personne concernée. Elle porte sur l'identité, le parcours professionnel déclaré et les références ; son résultat est consigné sous une forme qui n'expose aucune donnée qui ne serait pas nécessaire à la décision d'affectation.

Les données recueillies à cette occasion sont traitées selon le chapitre 8.2 et conservées pendant la durée de l'affectation augmentée de la durée légale applicable, puis supprimées.

4.3.3. Exigences en matière de formation initiale

La formation initiale précède l'exercice effectif du rôle. Elle couvre les politiques et la présente déclaration, les procédures du rôle, la politique de sécurité de l'information, les obligations de confidentialité et de protection des données à caractère personnel, et la conduite à tenir en cas d'incident. Elle est sanctionnée par une attestation versée au dossier d'audit.

4.3.4. Exigences et fréquence en matière de formation continue

Une formation continue est dispensée au moins annuellement, et à chaque évolution substantielle des politiques, de la présente déclaration, des procédures ou des systèmes. Le suivi de ces formations est vérifié lors du contrôle interne.

4.3.5. Fréquence et séquence de rotation entre différentes attributions

Aucune rotation périodique obligatoire n'est imposée : au format d'équipe du prestataire, une rotation systématique multiplierait les personnes ayant tenu un rôle sensible sans améliorer le contrôle. La garantie recherchée est obtenue autrement, par la séparation des attributions du chapitre 4.2.4, par le contrôle indépendant du chapitre 7.2 et par la traçabilité nominative du chapitre 4.2.3.

Une rotation est en revanche opérée lorsqu'un contrôle fait apparaître un cumul de fait, lorsqu'une absence durable empêcherait la tenue d'un rôle, ou lorsque la personne concernée en fait la demande motivée.

4.3.6. Sanctions en cas d'actions non autorisées

Une action non autorisée entraîne le retrait immédiat des droits d'accès de la personne concernée, l'ouverture d'une analyse selon le chapitre 4.7.1, et les suites disciplinaires prévues par le droit du travail applicable. Lorsque l'action a pu affecter une clé, un certificat ou une archive, la mesure conservatoire du chapitre 7.5 est appliquée sans attendre la conclusion de l'analyse.

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

Le personnel d'un tiers qui concourt à une fonction du chapitre 1.7 — au premier rang duquel le personnel de la plateforme exerçant les fonctions d'autorité d'enregistrement — est soumis par contrat aux mêmes exigences que le personnel du prestataire : vérification d'identité et d'antécédents, engagement de confidentialité écrit, formation initiale et continue, et respect de la séparation des attributions.

Le prestataire vérifie l'effectivité de ces obligations par le droit d'audit stipulé au contrat, exercé selon le chapitre 7. Aucune sous-délégation n'est admise sans autorisation écrite préalable.

4.3.8. Documentation fournie au personnel

Chaque personne tenant un rôle de confiance dispose des politiques, de la présente déclaration, de la politique de sécurité de l'information, des procédures de son rôle et des consignes d'incident, dans leur version en vigueur. La diffusion d'une nouvelle version est tracée, et l'accusé de prise de connaissance est conservé.

4.4. Procédures de constitution des données d'audit

La journalisation est ce qui rend le service vérifiable a posteriori. Un évènement non enregistré est un évènement dont il sera impossible d'établir qu'il a eu lieu ; c'est pourquoi la perte d'un flux de journalisation est traitée comme un incident au même titre qu'une atteinte.

4.4.1. Type d'évènements à enregistrer

Les évènements suivants sont enregistrés, avec la date, l'heure, l'identité de l'auteur et le résultat.

- Toute opération sur une clé d'autorité : génération, activation, désactivation, sauvegarde, restauration, destruction, ainsi que chaque cérémonie et son procès-verbal.
- Toute demande de certificat, son acceptation ou son rejet motivé, et la délivrance correspondante.
- Toute vérification d'identité opérée par l'autorité d'enregistrement, avec la fonction qui l'a conduite.
- Toute acceptation de certificat par un titulaire.
- Toute demande de révocation, l'authentification de son origine, la cause retenue, l'heure d'effet et l'heure de publication.
- Toute génération et toute publication d'une liste de révocation, et toute réponse d'état produite en cas d'anomalie.
- Toute opération de signature ou de cachet exécutée pour le compte d'un titulaire, avec l'empreinte des données et la référence du certificat.
- Tout accès physique à une zone sensible, et toute tentative d'accès en échec.
- Toute attribution, modification ou retrait d'un rôle de confiance ou d'un droit d'accès.
- Tout démarrage et tout arrêt d'un système concourant à une fonction du chapitre 1.7, et tout changement de configuration.
- Tout incident de sécurité, sa qualification, son traitement et sa clôture.
- Toute évolution des documents du registre de publication et toute notification adressée à l'autorité nationale.

Un enregistrement porte l'identité de la personne, jamais un compte partagé, et ne contient aucune donnée à caractère personnel qui ne serait pas nécessaire à l'établissement du fait consigné. Les données à signer ne sont pas journalisées : seule leur empreinte l'est.

4.4.2. Fréquence de traitement des journaux d'évènements

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

L'analyse est conduite par le responsable de sécurité. Une anomalie donne lieu à une analyse immédiate et, lorsqu'elle est qualifiée d'incident, à la procédure du chapitre 4.7.1. Le rapprochement entre composantes est ce qui permet de détecter un évènement enregistré par l'une et absent de l'autre, c'est-à-dire une perte de journalisation.

4.4.3. Période de conservation des journaux d'évènements

Les journaux sont conservés sur site pendant 1 mois, puis versés aux archives et conservés selon le chapitre 4.5.2. Le versement ne les rend pas moins accessibles : le délai maximum de récupération du chapitre 4.5.7 s'y applique.

4.4.4. Protection des journaux d'évènements

Les journaux sont protégés en intégrité et en confidentialité. La lecture est réservée aux rôles qui en ont besoin, au premier rang desquels le responsable de sécurité et le contrôleur ; l'écriture est réservée aux systèmes qui produisent les enregistrements ; aucune fonction ne permet la modification ni la suppression d'un enregistrement.

Un contrôle d'intégrité est appliqué à chaque lot de journaux versé aux archives, et vérifié à chaque récupération selon le chapitre 4.5.7.

4.4.5. Procédure de sauvegarde des journaux d'évènements

Les journaux sont sauvegardés selon la règle du chapitre 4.1.8, avec une copie hors site. La sauvegarde est vérifiée par une restauration exercée selon la fréquence du chapitre 4.7.4.

4.4.6. Système de collecte des journaux d'évènements

Les enregistrements sont produits par chaque composante et centralisés dans un dépôt d'audit protégé, dont la source de temps est celle du chapitre 5.8. La centralisation est ce qui rend possible le rapprochement du chapitre 4.4.2 ; l'absence de flux d'une composante pendant une période attendue est elle-même une anomalie.

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

Les personnes tenant un rôle de confiance sont informées, lors de la formation initiale et par la documentation du chapitre 4.3.8, de la nature des évènements enregistrés et de la finalité de cet enregistrement ; aucune notification n'est adressée évènement par évènement.

Le titulaire est informé, par les conditions générales d'utilisation et par la déclaration de divulgation, de ce que ses demandes, acceptations et opérations sont enregistrées, de la finalité de ces enregistrements et de la durée de leur conservation, conformément au chapitre 8.2.

4.4.8. Évaluation des vulnérabilités

Une veille sur les vulnérabilités affectant les composants employés est tenue en continu ; une vulnérabilité pertinente donne lieu à une analyse d'impact et à une correction dont le délai est fonction de la criticité. Une évaluation technique des systèmes exposés est conduite selon la fréquence du contrôle interne du chapitre 7.1 et après toute évolution substantielle.

Les résultats de ces évaluations ne sont pas publiés, pour la raison énoncée au chapitre 7.6 ; ils sont communiqués à l'autorité nationale sur sa demande.

4.5. Archivage des données

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.

