Politique de certification de l'AC YOUSIGN SAS - SIGN3 CA

v1.4.4 | Diffusion : C1 - Public

HISTORIQUE DES VERSIONS			
Version	**Objet de la modification**	**Date**	**Auteur**
1.4.4	Ajout d'un paragraphe de précision sur le principe de wrapping utilisé pour les sauvegardes de clés (Section Copie de la clé privée) Ajoute d'un paragraphe décrivant les principes de pré-génération des clés (Section Stockage de la clé privée dans un module cryptographique)	Jun 17, 2026	Etienne SELLAN
1.4.3	Ajout d'un paragraphe sur les cas où une AED conserve des archives au format papier (section Période de conservation des archives) Précision sur la constitution du dossier de preuve d'identité dans le cas d'une AE(D) (section Processus et responsabilités pour l'établissement d'une demande de certificat) Ajout de la nécessité d'applicabilité des mesures de sécurité de la PC lors de la sélection d'un prestataire externe (section Exigences vis-à-vis du personnel des prestataires externes) Ajout d'un paragraphe pour le service en ligne utilisé par l'OID `1.2.250.1.302.1.17.1.0` précisant que l'utilisateur dispose de 30 jours après la vérification initiale de son identité pour obtenir son certificat (section validation de l'identité du porteur)	3 mars 2026	Tony DUFOUR Fiona BOUVIER
1.4.2	Ajout de l'identification de l'AED pour les OID `1.2.250.1.302.1.22.1.0` et `1.2.250.1.302.1.23.1.0` (section types de noms)	22 mai 2025	Tony DUFOUR
1.4.1	Ajout de la possibilité pour l'Abonné de communiquer les justificatifs du Porteur à l'AE (sections validation de l'identité d'un individu et processus et responsabilités pour l'établissement d'une demande de certificat)	14 avr. 2025	Tony BELOT

1.4.0	Ajout d'une opération de translittération préalable à l'opération de comparaison par le service en ligne utilisé par l'OID `1.2.250.1.302.1.17.1.0` (section validation de l'identité du porteur) Changement de la taille de clé de 2048 vers 3072 bits pour : • les certificats des unités d'horodatage (section certificats des Unités d'Horodatage) • les certificats du service OCSP (section certificats du service OCSP) Ajout de la description du fonctionnement de l'extension OCSP *Archive CutOff* (section réponses OCSP) Corrections mineures syntaxiques	31 oct. 2024	Tony BELOT Etienne SELLAN
1.3.0	Ajout des OID spécifiques à chaque type de certificat. (section Identification du document) Introduction de l'AED pour certaines catégories de certificats. (section Autorités d'enregistrement) Introduction des responsabilités de l'AED et des processus d'habilitation des opérateurs AED. (section Autorités d'enregistrement déléguées) Clarification des obligations des porteurs de certificats et ajout des porteurs spécifiques comme les unités d'horodatage. (section Porteurs de certificats) Ajout des certificats émis via une AED. (section Domaines d'utilisation applicables) Introduction du Comité de Direction Technique pour évaluer la conformité. (section Entité déterminant la conformité d'une DPC avec cette PC) Ajout des CGU dans les documents publiés en ligne et clarification des informations. (section Informations devant être publiées)	21 juin 2024	Tony DUFOUR Tony BELOT Sarah MAZOUNI

	Mise à jour de la fréquence de publication des LAR et précision relative à la publication des CGU. (section Délais et fréquences de publication) Clarification des champs. (section Types de noms) La pseudonymisation est spécifiquement interdite. (section Pseudonymisation des noms) Détails supplémentaires sur la génération des bi-clés dans l'infrastructure Yousign. (section Méthode pour prouver la possession de la clé privée) Détails supplémentaires sur la validation par l'AED et les pièces d'identité acceptées. (section Validation de l'identité d'un individu) Ajout des cas d'identification par une AED. (section Identification et validation pour un renouvellement courant) Vérification d'identité par l'AE et l'AED, attestation de vérification d'identité. (section Exécution des processus d'identification et de validation de la demande) Détails sur l'information du demandeur en cas de rejet de la demande. (section Acceptation ou rejet de la demande) Mise à jour des causes. (section Causes possibles d'une révocation) Clarification des modalités de notification et de traitement des incidents. (section Procédure de traitement d'une demande de révocation) Clarification des qualifications et des compétences requises, ajout des exigences spécifiques pour les rôles impliqués dans l'AED. (section Qualifications, compétences et habilitations requises) Ajout de détails sur les évènements spécifiques à enregistrer, y compris ceux		

	liés à l'AED. (section Type d'évènements à enregistrer) Mise à jour de la description du partage des secrets pour les clés privée d'AC. (section Contrôle de la clé privée par plusieurs personnes) Ajout des méthodes de copie sécurisée des clés privées, y compris des exigences spécifiques pour les modules cryptographiques. (section Copie de la clé privée) Ajout de nouveaux types de certificats pour l'AED et ajustements des profils de certificats existants. (sections Certificats de l'ACP, Certificats de l'AC « YOUSIGN SAS - SIGN3 CA » et Certificats de personnes physiques) Mise à jour des profils de certificats avec des informations spécifiques pour les unités d'horodatage. (section Certificats des Unités d'Horodatage) Mise à jour des profils de certificats pour inclure les services OCSP avec des informations spécifiques pour l'AED. (section Certificats du service OCSP) Ajout des fréquences spécifiques d'audit pour les nouveaux rôles et entités introduits par l'AED. (section Fréquences et ou circonstances des évaluations) Mise à jour de la politique de protection des données pour inclure les exigences spécifiques aux processus AED. (section Politique de protection des données personnelles) Détails supplémentaires sur la notification et le consentement relatifs à l'utilisation des données personnelles dans les processus AED. (section Notification et consentement d'utilisation des données personnelles) Mise à jour de la section Autres problématiques métiers et légales		

1.2.0	Conversion du document afin de traiter les certificats de signature.	Apr 29, 2024	Tony BELOT
1.1.0	Correction du CN de l'unité d'horodatage	Apr 16, 2024	Tony DUFOUR
1.0.0	Création du document, généré à partir de la Politique de Certification de l'AC - YOUSIGN SAS - SIGN2 CA pour les certificats de cachet, version 1.04, avec les modifications suivantes : • Modification des références à l'AC Sign2 pour Sign3, mise à jour de l'OID et des adresses des CRL • Introduction du terme « entité sujette » (ou son représentant légal) afin de permettre une différence d'entité légale entre l'entité du RCC et l'entité pour laquelle un certificat est émis • Remplacement de la notion de « certificat du RCC » par « certificat de cachet » • Suppression de la référence à la politique de classification des informations (section identification du document) • Mise à jour de la liste des entités intervenant dans l'IGC et renvoi vers les définitions (section entités intervenant dans l'IGC) • Clarification de la notion de certificat de cachet (section domaines d'utilisation applicables) • Mise à jour de l'adresse de contact de l'AC et des modalités d'évaluation de la conformité (section gestion de la PC) • Revue des acronymes (section acronymes) et remplacement des termes complets présents dans le document par leurs acronymes • Ajout et revue des définitions existantes (section définitions) • Mise à jour du lien d'accès aux documents publics (section entités chargées de la mise à disposition des informations) • Ajout des CGU dans la liste des documents publiés en ligne dont l'intégrité est vérifiable et clarification des informations publiées et du moyen de protection	13 juil. 2023	Tony Belot