Cette convention de preuve est celle qu'exige l'exigence 13 du référentiel [Ref_Serv_Conf_NonQual]. Elle est publiée avec les conditions générales d'utilisation applicables à chaque service, de sorte que le titulaire et l'utilisateur de certificat connaissent, avant tout usage, la nature des preuves produites, leur mode d'établissement et de conservation, les conditions dans lesquelles elles sont mises à disposition en cas de désaccord, et les engagements des parties sur leur acceptation.

Le présent chapitre décrit ce qui est archivé, pendant combien de temps, comment les archives sont protégées, sauvegardées, datées, collectées et restituées.

4.5.1. Types de données à archiver

Les données archivées sont toutes les informations relatives à la fourniture d'un service de confiance ou échangées avec le prestataire dans le cadre d'une transaction électronique, qui servent à assurer la disponibilité et la continuité du service — y compris en cas de cessation — et à fournir des preuves en cas de contestation. C'est le périmètre que fixe l'exigence 16 du référentiel [Ref_Serv_Conf_NonQual].

- Les dossiers de preuve constitués à l'enregistrement : informations vérifiées, référence de la pièce produite, résultat de chaque contrôle, fonction ayant opéré et date.
- Les demandes de certificat, les décisions d'acceptation ou de rejet motivé, et les acceptations de certificats par les titulaires.
- Les certificats délivrés, les demandes et décisions de révocation, et les listes de révocation publiées.
- Les enregistrements des opérations de signature et de cachet exécutées pour le compte des titulaires.
- Les journaux d'évènements du chapitre 4.4.1, après leur période de conservation sur site.
- Les procès-verbaux de cérémonie de clés, les scripts approuvés et les registres de remise des parts de secret.
- Les versions successives des politiques, de la présente déclaration et des documents du registre de publication.
- Les contrats encadrant les fonctions déléguées, les rapports d'audit et les plans d'action.
- Les notifications adressées à l'autorité nationale et les accusés de réception correspondants.

Le dossier de preuve d'un titulaire est constitué à l'enregistrement, complété à chaque évènement du cycle de vie de ses certificats, et scellé selon le chapitre 4.5.3.

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 est celle de l'article 18 du décret n° 2-22-687, rendue applicable aux services autres que qualifiés par son article 23, et reprise par l'exigence 19 du référentiel [Ref_Serv_Conf_NonQual]. Elle survit à la cessation d'activité : le plan de cessation du chapitre 4.8 en organise l'exécution.

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

La suppression en fin de période est ce qu'exige l'exigence 20 du référentiel ; elle est exécutée sous double contrôle et son procès-verbal est lui-même conservé, faute de quoi il serait impossible d'établir qu'une donnée a été détruite plutôt que perdue.

4.5.3. Protection des archives

Les archives sont conservées par des systèmes fiables au sens de l'exigence 15 du référentiel [Ref_Serv_Conf_NonQual], qui garantissent que l'authenticité des données conservées peut être vérifiée, que seules des personnes autorisées peuvent introduire ou modifier des données, et qu'aucune donnée n'est rendue publiquement disponible pour un traitement sans le consentement de la personne concernée.

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

Le scellement est recommandé par l'exigence 14 du référentiel ; le prestataire le met en œuvre systématiquement, l'horodatage du chapitre 4.5.5 lui donnant en outre une date opposable. L'accès aux archives est nominatif, journalisé, et réservé aux rôles du chapitre 4.2.1 qui en ont besoin.

4.5.4. Procédure de sauvegarde des archives

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

Une copie des archives est conservée sur le site secondaire. La restauration est exercée 1 fois par an, au minimum et donne lieu à un procès-verbal ; une restauration qui n'aboutit pas est un incident au sens du chapitre 4.7.1.

4.5.5. Exigences d'horodatage des données

Chaque dossier de preuve et chaque lot d'archives est horodaté au moyen du service d'horodatage du prestataire, régi par YT-PH-TSA (1.3.6.1.4.1.[PEN].1.1.3). L'horodatage donne au scellement du chapitre 4.5.3 une date dont l'exactitude déclarée et la traçabilité à l'UTC sont celles de cette politique.

Les journaux d'évènements portent la date et l'heure de la source du chapitre 5.8, commune à toutes les composantes, ce qui rend le rapprochement du chapitre 4.4.2 possible.

4.5.6. Système de collecte des archives

Les archives sont collectées depuis chaque composante par un processus qui vérifie l'intégrité de chaque lot à la réception, l'inscrit à un inventaire, et rejette un lot dont le contrôle d'intégrité échoue. Un rejet est un incident.

4.5.7. Procédures de récupération et de vérification des archives

Le délai maximum de récupération d'une archive est de 2 jours ouvrés. La demande émane d'un rôle habilité, d'un titulaire justifiant de son identité pour ce qui le concerne, ou d'une autorité dans l'exercice de ses attributions ; elle est journalisée.

Chaque récupération est accompagnée de la vérification du scellement et du contrôle d'intégrité du lot. Une archive dont la vérification échoue est traitée comme un incident et fait l'objet d'une recherche sur la copie hors site.

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.

La pratique du changement de clé est la suivante.

1. Le remplacement est planifié à partir de la date calculée par la règle ci-dessus, et non à l'approche de l'expiration.
2. La nouvelle bi-clé est générée en cérémonie selon le chapitre 5.1.1.1, avec un nouveau suffixe de génération.
3. Le nouveau certificat d'autorité est publié dans le registre de publication 24 heures au moins avant la première délivrance sous cette clé.
4. L'ancienne clé cesse de signer des certificats mais continue de signer les listes de révocation des certificats qu'elle a délivrés, jusqu'à l'expiration du dernier d'entre eux.
5. L'ancienne clé est détruite selon le chapitre 5.2.10.1 après cette échéance, et la destruction fait l'objet d'un procès-verbal.

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

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 d'affecter la sécurité du service est remonté sans délai au responsable de sécurité, qui le qualifie, décide des mesures conservatoires et ouvre le traitement. La chaîne de remontée, les moyens de contact et les rôles de décision sont écrits et exercés.

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.

Cette notification est celle qu'imposent l'article 40 de la loi n° 43-20 et l'article 19 du décret n° 2-22-687, rendu applicable aux services autres que qualifiés par son article 23. Elle est adressée

immédiatement après la connaissance de l'atteinte, sans attendre la fin de l'analyse ; elle est complétée ensuite.

Le traitement d'un incident comporte la qualification, les mesures conservatoires, l'analyse de cause, la correction, la vérification de l'efficacité de celle-ci et la clôture. Chaque étape est datée et consignée ; le dossier rejoint les archives du chapitre 4.5.1.

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 du chapitre 4.1.8 et sur les moyens du site secondaire. L'ordre de reprise est fixé par le plan de continuité : la fonction de gestion des révocations et la fonction d'information sur l'état des certificats sont rétablies avant la fonction de délivrance, un utilisateur de certificat privé d'information d'état étant plus exposé qu'un demandeur privé de délivrance.

Une ressource corrompue n'est jamais remise en service sans vérification d'intégrité ; en cas de doute, elle est reconstruite à partir d'une source maîtrisée plutôt que réparée.

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

1. La clé compromise est immédiatement mise hors service et le certificat de la composante est révoqué selon le chapitre 3.9.3.2.
2. L'autorité nationale est informée selon le chapitre 4.7.1.
3. L'information est publiée dans le registre de publication, avec l'indication des certificats affectés et de la conduite à tenir par les utilisateurs de certificats.
4. Tous les certificats délivrés sous la clé compromise sont révoqués et les listes de révocation correspondantes sont publiées sans attendre l'échéance périodique.
5. Une nouvelle bi-clé est générée en cérémonie selon le chapitre 5.1.1.1 et le nouveau certificat d'autorité est publié.
6. Les titulaires concernés se voient délivrer de nouveaux certificats selon le chapitre 3.7, sans frais, la cause ne leur étant pas imputable.
7. L'analyse de cause et le plan d'action sont versés au dossier d'audit et suivis selon le chapitre 7.5.

La compromission de la clé de l'autorité racine YORYX TRUST Root CA G1 est le cas le plus grave : elle entraîne la révocation de toutes les autorités émettrices et de tous les certificats délivrés, la publication d'une nouvelle racine et la reprise de la chaîne de confiance par les utilisateurs de certificats. Le maintien de cette clé hors ligne, activée seulement en cérémonie, est ce qui rend ce scénario improbable.

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

Un plan de continuité et de reprise est écrit, approuvé et testé 1 fois par an ; les sauvegardes sont restaurées à l'essai 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.

Le site secondaire héberge les moyens permettant de rétablir les fonctions du chapitre 1.7 après un sinistre affectant le site principal. Le plan de continuité d'activité est en outre une condition de

l'agrément posée par l'article 33 e) de la loi n° 43-20 ; il est tenu à jour indépendamment de la démarche d'agrément.

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.

Ce délai est celui de l'article 37 de la loi n° 43-20. Le plan de cessation, écrit et tenu à jour, organise les opérations suivantes.

1. Information préalable de l'autorité nationale, dans le délai ci-dessus.
2. Information des titulaires, des utilisateurs de certificats connus et de la plateforme, par le registre de publication et par les espaces des titulaires.
3. Arrêt de la délivrance de nouveaux certificats à la date annoncée.
4. Maintien de la fonction de gestion des révocations et de la fonction d'information sur l'état des certificats jusqu'à l'expiration du dernier certificat délivré.
5. Révocation des certificats encore en cours de validité à la date de cessation effective, lorsque leur maintien n'est pas assuré par un repreneur.
6. Destruction des clés privées des autorités selon le chapitre 5.2.10.1, sous double contrôle et avec procès-verbal.
7. Transfert ou conservation des archives pour la durée restante de la période du chapitre 4.5.2, l'obligation de conservation de 7 ans survivant à la cessation.
8. Remise à l'autorité nationale des éléments qu'elle demande, et clôture documentée du plan.

Lorsqu'un autre prestataire reprend l'activité, la reprise porte sur les archives et sur la fonction d'information sur l'état des certificats ; elle ne dispense d'aucune des étapes ci-dessus et fait l'objet d'un accord écrit porté à la connaissance de l'autorité nationale.

5. MESURES DE SÉCURITÉ TECHNIQUES

5.1. Génération et installation de bi-clés

Le présent chapitre décrit où et comment chaque bi-clé est produite, comment les clés publiques circulent, quelles tailles sont retenues et comment la qualité de la génération est assurée.

5.1.1. Génération des bi-clés

Toute bi-clé mise en œuvre par le prestataire — clé d'autorité, clé de titulaire, clé de répondeur, clé d'unité d'horodatage — est générée à l'intérieur du module cryptographique matériel. Aucune bi-clé n'est générée par un logiciel d'usage général, et aucune clé privée n'est produite hors du module.

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.

Le script de cérémonie, écrit et approuvé avant exécution, fixe au minimum les points suivants ; il est le document dont l'exécution est ensuite constatée par le procès-verbal.

1. L'objet de la cérémonie : quelle autorité, quelle génération de bi-clé, quel algorithme et quelle taille, selon le chapitre 9.5.
2. Les rôles requis et le nom des fonctions qui les tiennent : porteurs de part de secret en nombre suffisant pour le quorum, opérateur, témoin, contrôleur.
3. L'état initial attendu du matériel et les contrôles préalables, y compris la vérification des scellés des contenants de parts de secret.
4. La séquence exacte des opérations, chacune énoncée de manière à être exécutée sans interprétation.
5. Les valeurs à saisir, notamment le nom distinctif du chapitre 2.1.1 et la période de validité du chapitre 9.2, de sorte qu'aucune valeur ne soit improvisée pendant la cérémonie.
6. Les points d'arrêt : les conditions dans lesquelles la cérémonie est interrompue et l'état dans lequel le matériel est laissé.
7. Les opérations de sauvegarde de la clé et de remise des parts de secret, avec le registre à signer.
8. Les vérifications finales : cohérence du certificat produit, empreinte relevée et consignée, remise en état hors ligne du matériel.

La cérémonie se déroule en zone sensible, sous double contrôle et en présence des témoins ; elle donne lieu à un procès-verbal signé par chaque participant, qui relève l'heure de chaque étape, les écarts éventuels au script et leur traitement, ainsi que l'empreinte du certificat produit. Le procès-verbal, le script approuvé et le registre de remise des parts rejoignent les archives du chapitre 4.5.1.

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

La clé de l'autorité racine YORYX TRUST Root CA G1 est 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. En dehors d'une cérémonie, le matériel qui la porte demeure hors ligne.

5.1.1.2. Clés porteurs générées par l'AC

Les données de création de signature ou 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 est déclenchée par la fonction de génération des certificats, pour un titulaire déjà identifié, et se déroule dans le module cryptographique matériel selon les algorithmes et les tailles du chapitre 9.6. La clé privée est immédiatement liée aux données d'activation du titulaire au sens du chapitre 5.4.1.2 ; aucune fenêtre n'existe pendant laquelle la clé serait utilisable sans l'action d'autorisation du titulaire.

Le titulaire n'a ni clé USB, ni carte à puce, ni lecteur à se procurer, et rien à installer : 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. Le modèle de service retenu ne comporte ni support remis, ni logiciel installé chez le titulaire, et la fonction de génération n'expose aucune interface permettant de soumettre une clé publique d'origine externe, comme le rappelle le chapitre 2.2.1.

5.1.1.4. Transmission de la clé privée à son propriétaire

Sans objet : aucune clé privée n'est transmise à quiconque. Les données de création du titulaire demeurent dans le module cryptographique matériel pour toute leur durée de vie et y sont détruites selon le chapitre 5.2.10.2 ; il n'existe aucun canal, chiffré ou non, par lequel elles pourraient être remises.

5.1.2. Transmission de la clé publique à l'AC

La clé publique d'un titulaire n'est pas transmise : elle est produite par le module dans la même opération que la clé privée, à la demande de la fonction de génération des certificats, qui la reçoit directement du module. Le trajet est interne au domaine du prestataire et n'emprunte aucun réseau exposé.

La clé publique d'une composante est relevée pendant la cérémonie du chapitre 5.1.1.1 et son empreinte est consignée au procès-verbal, ce qui permet de vérifier ultérieurement que le certificat publié porte bien la clé générée.

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, 24 heures sur 24, 7 jours sur 7, sans contrôle d'accès ni frais, et diffusés 24 heures au moins avant la première délivrance sous la clé correspondante.

L'utilisateur de certificat vérifie l'empreinte du certificat racine qu'il installe, par un canal distinct de celui du téléchargement ; le guide YT-GUIDE-USE indique la démarche. Cette vérification est ce qui protège la chaîne de confiance à son point d'ancrage, qu'aucune signature ne peut protéger.

5.1.4. Tailles des clés

Bi-clé	Algorithme et taille	Algorithme de signature
YORYX TRUST Root CA G1	RSA 4096 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
YORYX TRUST Signature CA G1	RSA 4096 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
YORYX TRUST Seal CA G1	RSA 4096 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
YORYX TRUST Timestamping CA G1	RSA 4096 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)
YORYX TRUST TSU 1 G1	RSA 3072 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 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.

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

La qualité des bi-clés est assurée par le module cryptographique matériel lui-même, dont c'est l'un des objectifs de sécurité énoncés à l'annexe 9.1 des politiques : générateur d'aléa qualifié par le module, contrôles internes à la génération, et passage en état sûr en cas de détection d'erreur.

La fonction de génération des certificats vérifie en outre, avant toute signature, que la clé publique reçue correspond à l'algorithme et à la taille attendus pour le certificat demandé, et rejette la demande dans le cas contraire.

5.1.6. Objectifs d'usage de la clé

L'usage de chaque bi-clé est fixé à la génération et rendu contraignant par l'extension Key Usage marquée critique, selon les gabarits publiés en annexe des politiques. Le tableau du chapitre 1.10.1.2 récapitule l'usage de chaque clé de composante.

Aucune bi-clé ne cumule un usage de signature et un usage de chiffrement ; aucune bi-clé de titulaire ne sert à l'authentification.