	en intégrité (section informations devant être publiées) • Mise à jour de la fréquence de publication des LAR et précision relative à la publication des CGU (section délais et fréquences de publication) • Clarification des champs existants et ajout des champs `OI` et `serialNumber` (section types de noms) • Mise à jour des procédures de l'AE et de l'AC de traitement des demandes (sections validation initiale de l'identité, demande de certificat, traitement d'une demande de certificat, délivrance du certificat, acceptation du certificat et délivrance d'un nouveau certificat suite au changement de la bi-clé) • Mise à jour des modalités d'utilisation et de protection des clés et des certificats, ainsi que des responsabilités (sections méthode pour prouver la possession de la clé privée, usages de la bi-clé et du certificat, méthode d'activation de la clé privée et protection des données d'activation) • Mise à jour des causes possibles d'une révocation de certificat de cachet (section certificats de cachet) • Ajout des personnes ayant connaissance du secret de révocation dans la liste des personnes autorisées à demander la révocation d'un certificat de cachet (section certificats de cachet) • Remplacement de la simple collecte du nom du demandeur par son identité complète, ainsi que de l'information permettant d'identifier précisément le certificat à révoquer (section révocation d'un certificat de cachet) • Mise à jour des modalités de notification en cas de demande de révocation d'un certificat (section révocation d'un certificat de cachet)		

	• Ajout des éléments à vérifier dans le cadre de la vérification du statut d'un certificat de cachet (section exigences de vérification de la révocation par les utilisateurs de certificats) • Ajout des modalités de publication de l'information de révocation d'une AC (section exigences spécifiques en cas de compromission de la clé privée) • Remplacement du terme « RCC » par « abonné » dans le cas de la relation contractuelle entre l'AC et celui-ci, suppression des relations hiérarchiques et réglementaires (section fin de la relation entre l'abonné et l'AC) • Suppression des canaux de révocation par téléphone et courrier, mise à jour de la procédure de révocation par courriel (section identification et validation d'une demande de révocation) • Suppression des informations concernant l'activation du service au sein du produit Yousign (section actions de l'AC concernant la délivrance du certificat) • Renommage des sections relatives aux clés des serveurs, mise à jour des informations de génération, d'utilisation et de protection des données d'activation (section données d'activation) • Remplacement du Siren Yousign par le Siret dans les champs des certificats (sections certificats de cachet et liste de Certificats Révoqués) • Réorganisation des annexes et suppression de l'annexe relative aux exigences de sécurité du dispositif du système de signature (sections clés serveurs et annexes sur les exigences de sécurité du module cryptographique de l'AC) • Ajout de la possibilité de stockage des clés privées des certificats de cachet en dehors du HSM et renommage de la section (section copie de la clé privée)		

	• Ajout de la méthode de désactivation des clés privées des certificats de cachet (section méthode de désactivation de la clé privée) • Ajout des champs d'extension *Subject Key Identifier* et *Authority Information Access*, ainsi que de la valeur *Digital Signature* dans les *Key Usage* des certificats de cachet (section certificats de cachet) • Traduction des termes anglais vers le français dans l'ensemble du document • Corrections mineures syntaxiques, de mise en forme, ou facilitant la lecture du document		

Table des matières

1. Introduction 17
    1.1. Présentation générale 17
    1.2. Identification du document 17
    1.3. Entités intervenant dans l'IGC 18
        1.3.1. Autorités de certification 18
        1.3.2. Autorités d'Enregistrement 19
        1.3.3. Autorités d'Enregistrement Déléguées 19
        1.3.4. Porteurs de certificats 20
        1.3.5. Utilisateurs de certificats 21
    1.4. Usage des certificats 21
        1.4.1. Domaines d'utilisation applicables 21
        1.4.2. Bi-clés et certificats d'AC et de composantes 22
        1.4.3. Domaines d'utilisation interdits 22
    1.5. Gestion de la PC 22
        1.5.1. Entité gérant la PC 22
        1.5.2. Point de contact 22
        1.5.3. Entité déterminant la conformité d'une DPC avec cette PC 23
    1.6. Définitions et acronymes 23
        1.6.1. Acronymes 23
        1.6.2. Définitions 24
2. Responsabilités concernant la mise à disposition des informations devant être publiées 28
    2.1. Entités chargées de la mise à disposition des informations 28
    2.2. Informations devant être publiées 28
    2.3. Délais et fréquences de publication 28
    2.4. Contrôle d'accès aux informations publiées 29
3. Identification et authentification 29
    3.1. Nommage 29
        3.1.1. Types de noms 29
        3.1.2. Nécessité d'utilisation de noms explicites 32
        3.1.3. Pseudonymisation des noms 32
        3.1.4. Règles d'interprétation des différentes formes de nom 32
        3.1.5. Unicité des noms 32
        3.1.6. Identification, authentification et rôle des marques déposées 33
    3.2. Validation initiale de l'identité 33
        3.2.1. Méthode pour prouver la possession de la clé privée 33
        3.2.2. Validation de l'identité d'un organisme 34
        3.2.3. Validation de l'identité d'un individu 34
            3.2.3.2. Habilitation d'un opérateur d'enregistrement 36
        3.2.4. Informations non vérifiées du porteur 36

3.2.5. Validation de l'autorité du demandeur 36
3.2.6. Certification croisée d'AC 37
3.3. Identification et validation d'une demande de renouvellement des clés 37
3.3.1. Identification et validation pour un renouvellement courant 37
3.3.2. Identification et validation pour un renouvellement après révocation 38
3.4. Identification et validation d'une demande de révocation 38
4. Exigences opérationnelles sur le cycle de vie des certificats 39
4.1. Demande de certificat 39
4.1.1. Origine d'une demande de certificat 39
4.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat 39
4.2. Traitement d'une demande de certificat 41
4.2.1. Exécution des processus d'identification et de validation de la demande 41
4.2.2. Acceptation ou rejet de la demande 42
4.2.3. Durée d'établissement du certificat 42
4.3. Délivrance du certificat 42
4.3.1. Actions de l'AC concernant la délivrance du certificat 42
4.3.2. Notification par l'AC de la délivrance du certificat 43
4.4. Acceptation du certificat 43
4.4.1. Démarche d'acceptation du certificat 43
4.4.2. Publication du certificat 43
4.4.3. Notification par l'AC aux autres entités de la délivrance du certificat 44
4.5. Usages de la bi-clé et du certificat 44
4.5.1. Utilisation de la clé privée et du certificat par le porteur 44
4.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat 45
4.6. Renouvellement d'un certificat 45
4.6.1. Causes possibles de renouvellement d'un certificat 45
4.6.2. Origine d'une demande de renouvellement 45
4.6.3. Procédure de traitement d'une demande de renouvellement 46
4.6.4. Notification au porteur de l'établissement du nouveau certificat 46
4.6.5. Démarche d'acceptation du nouveau certificat 46
4.6.6. Publication du nouveau certificat 46
4.6.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat 46
4.7. Délivrance d'un nouveau certificat suite au changement de la bi-clé 46
4.7.1. Causes possibles de changement d'une bi-clé 46
4.7.2. Origine d'une demande d'un nouveau certificat 47
4.7.3. Procédure de traitement d'une demande d'un nouveau certificat 47
4.7.4. Notification au porteur de l'établissement du nouveau certificat 47
4.7.5. Démarche d'acceptation du nouveau certificat 47
4.7.6. Publication du nouveau certificat 47
4.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat 47