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

Une clé privée n'existe qu'à l'intérieur du module cryptographique matériel, n'en sort jamais en clair, n'est activée que sous les conditions du chapitre 5.2.8 et est détruite selon le chapitre 5.2.10. Les chapitres qui suivent énoncent chacune de ces étapes, y compris celles qui ne s'appliquent pas et dont l'absence est elle-même une garantie.

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 par les autorités de certification présente les propriétés suivantes.

- les bi-clés d’autorité et les données de création de signature ou 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

Textes visés en cible pour ces propriétés :

- 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.

> **Point ouvert —** Les formalités préalables prévues par l’article 46 de la loi n° 43-20 pour les moyens de cryptologie sont accomplies auprès de l’autorité nationale.

5.2.1.2. Dispositifs de création de signature des porteurs

Aucun dispositif matériel n'est remis au titulaire : la fonction de création de signature est assurée, pour son compte et sous son contrôle exclusif, 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 des politiques.

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.

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.

Aucune part de secret n'est détenue en double par une même personne, et aucune personne ne détient plus d'une part, selon la règle du chapitre 4.2.4. Le quorum est vérifié physiquement au début de chaque cérémonie et consigné au procès-verbal.

5.2.3. Séquestre de la clé privée

Sans objet : aucune clé privée n'est mise sous séquestre, ni pour les autorités, ni pour les titulaires ; le chapitre 3.12.1 en énonce la raison et distingue la sauvegarde chiffrée du chapitre 5.2.4, qui n'est pas un séquestre.

5.2.4. Copie de secours de la clé privée

Les clés privées des autorités font l'objet d'une sauvegarde chiffrée, produite par le module cryptographique matériel et ne sortant jamais de celui-ci sous forme utilisable. Sa restauration est soumise au quorum du chapitre 5.2.2 et exercée sous double contrôle.

Les données de création des titulaires ne font l'objet d'aucune copie de secours : leur perte est traitée par la révocation du certificat et la délivrance d'un nouveau selon le chapitre 3.7, ce qui préserve le contrôle exclusif du signataire au prix d'une reprise de la bi-clé.

5.2.5. Archivage de la clé privée

Sans objet : aucune clé privée n'est archivée. Une clé privée archivée resterait utilisable après la fin de vie du certificat qui la couvre, ce qui contredirait la destruction prévue aux chapitres 5.2.10.1 et 5.2.10.2. Seules les clés publiques sont archivées, 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 ou depuis le module cryptographique matériel. Le seul mouvement admis est la sauvegarde chiffrée du chapitre 5.2.4 et sa restauration, l'une et l'autre soumises au quorum et au double contrôle, et l'une et l'autre journalisées.

Un transfert entre modules, lorsqu'il est nécessaire à la continuité d'activité entre le site principal et le site secondaire, emprunte le même mécanisme et se déroule en cérémonie.

5.2.7. Stockage de la clé privée dans un module cryptographique

Les clés privées demeurent dans le module cryptographique matériel pendant toute leur durée de vie ; elles y sont non exportables et non extractibles, et aucune copie en clair n'existe hors du

module. Le module détecte et signale les tentatives d'atteinte physique et passe en état sûr lorsqu'il en détecte une.

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 n'a lieu que dans le cadre d'une opération planifiée : cérémonie de génération, signature d'un certificat d'autorité émettrice, signature d'une liste de révocation d'autorités, ou restauration. Elle est journalisée avec l'identité des porteurs de part présents.

5.2.8.2. Clés privées des porteurs

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

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.

L'activation est propre à chaque opération : elle ne persiste pas au-delà de l'opération autorisée, et une session ouverte ne vaut pas autorisation. C'est ce qui distingue l'accès au service de l'autorisation d'une signature.

5.2.9. Méthode de désactivation de la clé privée

5.2.9.1. Clés privées d'AC

À l'issue de chaque opération planifiée, la clé d'autorité est désactivée et le matériel qui la porte est remis dans son état de repos ; pour l'autorité racine, cet état est hors ligne. La désactivation est constatée au procès-verbal de la cérémonie ou au journal d'évènements selon le cas.

5.2.9.2. Clés privées des porteurs

Les données de création d'un titulaire sont désactivées à la fin de chaque opération de signature ou de cachet. Elles le sont également, de manière durable, à la révocation du certificat, à l'expiration de celui-ci et à la fin de la relation selon le chapitre 3.11 ; la désactivation durable est suivie de la destruction du chapitre 5.2.10.2.

5.2.10. Méthode de destruction des clés privées

5.2.10.1. Clés privées d'AC

La destruction d'une clé privée d'autorité s'exécute à l'intérieur du module cryptographique matériel, en cérémonie, sous double contrôle et en présence de témoins, selon un script approuvé au préalable. Elle porte sur la clé et sur toutes ses sauvegardes chiffrées, et donne lieu à un procès-verbal signé conservé au dossier d'audit.

Elle intervient après le changement de clé du chapitre 4.6, lorsque le dernier certificat délivré sous cette clé a expiré, ou dans le cadre de la cessation d'activité du chapitre 4.8, ou immédiatement en cas de compromission selon le chapitre 4.7.3.

5.2.10.2. Clés privées des porteurs

Les données de création d'un titulaire sont détruites à l'intérieur du module cryptographique matériel après la révocation ou l'expiration du certificat correspondant et après la fin de la relation du chapitre 3.11. La destruction est journalisée ; elle porte sur la clé elle-même, aucune sauvegarde n'existant selon le chapitre 5.2.4.

La destruction n'affecte pas la vérifiabilité des signatures produites antérieurement : celle-ci repose sur le certificat et sur l'information d'état conservés selon le chapitre 4.5.1, non sur la subsistance de la clé privée.

5.2.11. Niveau d'évaluation sécurité du module cryptographique

Les textes visés comme cibles pour le niveau d'évaluation sont ceux du chapitre 5.2.1.1.

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.

> **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.

5.3. Autres aspects de la gestion des bi-clés

5.3.1. Archivage des clés publiques

Les clés publiques sont archivées avec les certificats qui les portent, selon le chapitre 4.5.1, et conservées pendant la durée du chapitre 4.5.2. Cet archivage est ce qui permet de vérifier, après l'expiration d'un certificat, une signature produite pendant sa période de validité.

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

Bi-clé et certificat	Durée de vie
YORYX TRUST Root CA G1	10 ans
Autorité de certification émettrice	6 ans
YORYX TRUST TSU 1 G1	5 ans
Répondeur d'information sur l'état des certificats	1 an
Certificat de signature — niveau simple	1 an
Certificat de signature — niveau avancé	3 ans

Bi-clé et certificat	Durée de vie
Certificat de cachet — niveau simple	1 an
Certificat de cachet — 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 couvre : aucune bi-clé n'est recertifiée, selon le chapitre 3.6, de sorte que la durée de vie de la clé et celle du certificat ne peuvent diverger.

5.4. Données d'activation

Les données d'activation sont ce sans quoi une clé privée ne peut être mise en œuvre. Elles prennent deux formes très différentes : des parts de secret réparties entre plusieurs porteurs pour une clé d'autorité, et les facteurs d'authentification que le titulaire est seul à détenir pour ses propres données de création.

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 données d'activation d'une clé d'autorité sont les parts de secret réparties selon le quorum du chapitre 5.2.2. Elles sont générées par le module cryptographique matériel pendant la cérémonie, remises immédiatement à leurs porteurs dans des contenants scellés, et inscrites au registre de remise.

Aucune part n'est produite en dehors d'une cérémonie, aucune part n'est reproduite, et aucune part n'est conservée par l'opérateur de la cérémonie.

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

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 facteurs d'authentification sont enrôlés par le titulaire lui-même lors de son inscription sur la plateforme, après vérification de son identité selon le chapitre 2.2.2. Ils ne sont ni générés ni détenus par le prestataire, qui n'en conserve que les éléments de vérification.

Cette pratique est ce qui donne son sens au contrôle exclusif : une donnée d'activation produite par le prestataire et remise au titulaire aurait, à un instant, existé hors de la détention exclusive de celui-ci.

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 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.

Le porteur d'une part est tenu par un engagement écrit d'en assurer la confidentialité, l'intégrité et la disponibilité, et de signaler sans délai toute atteinte au scellé. Une part dont le scellé est rompu est réputée compromise : la clé correspondante est traitée selon le chapitre 4.7.3.

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

Le titulaire protège ses facteurs d'authentification, ne les communique à personne et ne les enregistre pas en clair ; cette obligation figure dans les conditions générales d'utilisation. Le prestataire ne détient aucun facteur en clair et ne peut donc ni le restituer, ni le rejouer.

Perdre un moyen d’authentification ne fait perdre aucune donnée de création de signature ou de cachet : cela révoque ce moyen, que le titulaire réenrôle.

5.4.3. Autres aspects liés aux données d'activation

Le renouvellement d'un facteur d'authentification suit la procédure d'enrôlement du chapitre 5.4.1.2, précédée de la vérification de l'identité du titulaire à un niveau au moins équivalent à celui de l'enregistrement initial. La désactivation d'un facteur est immédiate et journalisée.

La perte de tous les facteurs d'un titulaire n'expose pas ses données de création : elle rend le service inaccessible jusqu'au réenrôlement, et devient une cause de révocation seulement dans le cas prévu au chapitre 3.9.1.1.

5.5. Mesures de sécurité des systèmes informatiques

5.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

- Chaque système concourant à une fonction du chapitre 1.7 est réduit aux services strictement nécessaires à cette fonction.
- L'accès administratif est nominatif, soumis à une authentification forte, limité aux rôles du chapitre 4.2.1 et journalisé selon le chapitre 4.4.1.
- Les correctifs de sécurité sont appliqués selon la criticité déterminée par la veille du chapitre 4.4.8, après vérification en environnement de recette.
- Les configurations sont documentées, versionnées et vérifiées périodiquement par rapport à l'état de référence ; un écart est un incident.
- L'horloge de chaque système est synchronisée sur la source du chapitre 5.8.
- Aucun accès n'est ouvert depuis un environnement de recette ou de développement vers un système de production.

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 matériel. Le niveau de sécurité recherché est celui qu'exige la norme ETSI

EN 319 401 en son chapitre 7, et il est vérifié par le contrôle interne et l'audit externe du chapitre 7, non par une attestation de tiers.

5.6. Mesures de sécurité liées au développement des systèmes

Toute évolution d'un système concourant à une fonction du chapitre 1.7 suit une procédure de gestion du changement écrite, qui sépare le demandeur, l'exécutant et le valideur selon le chapitre 4.2.2.

1. La demande de changement est enregistrée, motivée et qualifiée en risque et en impact.
2. Une analyse d'impact identifie les fonctions, les documents et, le cas échéant, les informations déclaratives affectés.
3. Le changement est vérifié en environnement de recette, séparé de la production selon le chapitre 4.1.1.
4. La mise en production est approuvée par une fonction distincte de celle qui l'exécute, et journalisée.
5. Le retour arrière est préparé avant la mise en production et exerçable.
6. Lorsque le changement affecte un élément au vu duquel la déclaration préalable a été effectuée, l'autorité nationale est notifiée selon le chapitre 1.11.1, avec le rapport d'analyse d'impact.

Le prestataire tient à jour la liste des changements standards, au sens de l'exigence 22 du référentiel [Ref_Serv_Conf_NonQual] : changements prédéfinis, à faible risque et à faible impact, qui suivent la procédure allégée et ne donnent pas lieu à notification. L'inscription d'un changement à cette liste est elle-même une décision documentée, revue au contrôle interne.

5.7. Mesures de sécurité réseau

L'architecture réseau isole les fonctions les unes des autres et n'expose à l'extérieur que ce qui doit l'être : la publication, la fonction d'information sur l'état des certificats et les interfaces de service. Les fonctions de génération et le module cryptographique matériel ne sont joignables que depuis les zones internes qui en ont besoin.

- Les flux entrants et sortants sont limités par une politique de filtrage restrictive, revue à chaque contrôle interne.
- Les échanges avec la plateforme et avec les titulaires sont chiffrés et authentifiés de part et d'autre.
- Les tentatives d'accès en échec sont journalisées et revues selon la fréquence du chapitre 4.4.2.
- Aucune administration n'est possible depuis un réseau public sans passer par les moyens d'accès contrôlés du chapitre 5.5.1.
- L'autorité racine n'est raccordée à aucun réseau.

Aucun élément de topologie, aucun nom de domaine interne et aucune adresse ne sont publiés : leur divulgation affaiblirait les mesures décrites, sans apporter au lecteur une information dont il ait besoin pour se fier au service.

5.8. Horodatage / Système de datation

Les composantes du prestataire sont synchronisées sur une source de temps de confiance traçable à l'UTC, distincte des autorités de certification et redondée. La synchronisation est vérifiée toutes les 24 heures et toute dérive est journalisée.

Le service d'horodatage électronique du prestataire, régi par YT-PH-TSA (1.3.6.1.4.1.[PEN].1.1.3), est le moyen par lequel les dossiers de preuve et les lots d'archives reçoivent une date opposable, selon le chapitre 4.5.5. L'exactitude déclarée, la traçabilité à l'UTC, la conduite à tenir en cas de perte de synchronisation et le profil du jeton sont énoncés par cette politique et ne sont pas repris ici.

Lorsque la perte de synchronisation avec l'UTC est détectée, ou lorsque l'exactitude déclarée ne peut plus être garantie, l'unité d'horodatage cesse immédiatement de délivrer des jetons. L'ajustement dû à une seconde intercalaire intervient durant la dernière minute du jour où elle est programmée, et l'heure exacte du changement est enregistrée.

6. PROFIL DES CERTIFICATS ET DES LCR

Les gabarits des certificats et des listes de révocation sont publiés en annexe des politiques : annexes 9.3 et 9.4 de YT-PC-SIGN pour la signature, les mêmes annexes de YT-PC-SEAL pour le cachet, et la politique YT-PH-TSA pour les certificats d'unité d'horodatage. L'annexe 9.7 donne l'identifiant d'objet de chacune de ces politiques. La présente déclaration ne reproduit pas les gabarits ; elle décrit comment ils sont appliqués et contrôlés.

6.1. Profil des certificats

Le contenu d'un certificat n'est jamais saisi : il est construit par la fonction de génération des certificats à partir du gabarit de la politique applicable et des seules informations validées par l'autorité d'enregistrement. La pratique ajoute au gabarit les contrôles suivants.

- Un contrôle de complétude : la génération est refusée si une information obligatoire du gabarit est absente du dossier validé.
- Un contrôle de cohérence du nom distinctif avec le chapitre 2.1, y compris l'unicité vérifiée selon le chapitre 2.1.3.
- Un contrôle de la période de validité au regard de la règle du chapitre 5.3.2, qui interdit qu'un certificat survive à celui de son autorité émettrice.
- Un contrôle de l'extension Key Usage, marquée critique et réduite au seul usage prévu par le chapitre 1.10.1.
- Un contrôle de la présence de l'identifiant de politique du niveau délivré et de l'identifiant ETSI de référence correspondant dans l'extension Certificate Policies.
- Un contrôle de la présence des points d'accès aux informations d'état, sans lesquels la vérification du chapitre 3.9.6 serait impraticable.
- Un contrôle interdisant toute extension propriétaire et toute donnée à caractère personnel qui ne serait pas nécessaire à l'usage du certificat.

Un certificat produit est vérifié avant sa remise : sa chaîne de certification, sa conformité au gabarit et son empreinte sont contrôlées, et le résultat est journalisé. Un certificat non conforme n'est pas remis ; il est révoqué et l'incident est traité selon le chapitre 4.7.1.

L'exigence 6 du référentiel [Ref_Serv_Conf_NonQual] impose que le certificat sur lequel repose une signature ou un cachet avancé soit conforme à la norme ETSI EN 319 411-1 ou ETSI EN 319 411-2, et repose au minimum sur un certificat de type LCP ; le chapitre 1.3 énonce la correspondance retenue entre les niveaux commerciaux et les politiques ETSI de référence, et les profils publiés en annexe des politiques la mettent en œuvre.