4.8. Modification du certificat 48
4.8.1. Causes possibles de modification d'un certificat 48
4.8.2. Origine d'une demande de modification d'un certificat 48
4.8.3. Procédure de traitement d'une demande de modification d'un certificat 48
4.8.4. Notification de l'établissement du certificat modifié 48
4.8.5. Démarche d'acceptation du certificat modifié 48
4.8.6. Publication du certificat modifié 48
4.8.7. Notification par l'AC aux autres entités de la délivrance du certificat modifié 49
4.9. Révocation et suspension des certificats 49
4.9.1. Causes possibles d'une révocation 49
4.9.1.1. Certificats de porteur 49
4.9.1.2. Certificats d'une composante de l'AC 50
4.9.2. Origine d'une demande de révocation 50
4.9.2.1. Certificats de porteur 50
4.9.2.2. Certificats d'une composante de l'IGC 50
4.9.3. Procédure de traitement d'une demande de révocation 51
4.9.3.1. Révocation d'un certificat de porteur 51
4.9.3.2. Révocation d'un certificat d'une composante de l'IGC 51
4.9.4. Délai accordé pour formuler la demande de révocation 52
4.9.5. Délai de traitement par l'AC d'une demande de révocation 52
4.9.5.1. Révocation d'un certificat de porteur 52
4.9.5.2. Révocation d'un certificat d'une composante de l'IGC 52
4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats 53
4.9.7. Fréquence d'établissement des LCR 53
4.9.8. Délai maximum de publication d'une LCR 53
4.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats 53
4.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats 53
4.9.11. Autres moyens disponibles d'information sur les révocations 54
4.9.12. Exigences spécifiques en cas de compromission de la clé privée 54
4.9.13. Causes possibles d'une suspension 54
4.9.14. Origine d'une demande de suspension 54
4.9.15. Procédure de traitement d'une demande de suspension 54
4.9.16. Limites de la période de suspension d'un certificat 55
4.10. Fonction d'information sur l'état des certificats 55
4.10.1. Caractéristiques opérationnelles 55
4.10.2. Disponibilité de la fonction 55
4.10.3. Dispositifs optionnels 55
4.11. Fin de la relation entre le porteur et l'AC 55
4.12. Séquestre de clé et recouvrement 56

4.12.1. Politique et pratiques de recouvrement par séquestre des clés 56
4.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session 56
5. Mesures de sécurité non techniques 56
5.1. Mesures de sécurité physique 56
5.1.1. Situation géographique et construction des sites 56
5.1.2. Accès physique 57
5.1.3. Alimentation électrique et climatisation 57
5.1.4. Vulnérabilité aux dégâts des eaux 57
5.1.5. Prévention et protection incendie 57
5.1.6. Conservation des supports 57
5.1.7. Mise hors service des supports 58
5.1.8. Sauvegardes hors site 58
5.2. Mesures de sécurité procédurales 58
5.2.1. Rôles de confiance 58
5.2.2. Nombre de personnes requises par tâche 60
5.2.3. Rôles exigeant une séparation des attributions 60
5.3. Mesures de sécurité vis-à-vis du personnel 60
5.3.1. Qualifications, compétences et habilitations requises 60
5.3.2. Procédures de vérification des antécédents 61
5.3.3. Exigences en matière de formation initiale 61
5.3.4. Exigences et fréquence en matière de formation continue 61
5.3.5. Fréquence et séquence de rotation entre différentes attributions 61
5.3.6. Sanctions en cas d'actions non autorisées 61
5.3.7. Exigences vis-à-vis des prestataires externes 62
5.3.8. Documentation fournie au personnel 62
5.4. Procédure de constitution des données d’audit 62
5.4.1. Type d'évènements à enregistrer 62
5.4.2. Fréquence de traitement des journaux d'évènements 64
5.4.3. Période de conservation des journaux d'évènements 64
5.4.4. Protection des journaux d'évènements 64
5.4.5. Procédure de sauvegarde des journaux d'évènements 65
5.4.6. Système de collecte des journaux d'évènements 65
5.4.7. Notification de l'enregistrement d'un évènement au responsable de l'événement 65
5.4.8. Évaluation des vulnérabilités 65
5.5. Archivage des données 65
5.5.1. Types de données à archiver 65
5.5.2. Période de conservation des archives 66
5.5.3. Protection des archives 67
5.5.4. Procédure de sauvegarde des archives 67

5.5.5. Exigences d'horodatage des données 67
5.5.6. Système de collecte des archives 68
5.5.7. Procédures de récupération et de vérification des archives 68
5.6. Changement de clé d'AC 68
5.7. Reprise suite à la compromission et sinistre 68
5.7.1. Procédures de remontée et de traitement des incidents et des compromissions 68
5.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) 69
5.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante 69
5.7.4. Capacités de continuité d'activité suite à un sinistre 70
5.8. Fin de vie de l'IGC 70
5.8.1. Transfert d'activité ou cessation d'activité affectant une composante de l'IGC 70
5.8.2. Cessation d'activité affectant l'AC 71
6. Mesures de sécurité techniques 72
6.1. Génération des bi-clés 72
6.1.1. Clés d'AC 72
6.1.2. Clés des porteurs 73
6.2. Transmission de la clé privée à son propriétaire 73
6.3. Transmission de la clé publique à l'AC 74
6.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats 74
6.5. Tailles des clés 74
6.6. Vérification des paramètres de génération des bi-clés et de leur qualité 74
6.7. Objectifs d'usage de la clé 75
6.8. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques 75
6.8.1. Standards et mesures de sécurité pour les modules cryptographiques 75
6.8.2. Contrôle de la clé privée par plusieurs personnes 75
6.8.3. Séquestre de la clé privée 76
6.8.4. Copie de la clé privée 76
6.8.5. Archivage de la clé privée 76
6.8.6. Transfert de la clé privée vers / depuis le module cryptographique 77
6.8.7. Stockage de la clé privée dans un module cryptographique 77
6.8.8. Méthode d'activation de la clé privée 77
6.8.9. Méthode de désactivation de la clé privée 78
6.8.10. Méthode de destruction des clés privées 78
6.8.11. Niveau de qualification du module cryptographique et des dispositifs de création de signature 79
6.9. Autres aspects de la gestion des bi-clés 79
6.9.1. Archivage des clés publiques 79
6.9.2. Durées de vie des bi-clés et des certificats 79

6.10. Données d’activation 80
6.10.1. Génération et installation des données d'activation 80
6.10.1.1. Clés de l'AC 80
6.10.1.2. Clés des certificats de porteurs 80
6.10.2. Protection des données d'activation 81
6.10.2.1. Clés de l'AC 81
6.10.2.2. Clés des certificats de porteurs 81
6.10.3. Autres aspects liés aux données d'activation 81
6.11. Mesures de sécurité des systèmes informatiques 81
6.11.1. Exigences de sécurité technique spécifiques aux systèmes informatiques 81
6.11.2. Niveau de qualification des systèmes informatiques 82
6.12. Mesures de sécurité liées au développement des systèmes 82
6.12.1. Mesures liées à la gestion de la sécurité 82
6.12.2. Niveau d'évaluation sécurité du cycle de vie des systèmes 82
6.13. Mesures de sécurité réseau 82
6.14. Horodatage 83
7. Profil des certificats et des LCR 83
7.1. Profils de certificats 83
7.1.1. Certificats de l’ACP 83
7.1.2. Certificats de l'AC « YOUSIGN SAS - SIGN3 CA » 84
7.1.3. Certificats de personnes physiques 85
7.1.4. Certificats des Unités d'Horodatage 87
7.1.5. Certificats du service OCSP 89
7.2. Liste de Certificats Révoqués 90
7.3. Jetons OCSP 91
7.3.1. Requêtes OCSP 91
7.3.2. Réponses OCSP 91
8. Audit de conformité et autres évaluations 92
8.1. Fréquences et ou circonstances des évaluations 92
8.2. Identités et qualifications des évaluateurs 92
8.3. Relations entre évaluateurs et entités évaluées 92
8.4. Sujets couverts par les évaluations 93
8.5. Actions prises suite aux conclusions des évaluations 93
9. Autres problématiques métiers et légales 93
9.1. Tarifs 93
9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats 93
9.1.2. Tarifs pour accéder aux certificats 93
9.1.3. Tarifs pour accéder aux LCR et répondeur OCSP 93
9.1.4. Politique de remboursement 94
9.2. Responsabilité financière 94
9.2.1. Couverture par les assurances 94