6.2. Profil des LCR

Les listes de révocation sont conformes à la norme IETF RFC 5280 et au gabarit publié en annexe des politiques. Elles sont générées et publiées selon les chapitres 3.9.7 et 3.9.8 ; le champ nextUpdate est positionné à 72 heures et le numéro de liste est strictement croissant, ce qui permet à un utilisateur de certificat de détecter le remplacement d'une liste par une version antérieure.

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.

Chaque liste produite est vérifiée avant publication : signature, période couverte, numéro de liste et cohérence avec l'état enregistré par la fonction de gestion des révocations. Une liste non conforme n'est pas publiée et la publication précédente reste en vigueur jusqu'à correction, la publication d'une liste erronée étant plus dommageable qu'un retard borné par le champ nextUpdate.

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 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.

> **Point ouvert —** 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).

La durée de validité d'un agrément ne peut excéder trois ans et la demande de renouvellement est présentée quatre mois au moins avant l'expiration de sa validité, en application des articles 15 et 17 du décret n° 2-22-687. Le délai de décision de l'autorité nationale sur une demande d'agrément et les frais correspondants s'apprécient selon les modalités et les délais fixés par l'autorité nationale.

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. Le droit d'audit stipulé au contrat du chapitre 1.9.2 lui ouvre le même accès chez le tiers exerçant les fonctions d'autorité d'enregistrement.

7.4. Sujets couverts par les évaluations

- La conformité de la présente déclaration aux politiques citées au chapitre 1.1.
- La conformité des opérations effectivement conduites à la présente déclaration, vérifiée par sondage sur les dossiers de preuve.
- 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, et la tenue des cérémonies.
- 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, et l'effectivité du scellement du chapitre 4.5.3.
- 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 et du chapitre 8.2.
- La tenue à jour des informations déclaratives et l'exécution des notifications du chapitre 1.11.1.
- 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. La mesure conservatoire est décidée avant l'analyse de cause, non après.

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 figurent dans les conditions générales d'utilisation YT-CGU-PP, YT-CGU-PM et YT-CGU-TSA, et dans les déclarations de divulgation YT-PDS-CERT et YT-PDS-TSA, dont l'annexe 9.7 donne les identifiants d'objet. Le présent chapitre traite de la vie du présent document et des matières que le plan de référence ne couvre pas et que la loi impose.

Les tarifs des services de confiance fournis par le prestataire figurent sous l'identifiant YT-PRICING ; la révocation d'un certificat, l'accès aux listes de révocation et au service d'information sur l'état des certificats, la vérification publique d'une signature, d'un cachet ou d'un jeton, l'accès aux documents du registre de publication et le traitement d'une réclamation sont fournis sans frais.

8.1. Durée et fin anticipée de validité de la PC

La présente déclaration a sa propre durée de vie, distincte de celle des certificats délivrés sous son empire : un certificat demeure régi par la version en vigueur à sa délivrance.

8.1.1. Durée de validité

La présente déclaration 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 déclaration prend fin par anticipation dans trois cas : la cessation des services qu'elle décrit, 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 le chapitre 4.8 est appliqué lorsque la cause est une cessation d'activité. La fin de la déclaration 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.

8.2. Protection des données à caractère personnel

Le traitement des données à caractère personnel opéré à l'occasion des services est soumis à la Loi n° 09-08 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel. L'autorité compétente est la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP).

Les données traitées sont limitées à ce qui est nécessaire à la fourniture du service : les informations destinées à figurer dans le certificat, les éléments établissant la vérification de l'identité, les éléments de vérification des facteurs d'authentification, et les enregistrements des

opérations. Aucune donnée de santé, aucune donnée sensible et aucune donnée sans lien avec le service ne sont collectées.

Les finalités sont la délivrance et la gestion des certificats, l'exécution des opérations de signature et de cachet, la production des preuves exigées par la réglementation, et le respect des obligations de conservation. Aucune donnée n'est traitée à des fins de prospection, de profilage ou de mesure d'audience.

Le prestataire s'astreint aux obligations que l'exigence 17 du référentiel [Ref_Serv_Conf_NonQual] met à sa charge :

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

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

Ces droits s'exercent auprès du point de contact du chapitre 1.11.2, sur justification de l'identité du demandeur. Le prestataire répond dans les délais de la loi applicable ; une réponse insatisfaisante ouvre la voie de la réclamation du chapitre 8.4 et, en dernier ressort, de la saisine de la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP). L'exigence 18 du référentiel impose la mise en œuvre effective de ces moyens.

Les durées de conservation sont celles du chapitre 4.5.2 : la durée légale l'emporte sur le droit à l'effacement pour les données qui composent une preuve, et l'exigence 15 du référentiel subordonne au consentement de la personne concernée toute mise à disposition publique des données conservées à des fins de traitement. À l’issue de la période de conservation, les données archivées sont supprimées ou détruites de manière irréversible, et l’opération est journalisée.

Les données recueillies pour la vérification des antécédents du personnel sont traitées selon le chapitre 4.3.2. La CNDP distingue la notification d’une déclaration et la demande d’autorisation préalable, ainsi que la demande de transfert à l’étranger. Ce régime est indépendant de celui de la loi n° 43-20 : un prestataire dépose auprès de la DGSSI au titre de la loi n° 43-20 et notifie séparément ses traitements à la CNDP au titre de la loi n° 09-08.

> **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.

8.3. Responsabilité, garanties et assurance

Le prestataire demeure responsable, vis-à-vis de toute partie externe à l'infrastructure, des prestations fournies par ses composantes et par les tiers auxquels il confie une fonction, y compris

la vérification de l'identité déléguée selon le chapitre 1.9.2. La délégation d'une fonction n'emporte jamais délégation de la responsabilité.

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

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

Le plafond de responsabilité par certificat et par sinistre, les exclusions et les limites de garantie sont énoncés par les politiques et repris, en termes opposables, dans les conditions générales d'utilisation et dans les déclarations de divulgation ; la présente déclaration ne les reproduit pas. Pour le service d'horodatage, ce plafond s'entend par jeton d’horodatage et par sinistre, dans les mêmes conditions. Cette limitation ne s’applique pas en cas de dol ou de faute lourde du prestataire. Les cas d'exclusion retenus pour les services de certificats sont les suivants.

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

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

Le prestataire ne garantit ni la valeur juridique qu'une autorité, une juridiction ou un tiers reconnaîtra à une signature ou à un cachet produits au moyen d'un certificat non qualifié, ni l'acceptation de ce certificat par un service déterminé : la présomption de fiabilité est réservée au niveau qualifié par la loi n° 43-20, et le chapitre 1.3 le rappelle.

8.4. Réclamations, droit applicable et règlement des litiges

Toute réclamation est adressée au point de contact du chapitre 1.11.2 et traitée selon la procédure publiée sous l'identifiant YT-COMPLAINTS. Le prestataire en accuse réception dans un délai de 5 jours ouvrés et y répond dans un délai de 30 jours calendaires ; une demande d'examen de second niveau est traitée dans un délai de 15 jours calendaires.

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

La DGSSI est l’autorité nationale des services de confiance ; elle contrôle a posteriori les prestataires non agréés (article 52 de la loi n° 43-20). La CNDP est l’autorité compétente en matière de protection des données à caractère personnel au titre de la loi n° 09-08.

Le droit applicable est le droit marocain. À défaut de règlement amiable, les juridictions compétentes sont les tribunaux compétents de Marrakech.

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

9. ANNEXES

9.1. Exigences de sécurité

Les objectifs de sécurité opposables sont énoncés par les annexes 9.1.1 et 9.1.2 des politiques. La présente annexe décrit comment leur satisfaction est obtenue et vérifiée.

9.1.1. Exigences sur les objectifs de sécurité du module cryptographique

Le module cryptographique matériel employé pour générer et mettre en œuvre les clés d'autorité, ainsi que pour générer les données de création des titulaires, présente les propriétés énumérées au chapitre 5.2.1.1. La pratique du prestataire ajoute les vérifications suivantes.