9.2.2. Autres ressources 94
9.2.3. Couverture et garantie concernant les entités utilisatrices 94
9.3. Confidentialité des données professionnelles 94
9.3.1. Périmètre des informations confidentielles 94
9.3.2. Informations hors du périmètre des informations confidentielles 94
9.3.3. Responsabilités en termes de protection des informations confidentielles 95
9.4. Protection des données personnelles 95
9.4.1. Politique de protection des données personnelles 95
9.4.2. Responsabilité en termes de protection des données à caractère personnel 95
9.4.3. Notification et consentement d'utilisation des données personnelles 96
9.4.4. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives 96
9.4.5. Autres circonstances de divulgation d'informations personnelles 96
9.5. Droits sur la propriété intellectuelle et industrielle 97
9.6. Interprétations contractuelles et garanties 97
9.7. Limite de responsabilité 97
9.8. Indemnités 97
9.9. Durée et fin anticipée de validité de la PC 98
9.9.1. Durée de validité 98
9.9.2. Fin anticipée de validité 98
9.9.3. Effets de la fin de validité et clauses restant applicables 98
9.10. Amendements à la PC 98
9.10.1. Procédures d'amendements 98
9.10.2. Mécanisme et période d'information sur les amendements 98
9.10.3. Circonstances selon lesquelles l'OID doit être changé 98
9.11. Dispositions concernant la résolution de conflits 99
9.12. Juridictions compétentes 99
9.13. Conformité aux législations et réglementations 99
9.14. Dispositions diverses 99
9.14.1. Interprétation 99
9.14.2. Force majeure 100
10. Annexes sur les exigences de sécurité du module cryptographique de l'AC 100
10.1. Exigences sur les objectifs de sécurité 100
10.2. Exigences sur la certification 101

1. Introduction

1.1. Présentation générale

La société Youtrust est un Fournisseur de service de confiance, qui fournit auprès de ses clients et pour son usage propre des services impliquant des certificats électroniques et en particulier une signature électronique.

Dans ce cadre, ce document constitue la Politique de Certification (PC) ainsi que la Déclaration de Pratiques de Certification (DPC) de l'Autorité de Certification «YOUSIGN SAS - SIGN3 CA », pour les services identifiés à la section identification du document. Ce document regroupe l'ensemble des engagements et des pratiques de Youtrust dans le cadre du déploiement et de l'exploitation de l'AC « YOUSIGN SAS - SIGN3 CA », tant sur les plans techniques que organisationnels.

La société Youtrust a été dénommée Yousign jusqu'au 01/07/2026, date à laquelle sa dénomination sociale a été modifiée au RCS sans changement de SIREN. De ce fait, les Autorités de Certification portent le nom de Yousign et conservent un identifiant correct de la personne morale Youtrust.

La chaîne de certification est la suivante :

- AC Racine : `YOUSIGN SAS - ROOT2 CA`
- AC Émettrice : `YOUSIGN SAS - SIGN3 CA`

Note : Le chapitrage du présent document correspond au plan type tel que donné par la [RFC3647].

1.2. Identification du document

Le présent document décrit plusieurs Politiques de Certification (PC) de l'Autorité de Certification `YOUSIGN SAS - SIGN3 CA`. Les identifiants de ces politiques sont :

- OID `1.2.250.1.302.1.17.1.0` : certificats de signature de niveau LCP de la norme ETSI 319 411-1 pour lesquels l'enregistrement est réalisé par un service en ligne entièrement automatisé ;
- OID : `1.2.250.1.302.1.19.1.0` pour les certificats d'horodatage de niveau NCP+ de la norme ETSI 319 411-1 ;
- OID : `1.2.250.1.302.1.20.1.0` pour les certificats OCSP de l'AC ;

- OID `1.2.250.1.302.1.22.1.0` : certificats de signature de niveau LCP de la norme ETSI 319 411-1 pour lesquels l'enregistrement est réalisé en ligne ;
- OID `1.2.250.1.302.1.23.1.0` pour les certificats de signature de niveau NCP+ de la norme ETSI 319 411-1 pour lesquels l'enregistrement est réalisé en face à face physique (ou méthode reconnue comme équivalente).

Les éléments spécifiques à une politique sont précédés de l'OID de cette politique entre crochets . Plusieurs OID peuvent être spécifiés, dans ce cas ils sont ajoutés les uns à la suite des autres. Dans le cas où un élément s'applique à tous les OID décrits dans ce document, soit le tag `[tous les OID]` est utilisé, soit aucun tag n'est précisé.

Les OID peuvent évoluer en cas de modifications importantes de la PC. Lorsqu'un nouvel OID est généré, le dernier chiffre est incrémenté. La version initiale utilise le chiffre 0.

1.3. Entités intervenant dans l'IGC

1.3.1. Autorités de certification

La notion d'AC telle qu'utilisée dans la présente PC est définie à la section « Définitions ».

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation, etc.) et s'appuie pour cela sur une infrastructure technique : une IGC. Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.

Quelle que soit l'organisation opérationnelle mise en œuvre, y compris en cas de recours à des prestataires ou fournisseurs, l'AC reste in fine responsable vis-à-vis de toute partie externe à l'IGC (porteurs, utilisateurs de certificats, etc.) des prestations fournies et du respect des engagements pris dans cette PC.

Lorsque l'AC utilise une composante fournie par un tiers, elle s'assure qu'elle respecte les exigences d'interface du fournisseur et que la sécurité et les fonctionnalités requises par cette composante sont cohérentes avec les exigences appropriées de la présente politique.

Afin d'éviter tout conflit d'intérêt, les demandeurs de certificat sont externes à l'IGC, sauf pour les cas suivants :

- **[1.2.250.1.302.1.17.1.0]**
  Les personnels Youtrust peuvent demander un certificat en suivant la procédure nominale.
- **[1.2.250.1.302.1.19.1.0]**
  L'AC émet des certificats pour son UH, après vérification de l'origine de la demande.
- **[1.2.250.1.302.1.20.1.0]**
  L'AC émet des certificats pour sa composante OCSP, après vérification de l'origine de la demande.
- **[1.2.250.1.302.1.22.1.0]**
  [1.2.250.1.302.1.23.1.0]
  Les opérateurs d'enregistrement peuvent demander un certificat en suivant la procédure nominale, sans toutefois pouvoir s'enregistrer eux-mêmes.

1.3.2. Autorités d'Enregistrement

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
L'AE vérifie l'identité du futur porteur de certificat comme décrit à la section « Validation initiale de l'identité ».

[1.2.250.1.302.1.19.1.0]
L'AE vérifie l'identité du demandeur du certificat d'horodatage et sa légitimité via le processus d'enregistrement associé. L'AE est opérée par un service interne à Youtrust.

[1.2.250.1.302.1.20.1.0]
L'AC de Youtrust procède elle-même à l'enregistrement du porteur.

1.3.3. Autorités d'Enregistrement Déléguées

[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]

L'AE peut déléguer tout ou partie de ses fonctions à une AED, en relation contractuelle avec elle, incluant le recours à des services automatisé de vérification d'identité.

L'AED agit dans le respect de la présente PC.
Une ou plusieurs des tâches suivantes peuvent être effectuées par l'AED :

- la collecte des données d'identité du futur porteur de certificat (nom, prénom) et de ses coordonnées (numéro de téléphone et adresse email) ;
- la vérification d'identité du futur porteur de certificat ;
- la production d'une attestation de vérification d'identité ;
- la constitution d'un dossier de preuve d'identité intégrant les données d'identité et les coordonnées du futur porteur, ainsi que des preuves en support de la vérification d'identité effectuée;
- l'enregistrement de l'identité et des coordonnées du futur porteur auprès de l'AE ;
- l'archivage du dossier de preuve d'identité et de l'attestation de vérification d'identité.

L'AED dispose de son propre personnel et peut, de plus, déléguer tout ou partie de ses fonctions à des opérateurs d'enregistrement de proximité.
Cette délégation doit toujours être réalisée par l'AED en respectant le cadre de la présente PC et les dispositions contractuelles liant l'AED à Youtrust.

1.3.4. Porteurs de certificats

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
Le porteur de certificat est une personne physique.
Le porteur respecte les conditions qui lui incombent définies dans la PC de l'AC YOUSIGN SAS - SIGN3 CA et résumées dans les CGU qu'il doit accepter avant l'émission de son certificat.

[1.2.250.1.302.1.19.1.0]
Les porteurs sont les unités d'horodatage du service Youtrust, représentés par le responsable des unités d'horodatage.

[1.2.250.1.302.1.20.1.0]

Le porteur est le service OCSP de l'AC représenté par le responsable de l'application OCSP.

1.3.5. Utilisateurs de certificats

La notion d'utilisateur est définie à la section « Définitions ».

1.4. Usage des certificats

1.4.1. Domaines d'utilisation applicables

[1.2.250.1.302.1.17.1.0]

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

Le certificat peut être utilisé pour signer un document ou un message dans tous les domaines pour lesquels une signature est requise à titre de validité ou de preuve et en particulier :

- signature électronique par un porteur, puis vérification de cette signature par une administration ou une entreprise par voie électronique,
- signature électronique par un porteur, puis vérification de cette signature par une personne physique.

Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

[1.2.250.1.302.1.19.1.0]

Les certificats d'horodatage ne sont utilisables que pour signer les contremarques produites par les unités d'horodatage du service Youtrust. Le service d'horodatage dont dépendent ces unités d'horodatage est un service qualifié au sens eIDAS.

[1.2.250.1.302.1.20.1.0]

Les certificats OCSP ne sont utilisables que pour signer les jetons OCSP produits par les répondeurs OCSP de l'AC `YOUSIGN SAS - SIGN3 CA` du service Youtrust.

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

Cette PC comporte également des exigences concernant les bi-clés et certificats de l'AC (signature des certificats émis, des LCR et LAR) ainsi que des clés, bi-clés et certificats des composantes de l'IGC (sécurisation des échanges entre composantes, authentification des opérateurs, etc.).

L'AC génère et signe différents types d'objets : certificats, LCR et LAR. Pour signer ces objets, l'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur dans la hiérarchie des AC que Youtrust met en œuvre. Les réponses OCSP de l'AC sont signées par un certificat émis par l'AC pour un répondeur OCSP de Youtrust.

Les bi-clés et certificats de l'AC ne sont utilisés que pour la signature de certificats, de LCR et LAR, et ne doivent être utilisés qu'à cette fin. Ils ne doivent notamment être utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

1.4.3. Domaines d'utilisation interdits

Tout domaine d'application n'étant pas prévu dans la section « Usage des certificats », est interdit. De plus, les usages du certificat doivent être en conformité avec la législation et la réglementation.

1.5. Gestion de la PC

1.5.1. Entité gérant la PC

La société Youtrust est responsable de la PC.

1.5.2. Point de contact

Toute demande relative à la présente PC doit être adressée à :

Gestion des AC Youtrust 36 rue de Saint Petersbourg 75008 Paris authority@yousign.com

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

Youtrust met en œuvre un Comité de Direction Technique Youtrust. Celui-ci organise des audits et évaluations permettant de s'assurer de la conformité des pratiques (techniques et organisationnelles) aux engagements de l'AC pris dans cette PC.

1.6. Définitions et acronymes

1.6.1. Acronymes

Acronyme	Signification	Traduction
AC	Autorité de Certification	-
ACI	Autorité de Certification Intermédiaire	-
ACP	Autorité de Certification Primaire	-
AE	Autorité d'Enregistrement	-
AED	Autorité d'Enregistrement Déléguée	-
CGU	Conditions Générales d'Utilisation	-
DN	Distinguished Name	Nom distinctif
DPC	Déclaration des Pratiques de Certification	-
HSM	Hardware Security Module	Module cryptographique
IDS	Intrusion Detection System	Système de détection d'intrusion
IGC	Infrastructure de Gestion de Clés	-
LAR	Liste des certificats d'Autorités de Certification Révoqués	-
LCR	Liste des Certificats Révoqués	-
MRZ	Machine-Readable Zone	Zone de lecture optique
OCSP	Online Certificate Status Protocol	Protocole réseau de statut de certificat

Acronyme	Signification	Traduction
OID	Object Identifier	Identifiant d'objet
PC	Politique de Certification	-
RSA	Rivest Shamir Adelman	-
SMS	Short Message Service	Service de messages textes
UH	Unité d'Horodatage	-
URL	Uniform Resource Locator	Localisateur uniforme de ressource
VPN	Virtual Private Network	Réseau virtuel privé

1.6.2. Définitions

Terme	Signification
Abonné	L'abonné est une personne morale cliente de la société Youtrust. Un lien contractuel existe entre l'abonné et la société Youtrust.
Autorité d'Enregistrement	Autorité interne ou externe à la société Youtrust, responsable de la vérification d'identité du futur porteur de certificat et de son enregistrement auprès de l'AC. Dans le cas de l'externalisation, une convention est formalisée entre la société Youtrust et l'AE.
Autorité d'Enregistrement Déléguée	Éventuel délégataire de l'AE, sur tout ou partie de ses fonctions.
Autorité d'Horodatage	Autorité responsable de la gestion d'un service d'horodatage.
Autorité de Certification	Au sein d'un Fournisseur de services de confiance, une AC a en charge, au nom et sous la responsabilité de celui-ci, l'application d'au moins une PC et est identifiée comme telle, en tant qu'émetteur (champ « *issuer* » du certificat), dans les certificats émis au titre de cette PC.
Bi-clé	Une bi-clé est une clé électronique constituée d'une clé publique et d'une clé privée, mathématiquement liées entre elles, utilisées dans des algorithmes de cryptographie dits à clé publique ou asymétrique telle que la signature électronique.
Certificat électronique	Fichier électronique attestant qu'une bi-clé appartient à la personne physique, morale, à l'élément matériel ou logiciel

Terme	Signification
	identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une AC. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique, morale, l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.
Clé privée	Clé de la bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité.
Clé publique	Clé de la bi-clé asymétrique d'une entité qui peut être rendue publique.
Code d'authentification	Code à usage unique utilisé comme élément de vérification d'identité du demandeur de certificat
Comité de Direction Technique	Le comité de direction technique est un comité interne à Youtrust chargé du bon fonctionnement de l'IGC Youtrust.
Composante	Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC. L'entité responsable de la composante peut être Youtrust elle-même ou une entité externe liée par voie contractuelle, réglementaire ou hiérarchique.
Déclaration des Pratiques de Certification	Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique et en conformité avec la ou les PC qu'elle s'est engagée à respecter.
Demande de certificat	Formulaire identifiant le demandeur (futur porteur) de certificat, les futurs attributs du certificat, et contextualisant cette demande (nom de l'AC et OID du service).
Dossier d'enregistrement	Dossier regroupant : • l'ensemble des éléments de preuves relatifs à l'identification du futur porteur du certificat ou un pointeur vers le dossier de preuve d'identité ; • les CGU acceptées par le futur porteur ; • la demande de certificat du futur porteur.