- L'état du module et la validité de ses scellés sont contrôlés au début de chaque cérémonie et le contrôle est consigné au procès-verbal.
- Les journaux propres au module sont extraits, horodatés et versés aux archives avec les journaux d'évènements du chapitre 4.4.1.
- Le passage du module en état sûr, quelle qu'en soit la cause, est traité comme un incident selon le chapitre 4.7.1 et interdit toute reprise d'exploitation avant analyse.
- Aucune fonction du module autre que celles nécessaires aux services déclarés n'est activée l'inventaire des fonctions activées est revu à chaque contrôle interne.
- Toute intervention de maintenance sur le module est planifiée, accompagnée par une personne tenant un rôle de confiance, et consignée.

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 signature

Le dispositif de création de signature, mis en œuvre pour le compte du titulaire à l'intérieur du module cryptographique matériel, répond aux objectifs énoncés à l'annexe 9.1.2 des politiques. La pratique qui les rend effectifs est décrite aux chapitres 5.1.1.2, 5.2.8.2 et 5.4 : génération dans le module, liaison immédiate aux données d'activation du titulaire, autorisation propre à chaque opération, et absence de tout canal de sortie de la clé privée.

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 déclaration 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_AUDIT_EXT	Fréquence de l'audit externe indépendant	tous les 2 ans	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 génération des listes de révocation	24 heures	3.9.7
F_PUB_LCR_AC	Fréquence de génération de la liste de révocation des autorités émettrices	6 mois, et à chaque révocation d’un certificat d’autorité émettrice	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
F_TEST_REST	Fréquence de test de restauration des sauvegardes	1 fois par an, au minimum	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
T_AC_MAX	Indisponibilité maximale mensuelle de ces systèmes	4 heures	3.10.2
T_C_AC_MAX	Durée de vie maximale du certificat de l'autorité racine	10 ans	5.3.2

Variable	Description	Valeur	Chapitre
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_LCR_NEXT	Échéance annoncée dans le champ nextUpdate d'une liste de révocation	72 heures	3.9.7
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
T_REV_MAX	Indisponibilité maximale mensuelle de cette fonction	2 heures	3.10.2

Variable	Description	Valeur	Chapitre
T_TRAIT_REV	Délai maximum de traitement d'une demande de révocation	24 heures	3.9.5.1
T_PUB_ETAT	Délai maximum de publication de l'information d'état après traitement	24 heures	3.9.5.1
T_OCSP_MAX	Délai maximum de prise en compte d'une révocation par le service en ligne	24 heures	3.9.9
T_SYNC	Périodicité de vérification de la synchronisation de la source de temps	24 heures	5.8
T_PREAVIS	Préavis de prise d'effet d'une modification substantielle	30 jours	1.11.4
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 gabarit d'un certificat d'autorité de certification est publié à l'annexe 9.3 des deux politiques de certification, dont l'annexe 9.7 donne les identifiants d'objet ; il respecte par ailleurs les exigences de la norme IETF RFC 5280. La présente déclaration n'en reproduit pas le contenu et énonce ce que la pratique y ajoute.

Élément du gabarit	Ce que la pratique en fait
Nom distinctif	Composé selon le chapitre 2.1.1 (C=MA, O=YORYX TRUST SASU, organizationIdentifier=NTRMA-184667, CN=YORYX TRUST Root CA G1) et inscrit dans le script de cérémonie, jamais saisi librement.
Numéro de série	Produit par un générateur non prévisible et vérifié unique au sein du domaine de l'autorité émettrice avant signature.
Période de validité	10 ans pour l'autorité racine et 6 ans pour une autorité émettrice ; la date de fin est calculée par le script et contrôlée au regard du chapitre 5.3.2.
Extension Basic Constraints	cA à vrai, marquée critique ; la profondeur de la hiérarchie est bornée, ce qui interdit l'apparition d'un niveau non prévu.
Extension Key Usage	keyCertSign et cRLSign uniquement, marquée critique ; l'absence de tout autre bit est vérifiée avant remise.

Élément du gabarit	Ce que la pratique en fait
Extension Certificate Policies	Portée par les certificats d'autorité émettrice, avec les identifiants des politiques sous lesquelles l'autorité délivre.
Points d'accès aux informations d'état	Contrôlés présents pour tout certificat non auto-signé, faute de quoi la vérification du chapitre 3.9.6 serait impraticable.
Empreinte du certificat produit	Relevée en cérémonie, consignée au procès-verbal, et comparée à celle du certificat publié dans le registre de publication.

9.4. Détails sur le gabarit d'un certificat porteur

Le gabarit d'un certificat de titulaire est publié à l'annexe 9.4 des politiques. La présente déclaration énonce les contrôles appliqués à chaque génération, énumérés au chapitre 6.1, et précise ci-dessous les points sur lesquels la pratique est plus stricte que le gabarit.

Point	Pratique retenue
Données à caractère personnel	Le champ Subject ne porte que ce que le gabarit impose ; aucune adresse, aucune date de naissance et aucun numéro de pièce d'identité n'y figurent, conformément au chapitre 8.2.
Extension Extended Key Usage	Non employée : la limitation d'usage résulte de l'extension Key Usage et du chapitre 1.10.1.1, et une seconde expression de la même limite pourrait la contredire.
Extensions propriétaires	Aucune. Une extension propriétaire rendrait le certificat inexploitable par les logiciels de vérification du marché, contrairement au chapitre 2.2.5.
Identifiants de politique	L'identifiant de la politique du niveau délivré et l'identifiant ETSI de référence correspondant sont tous deux portés, ce qui permet à un utilisateur de certificat d'apprécier le niveau sans connaître notre arc.
Correspondance avec le dossier	Chaque valeur portée par le certificat est rattachable à une information vérifiée du dossier de preuve du chapitre 4.5.1.

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

Autorité	Algorithme et taille de clé	Algorithme de signature	Empreinte
YORYX TRUST Signature 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
YORYX TRUST Timestamping CA G1	RSA 4096 bits	sha256WithRSAEncryption (RSASSA-PKCS1-v1_5, SHA-256)	SHA-256
YORYX TRUST TSU 1 G1	RSA 3072 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). C'est ce qu'impose l'exigence 26 du référentiel [Ref_Serv_Conf_NonQual] pour les algorithmes et les mécanismes cryptographiques mis en œuvre. MD5, SHA-1 et toute longueur de clé RSA inférieure à 2048 bits sont proscrits.

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.

La pratique du prestataire consiste à réexaminer ces choix à chaque contrôle interne, au regard des recommandations en vigueur ; une suite jugée insuffisante entraîne le changement de clé du chapitre 4.6 et non la seule mise à jour du présent document.

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.
Formats de signature et de cachet admis	PAdES (ETSI EN 319 142-1) ; XAdES (ETSI EN 319 132-1) ; CAdES (ETSI EN 319 122-1)

Élément	Valeur
Conteneurs associés	ASiC (ETSI EN 319 162-1)

Les formats ci-dessus sont ceux qu'autorise l'exigence 25 du référentiel [Ref_Serv_Conf_NonQual] ; aucun autre format n'est produit par le service de signature. 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 déclaration.

YT-PC-SIGN (1.3.6.1.4.1.[PEN].1.1.1) — Politique de certification, signature électronique.

YT-PC-SEAL (1.3.6.1.4.1.[PEN].1.1.2) — Politique de certification, cachet électronique.

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-PDS-TSA (1.3.6.1.4.1.[PEN].1.3.2) — Déclaration de divulgation PKI pour l'horodatage.

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-CGU-TSA (1.3.6.1.4.1.[PEN].1.4.3) — Conditions générales d'utilisation, horodatage.

YT-FORM-SUBSCRIBER — Formulaire d'enregistrement du porteur.

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-PRICING — Tarifs.

YT-COMPLAINTS — Procédure de réclamation.

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

La politique d’horodatage suit le plan type détaillé de l’annexe 9.8 de la PC-type de la DGSSI, complété par le chapitre 6 de la norme ETSI EN 319 421. Cette matière ne relève pas de la présente déclaration : les pratiques d'horodatage du prestataire sont énoncées par YT-PH-TSA (1.3.6.1.4.1.[PEN].1.1.3), qui suit ce plan type. Les seuls points de contact entre les deux documents sont l'horodatage des dossiers de preuve du chapitre 4.5.5, le système de datation du chapitre 5.8 et les clés de l'unité d'horodatage YORYX TRUST TSU 1 G1, générées et protégées selon le chapitre 5.1.1.1.

Les politiques de certification suivent le plan de la PC-type de la DGSSI (chapitres 1 à 9), elle-même conforme au cadre IETF RFC 3647.

9.9. Matrice de traçabilité [Ref_Serv_Conf_NonQual] — exigences 1 à 28

Le tableau ci-dessous rattache chacune des vingt-huit exigences du référentiel d'exigences de conformité relatives aux services de confiance non qualifiés au document et à la section qui y répondent. Une ligne dont la colonne « Document » ne désigne pas la présente déclaration renvoie à une politique du registre de publication, citée par son identifiant et son identifiant d'objet ; la présente déclaration décrit alors la pratique correspondante sans reprendre l'exigence.

Documents cités par la matrice

Identifiant du document	Identifiant d'objet
YT-DPC	1.3.6.1.4.1.[PEN].1.2
YT-PC-SIGN	1.3.6.1.4.1.[PEN].1.1.1
YT-PC-SEAL	1.3.6.1.4.1.[PEN].1.1.2
YT-PH-TSA	1.3.6.1.4.1.[PEN].1.1.3

N°	Exigence (résumé)	Document	Section
1	Prendre connaissance de l'ensemble du cadre juridique et normatif ; en cas d'incohérence, la loi et le décret prévalent et la suspicion est remontée à l'autorité nationale avant toute mise en œuvre.	YT-DPC	1.1 Présentation générale
2	Se conformer à la norme ETSI EN 319 401, quel que soit le service fourni : analyse de risque, politiques et pratiques, conditions générales, politique de sécurité, organisation, ressources humaines, biens, accès, contrôles cryptographiques, sécurité physique, exploitation, réseau, incidents, preuves, continuité et cessation.	YT-DPC	4 MESURES DE SÉCURITÉ NON TECHNIQUES
3	Se conformer à la norme ETSI EN 319 411-1 pour la délivrance de certificats destinés à la signature ou au cachet électronique avancé.	YT-PC-SIGN	1.1 Présentation générale
4	Se conformer à la norme ETSI EN 319 421 pour le service d'horodatage électronique.	YT-PH-TSA	3 POLITIQUE D’HORODATAGE
5	Se conformer à la norme ETSI EN 319 531 pour un service d'envoi recommandé électronique.	YT-DPC	1.1 Présentation générale
6	Faire reposer la signature ou le cachet avancé sur un certificat conforme à la norme ETSI EN 319 411-1 ou ETSI EN 319 411-2, de type LCP au minimum.	YT-PC-SIGN	6.1 Profil des certificats
7	Garantir l'usage des clés de signature sous le contrôle exclusif du signataire, avec un niveau de confiance élevé assuré par une authentification forte multifacteur propre à l'usage des clés.	YT-PC-SIGN	5.4 Données d’activation
8	Garantir l'usage des clés de cachet sous le contrôle du créateur du cachet, par une authentification forte de celui-ci.	YT-PC-SEAL	5.4 Données d’activation

N°	Exigence (résumé)	Document	Section
9	Lier la signature ou le cachet aux données associées de telle sorte que toute modification ultérieure soit détectable, par une fonction d'empreinte conforme.	YT-DPC	3.5 Usages de la bi-clé et du certificat
10	Encadrer par un contrat écrit préalable la délégation de la vérification d'identité à une autorité d'enregistrement tierce : obligations, rôles, responsabilités, moyens de contrôle et établissement des preuves.	YT-DPC	2.2 Validation initiale de l'identité
11	Admettre les dispositions de vérification d'identité du référentiel [Ref_Deliv_Cert_Qual] comme suffisantes pour la délivrance de certificats non qualifiés de type NCP et NCP+.	YT-PC-SIGN	2.2 Validation initiale de l'identité
12	Soumettre à l'accord préalable de l'autorité nationale, et à publication par arrêté, tout procédé alternatif au certificat électronique.	YT-DPC	1.11 Gestion de la PC
13	Établir une convention de preuve définissant la nature, la portée, l'établissement, la conservation, la mise à disposition et l'interprétation des preuves, ainsi que les engagements des parties.	YT-DPC	4.5 Archivage des données
14	Sceller les dossiers de preuve par un cachet électronique du prestataire afin d'en renforcer la fiabilité et l'intégrité.	YT-DPC	4.5.3 Protection des archives
15	Employer des systèmes fiables de conservation : authenticité vérifiable, introduction et modification réservées aux personnes autorisées, mise à disposition publique subordonnée au consentement de la personne concernée.	YT-DPC	4.5.4 Procédure de sauvegarde des archives
16	Conserver toutes les informations relatives à la fourniture du service et aux transactions, utiles à la continuité du service et à la production de preuves.	YT-DPC	4.5.1 Types de données à archiver

N°	Exigence (résumé)	Document	Section
17	Conserver les données à caractère personnel conformément à la loi n° 09-08 et aux délibérations de la CNDP, et respecter le secret, la sécurité et la confidentialité.	YT-DPC	8.2 Protection des données à caractère personnel
18	Mettre en œuvre les moyens permettant à un utilisateur justifiant de son identité d'exercer ses droits d'accès, de rectification et d'opposition.	YT-DPC	8.2 Protection des données à caractère personnel
19	Garantir la conservation et l'accessibilité des données pendant sept ans, y compris après une cessation d'activité.	YT-DPC	4.5.2 Période de conservation des archives
20	Garantir la suppression ou la destruction des données conservées à la fin de la période de conservation.	YT-DPC	4.5.2 Période de conservation des archives
21	Notifier à l'autorité nationale, dans les meilleurs délais, toute modification d'un élément au vu duquel la déclaration préalable a été effectuée.	YT-DPC	1.11 Gestion de la PC
22	Définir et tenir à jour la liste des changements techniques ou paramétriques standards, prédéfinis, à faible risque et à faible impact.	YT-DPC	5.6 Mesures de sécurité liées au développement des systèmes
23	Accompagner toute notification de modification d'un rapport d'analyse des impacts de celle-ci.	YT-DPC	1.11 Gestion de la PC
24	Transmettre la notification de modification par envoi recommandé ou par dépôt contre récépissé, avec les versions à jour des documents impactés.	YT-DPC	1.11.2 Point de contact
25	N'employer, pour les signatures et cachets avancés et leurs conteneurs, que les formats PAdES, XAdES, CAdES et ASiC.	YT-PC-SIGN	1.10 Usage des certificats
26	Mettre en œuvre des algorithmes et des mécanismes cryptographiques conformes à la norme ETSI TS 119 312.	YT-DPC	9.5 Algorithmes de signature et taille de clés des AC

N°	Exigence (résumé)	Document	Section
27	Garantir l'exactitude et le maintien à jour des informations déclaratives publiées sur la liste déclarative de l'autorité nationale.	YT-DPC	1.11.1 Entité gérant la PC
28	Préciser sur le formulaire de déclaration préalable les informations publiées sur la liste déclarative, dont l'identifiant d'objet et l'adresse de la politique de chaque service.	YT-DPC	1.6 Identification du document

Le résumé de la colonne « Exigence » est une reformulation destinée à la lecture du tableau ; le texte opposable est celui du référentiel, et c'est lui qui prévaut. La correspondance est vérifiée à chaque contrôle interne du chapitre 7.1 et à chaque évolution de la présente déclaration selon le chapitre 1.11.4.

L'exigence 5 concerne l'envoi recommandé électronique, service qui ne figure pas parmi les services déclarés du chapitre 1.4 : elle est sans objet en l'état, et sa mention au chapitre 1.1 vaut engagement de s'y conformer si ce service venait à être déclaré. L'exigence 12 concerne un procédé alternatif au certificat électronique, qui n'est pas mis en œuvre : le chapitre 1.11 énonce la conduite à tenir si le prestataire venait à en envisager un.