Terme	Signification
Dossier de preuve d'identité	Dossier regroupant l'ensemble des éléments de preuves relatifs à l'identification du futur porteur du certificat et garantissant l'unicité de l'identification.
Entité	Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.
Fonction d'information sur l'état des certificats	Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR).
Fonction de génération des certificats	Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du porteur ainsi que de la fonction de génération des éléments secrets du porteur.
Fonction de génération des éléments secrets du porteur	Cette fonction génère la bi-clé du porteur.
Fonction de gestion des révocations	Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
Fonction de publication	Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats.
Fournisseur de service de confiance	Un Fournisseur de service de confiance est une entité qui propose un ou plusieurs services de confiance au titre du règlement eIDAS, dont celui de délivrance et de gestion de Certificats électroniques.
Infrastructure de Gestion de Clés	Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, d'une entité d'archivage, d'une entité de publication, etc.

Terme	Signification
Magic Link	Lien d'authentification unique et temporaire permettant d'accéder au parcours de signature.
Modules cryptographiques	Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée utilisée pour conserver et mettre en œuvre la clé privée d'AC, les bi-clés des certificats de porteur et réaliser des opérations cryptographiques.
Opérateur d'enregistrement	Personne physique ayant pour rôle tout ou partie des fonctions de l'AE(D).
Personne autorisée	Il s'agit d'une personne autre que le porteur qui est autorisée par la PC de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, etc.). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du porteur.
Politique de Certification	Ensemble de règles, identifiées par un OID, définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.
Porteur	La personne physique identifiée dans le certificat et qui est la seule personne autorisée à utiliser la clé privée correspondant à la clé publique qui est dans le certificat.
Service de signature Youtrust	Le service de signature fourni par Youtrust permettant à un porteur d'utiliser la clé privée correspondant à la clé publique qui est dans le certificat qui l'identifie en vue de réaliser des signatures électroniques de données et d'autoriser la signature de ces données par d'autres utilisateurs. C'est le seul système autorisé à accéder aux clés privées des porteurs. Pour pouvoir utiliser leur clé privée, les porteurs doivent s'authentifier via un Code d'authentification.
Utilisateur	Un utilisateur est une personne physique ou morale ayant accès à un fichier signé, dont la signature a été générée par la clé privée d'un certificat émis par l'AC couverte par

Terme	Signification
	cette PC. Il est à noter qu'aucun lien direct n'existe entre la société Youtrust et un utilisateur.

2. Responsabilités concernant la mise à disposition des informations devant être publiées

2.1. Entités chargées de la mise à disposition des informations

Youtrust a mis en place une page regroupant les publications à l'adresse suivante : https://youtrust.com/fr-fr/documentation-technique-des-certifications

2.2. Informations devant être publiées

Youtrust publie les informations suivantes :

- l'ensemble des PC gérées par Youtrust, dont la présente ;
- les listes de révocation (LCR/LAR) ;
- les certificats de la hiérarchie d'AC jusqu'à l'AC racine ;
- les CGU Youtrust pour les différentes AC.

Les PC, les certificats et les CGU publiés en ligne sont accompagnés d'une empreinte (algorithme SHA-256) permettant d'en vérifier l'intégrité.

Un espace du lieu de publication est réservé à l'archivage des anciennes versions des données publiées.

2.3. Délais et fréquences de publication

Les délais et fréquences de publication sont les suivants :

- La PC est publiée avant toute émission d'un certificat final ;
- les LCR sont publiées quotidiennement, les LAR annuellement ou suite à une révocation d'AC ;

- les certificats d'AC sont publiés suite à leur émission et avant toute signature d'un certificat final ;
- les CGU sont publiées suite à chaque mise à jour et avant toute émission d'un certificat final.

Ces informations sont disponibles sept jours sur sept, vingt-quatre heures sur vingt-quatre, avec une disponibilité de 99.7% sur un mois.

Le Comité de Direction Technique Youtrust décide des différentes parties (clients, utilisateurs, sous-traitants de la fourniture du service, organismes de contrôle, etc.) à informer lors de la publication effective ou à venir d'une nouvelle PC (version initiale ou modification d'une PC existante) selon la nature des évolutions apportées. En particulier, les clients de Youtrust, les porteurs et les utilisateurs de certificats sont informés des changements à venir dès lors que l'évolution est susceptible d'affecter leur adhésion au service.

2.4. Contrôle d'accès aux informations publiées

Toutes les informations publiées indiquées ci-dessus, sont publiques et ne font pas l'objet de restrictions d'accès.

L'accès en modification aux données publiées est restreint aux équipes internes Youtrust en charge de publier les documents sur l'espace de publication. Un contrôle d'accès fort et nominatif est mis en place, respectant la politique de mot de passe Youtrust qui est conforme aux exigences réglementaires en vigueur.

3. Identification et authentification

3.1. Nommage

3.1.1. Types de noms

Les noms utilisés sont conformes aux spécifications de la norme [X.500].

Les certificats sont conformes à la norme [X.509]. Les certificats seront identifiés par un DN conforme aux spécifications de la norme [X.501].

[1.2.250.1.302.1.17.1.0]

Nom du champ	Description	Obligatoire
CN	CommonName Nom et prénom du porteur	Oui
serialNumber	serialNumber Date et heure de lancement de la génération du certificat	Oui
SN	surname Nom du porteur	Non
GN	givenName Prénom du porteur	Non
C	Country FR	Oui

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

Nom du champ	Description	Obligatoire
CN	CommonName Nom et prénom du porteur	Oui
serialNumber	serialNumber Date et heure de lancement de la génération du certificat	Oui
OU	OrganisationUnit Identification de l'AED au format identifiant:nom Le nom peut être tronqué	Oui
SN	surname Nom du porteur	Non

Nom du champ	Description	Obligatoire
GN	givenName Prénom du porteur	Non
C	Country FR	Oui

[1.2.250.1.302.1.19.1.0]

Nom du champ	Description	Obligatoire
CN	CommonName « Yousign timestamp unit N » avant le changement de nom, ou « Youtrust timestamp unit N », où « N » est un numéro	Oui
serialNumber	serialNumber Date et heure de lancement de la génération du certificat	Oui
OI	OrganizationIdentifier NTRFR-794513986	Oui
O	Organization YOUSIGN SAS	Oui
C	Country FR	Oui

[1.2.250.1.302.1.20.1.0]

Nom du champ	Description	Obligatoire
CN	CommonName « OCSP Service N Youtrust », où « N » est un numéro	Oui
serialNumber	serialNumber	Oui

Nom du champ	Description	Obligatoire
	Date et heure de lancement de la génération du certificat	
OI	OrganizationIdentifier NTRFR-794513986	Oui
O	Organization YOUSIGN SAS	Oui
C	Country FR	Oui

Les certificats de test émis par l'AC YOUSIGN SAS - SIGN3 CA sont identifiables par l'ajout du préfixe « TEST – » dans la valeur de l'attribut CN, par exemple :
CN = TEST – Jean DUPONT,...
En dehors de cette spécificité, les certificats de tests émis par l'AC YOUSIGN SAS - SIGN3 CA suivent les mêmes processus que les certificats de production nominale.

3.1.2. Nécessité d'utilisation de noms explicites

Les noms contenus dans les certificats sont explicites.

3.1.3. Pseudonymisation des noms

La présente PC n'autorise pas l'utilisation de pseudonyme dans les certificats.

3.1.4. Règles d'interprétation des différentes formes de nom

Les éléments contenus dans la section « Identification et authentification » fournissent les explications permettant d'interpréter correctement les différentes formes de nom.

3.1.5. Unicité des noms

Pour assurer l'unicité des noms, l'AE ajoute dans le DN un champ serialNumber correspondant à la date et à l'heure de lancement de la génération du certificat.

3.1.6. Identification, authentification et rôle des marques déposées

L'AE se réserve le droit de suspendre la génération d'un certificat si le CN est susceptible d'être lié ou de porter préjudice à un quelconque titre ou droit de propriété intellectuelle.

Si un tel cas arrive, l'AE demandera au porteur les informations et documents démontrant la légitimité de son CN. A défaut, le porteur devra demander la génération d'un nouveau certificat avec une modification du CN permettant d'éviter la reprise et résoudre le litige.

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clé privée

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
Les bi-clés des porteurs sont générées dans le dispositif de création de signature de l'infrastructure Youtrust, et la preuve de possession de clé est construite sous forme de CSR signée avec la clé privée du porteur.
Youtrust met en œuvre des moyens techniques et organisationnels afin d'assurer que la clé privée ne sera utilisée que par le porteur.
En aucun cas Youtrust ne pourra utiliser cette clé pour son propre usage ou pour le compte d'une autre personne que le porteur.

[1.2.250.1.302.1.19.1.0]
Le responsable de l'unité d'horodatage présente une CSR signée avec la clé privée de l'UH.

[1.2.250.1.302.1.20.1.0]
Les certificats OCSP sont produits par l'AC pour son propre usage. Le responsable de l'application OCSP présente une CSR signée avec la clé privée du répondeur.

3.2.2. Validation de l'identité d'un organisme

Sans objet.

3.2.3. Validation de l'identité d'un individu

3.2.3.1. Validation de l'identité du porteur

[1.2.250.1.302.1.17.1.0]

La validation initiale de l'identité du porteur est réalisée par l'AE avec un service en ligne entièrement automatisé.

L'AE vérifie l'identité du futur porteur en s'appuyant sur une pièce d'identité fournie par celui-ci, directement à l'AE ou à l'abonné qui la transmettra à l'AE. Les pièces d'identité acceptées sont :

- la carte d'identité ;
- le passeport ;
- la carte de séjour.

Les attributs présents sur la pièce d'identité et nécessaires pour la demande de certificat sont extraits et comparés par le service en ligne avec les informations saisies par l'abonné. Dans le cas où des caractères spéciaux sont présents dans les informations saisies par l'abonné, le service en ligne opère une translittération, visible dans la demande de certificat, sur ceux-ci, préalablement à l'opération de comparaison.

À l'issue de la vérification initiale de l'identité, l'utilisateur dispose d'un délai de trente (30) jours pour obtenir son certificat, sans qu'il lui soit nécessaire de procéder à une nouvelle vérification d'identité, et ce, nonobstant l'expiration éventuelle du document d'identité présenté lors de ladite vérification.

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

La validation initiale de l'identité du porteur est réalisée par l'AE(D) auprès d'un opérateur d'enregistrement.

L'AE(D) vérifie l'identité du futur porteur en s'appuyant sur un document d'identité fournie par celui-ci. Les documents d'identité doivent cumuler les critères suivants pour être acceptées :

- La pièce est officiellement reconnue comme justificatif d'identité par l'Etat ayant émis le document ;
- L'AE(D) est en capacité d'authentifier le document.

L'AE(D) s'assure de l'authenticité et de la validité de la pièce d'identité :

- La pièce ne présente pas de modification apparente (pièce endommagée, surchargée, etc.) ;
- La date de validité de la pièce n'a pas été dépassée ;
- Les attributs présents sur la pièce d'identité et nécessaires pour la demande de certificat correspondent.

L'AE(D) collecte les coordonnées du porteur (numéro de téléphone et adresse email) et les attributs présents sur le document d'identité (prénom(s) et nom). Elle constitue le dossier de preuve d'identité puis génère une attestation de vérification d'identité.

L'AE(D) transmet à l'AC Youtrust les éléments utiles à la génération du certificat.

[1.2.250.1.302.1.23.1.0]

En complément, les contrôles supplémentaires suivants doivent être appliqués par l'AE(D) :

- La validation d'identité du porteur est réalisée en face à face physique (ou méthode reconnue comme équivalente) avec un opérateur d'enregistrement ;
- Les marqueurs de sécurité de la pièce présentée doivent être vérifiés (hologrammes, encres variables, etc.) ;
- Les attributs de la pièce d'identité permettant la reconnaissance physique de son porteur sont cohérents avec la personne présente.

[1.2.250.1.302.1.19.1.0]

Le responsable de l'unité d'horodatage Youtrust s'adresse à l'AE pour l'obtention d'un certificat d'UH. L'AE valide l'identité du demandeur par vérification en face à face physique (ou méthode reconnue comme équivalente) d'une pièce d'identité (carte

d'identité ou passeport) puis vérifie dans l'organigramme interne que le demandeur est bien responsable de l'unité d'horodatage et donc de son certificat.

[1.2.250.1.302.1.20.1.0]

Les certificats OCSP sont produits par l'AC pour son propre usage, sur demande du responsable de l'application OCSP. L'AC vérifie dans l'organigramme interne que le demandeur est bien responsable de l'application OCSP d'après la gestion des rôles de confiance.

3.2.3.2. Habilitation d'un opérateur d'enregistrement

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

L'AE(D) doit établir et respecter un processus d'habilitation et de gestion de ses opérateurs, notamment en :

- Maintenant une liste de ses opérateurs ;
- Vérifiant l'identité de ses opérateurs ;
- Maintenant avec ses opérateurs des liens hiérarchiques ou contractuels ;
- Contrôlant la compétence de ses opérateurs et leur acceptation des obligations qui leur incombent ;
- En identifiant et en authentifiant les opérateurs sur son système d'information.

3.2.4. Informations non vérifiées du porteur

La présente PC ne formule pas d'exigence spécifique sur le sujet.

3.2.5. Validation de l'autorité du demandeur

[1.2.250.1.302.1.19.1.0]

L'AE vérifie dans la gestion des rôles de confiance que le demandeur est bien responsable de l'unité d'horodatage.

[1.2.250.1.302.1.20.1.0]

L'AC vérifie dans la gestion des rôles de confiance que le demandeur est bien responsable de l'application OCSP.

[1.2.250.1.302.1.17.1.0]

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

Aucune vérification n'est effectuée, le porteur étant une personne physique agissant en son nom propre.

3.2.6. Certification croisée d'AC

Sans objet.

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

3.3.1. Identification et validation pour un renouvellement courant

[1.2.250.1.302.1.17.1.0]

[1.2.250.1.302.1.19.1.0]

[1.2.250.1.302.1.20.1.0]

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

L'identification et la validation de l'identité du porteur pour un renouvellement correspond à une nouvelle demande de certificat. Le processus spécifié dans la section « Validation initiale de l'identité » s'applique.

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

Alternativement, la vérification d'identité du porteur peut être considérée comme valable pour une durée de trois (3) ans à condition que la date d'expiration de la pièce d'identité présentée initialement ne soit pas atteinte au moment de la communication par l'AE(D) des informations du porteur à l'AC Youtrust. Si ces conditions ne sont pas remplies, l'identification du porteur pour l'émission d'un nouveau certificat s'effectue selon le processus spécifié dans la section « Validation initiale de l'identité ».

La date de vérification d'identité du futur porteur est vérifiée par l'AE via l'attestation de vérification d'identité transmise par l'AED.

3.3.2. Identification et validation pour un renouvellement après révocation

[1.2.250.1.302.1.17.1.0]

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

Sans objet, les certificats de signature sont éphémères et ne peuvent pas être révoqués.

[1.2.250.1.302.1.19.1.0]

[1.2.250.1.302.1.20.1.0]

L'identification et la validation de l'identité du porteur pour un renouvellement après révocation correspond à une demande initiale de certificat. Le processus spécifié dans la section « Validation initiale de l'identité » s'applique.

3.4. Identification et validation d'une demande de révocation

[1.2.250.1.302.1.17.1.0]

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

Ces certificats de signature sont des certificats éphémères, c'est-à-dire dont la durée de validité est largement inférieure au délai de traitement d'une demande de révocation fixé à un (1) jour.

En conséquence, aucun processus de révocation n'existe ni pour le porteur, ni pour l'AE (D), ni pour l'AC. Toutefois, le porteur, l'AE(D) peuvent notifier l'AC d'un incident relatif à l'un de ces certificats en utilisant le point de contact de l'AC défini au paragraphe Point de contact. Les incidents déclarés sont enregistrés et traités par l'AC.

[1.2.250.1.302.1.19.1.0]

Le responsable de l'autorité d'horodatage s'adresse en personne à l'AE, qui l'identifie sur la base de la gestion des rôles de confiance de Youtrust.

[1.2.250.1.302.1.20.1.0]

La révocation d'un certificat OCSP est une décision exceptionnelle qui serait traitée comme en tant que révocation d'un certificat d'une composante de l'AC (cf. section

révocation et suspension des certificats). Le responsable de l'application OCSP s'adresse en personne à l'AC, qui l'identifie sur la base de la gestion des rôles de confiance de Youtrust.

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
La demande de certificat provient du besoin de faire signer par un porteur un document.

[1.2.250.1.302.1.19.1.0]
La demande de certificat provient du besoin d'apposer des contremarques de temps.

[1.2.250.1.302.1.20.1.0]
La demande de certificat provient du besoin de signer les réponses aux requêtes OCSP.

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

[1.2.250.1.302.1.17.1.0]
La demande de certificat est initiée par le porteur qui se rend sur le service en ligne de l'AE via un *magic link* reçu dans une invitation à signer.
Le porteur fournit les informations demandées par l'AE (notamment pour valider son identité), accepte les CGU de l'AC et signe sa demande de certificat. Si le parcours de signature implémenté par l'abonné le permet, ce dernier peut transmettre à l'AE la pièce d'identité du porteur, qui n'est alors pas demandée à celui-ci. L'AE établit le dossier d'enregistrement du futur porteur comprenant au moins :

- le nom et prénom du porteur à utiliser dans le certificat ;
- le numéro de téléphone du porteur utilisé à des fins d'authentification ;

- la MRZ extraite de la pièce d'identité du porteur, à défaut une copie de l'intégralité de la pièce d'identité du futur porteur ;
- les CGU acceptées par le futur porteur ;
- la demande de certificat du futur porteur.

L'AE s'assure de disposer d'une information permettant de contacter le futur porteur du certificat, l'adresse électronique ou le numéro de téléphone étant obligatoires.

[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
La demande de certificat est initiée par le porteur qui se rend auprès d'une AE(D) dans le but de signer un document.
Le porteur fournit les informations demandées par l'AE(D), notamment pour valider son identité. L'AE(D) constitue le dossier de preuve d'identité comprenant :

- les noms et prénoms du porteur à utiliser dans le certificat ;
- le numéro de téléphone du porteur à des fins d'authentification ;
- tout identifiant unique de document garantissant l'unicité du document, ou à défaut une copie de l'intégralité de la pièce d'identité du futur porteur.

L'AE(D) génère une attestation de vérification d'identité (sauf éventuellement dans le cas d'une nouvelle demande de certificat pour un porteur déjà enregistré), puis transmet à l'AC Youtrust les éléments de l'identité constituant la génération du certificat.

La demande de certificat est poursuivie par le porteur sur le service en ligne de l'AC Youtrust via un *magic link* reçu dans une invitation à signer.
Le porteur accepte les CGU de l'AC et signe sa demande de certificat.

L'AE(D) établit le dossier d'enregistrement du futur porteur comprenant au moins :

- les noms et prénoms du porteur à utiliser dans le certificat ;
- le numéro de téléphone du porteur utilisé à des fins d'authentification ;
- l'identifiant de l'attestation de vérification d'identité ;
- les CGU acceptées par le futur porteur ;
- la demande de certificat du futur porteur.

[1.2.250.1.302.1.19.1.0]

Le futur porteur établit directement le dossier d'enregistrement comprenant :

- une copie de sa pièce d'identité en cours de validité ;
- une demande de certificat sous forme de CSR comportant le nom complet de l'unité d'horodatage ;
- les conditions générales d'utilisation qu'il a signées.

Le futur porteur transmet le dossier à l'AE qui effectue les vérifications d'identité et d'autorité.

[1.2.250.1.302.1.20.1.0]
Le processus de demande et de génération du certificat OCSP suit une procédure interne qui n'est pas détaillée dans cette PC. Une cérémonie des clés est menée dans un environnement sécurisé et fait l'objet d'un procès-verbal signé par l'AC.

4.2. Traitement d'une demande de certificat

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

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
La vérification d'identité est réalisée par l'AE(D) conformément au processus décrit dans la section « Validation initiale de l'identité ».
Le cas échéant, l'AE(D) vérifie que l'attestation de vérification d'identité est encore valide au regard des critères définis dans la section « Identification et validation pour un renouvellement courant ».
L'AE s'assure de l'acceptation des CGU et de la validation de la demande de certificat par le futur porteur.

[1.2.250.1.302.1.19.1.0]
Une fois la vérification d'identité réalisée par un opérateur de l'AE conformément au processus décrit dans la section « Validation initiale de l'identité », la demande est transmise à l'AC et le dossier d'enregistrement est conservé dans le script de cérémonie de la génération du certificat de l'unité d'horodatage.

4.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE(D) ou l'AC en informe le demandeur en justifiant le rejet.

4.2.3. Durée d'établissement du certificat

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.19.1.0]
L'AE et l'AC doivent s'efforcer de traiter la demande de certificat dans un délai raisonnable. Néanmoins, il n'y a aucune restriction concernant la durée maximale ou minimale de traitement.

[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
L'AE(D) s'efforce de traiter les phases de validation d'identité et d'enregistrement sans délai indu. Le dossier d'enregistrement demeure valide tant que les conditions décrites à la section « Identification et validation d'une demande de renouvellement des clés » sont respectées et permet ainsi l'établissement de la demande de certificat. Néanmoins, il n'y a aucune restriction concernant la durée maximale ou minimale de traitement entre la demande de certificat et l'établissement de celui-ci par l'AC.

4.3. Délivrance du certificat

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

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
Le processus de génération du certificat est lié de manière sécurisée au processus de génération de la bi-clé. La clé privée et le certificat sont intégrés au module cryptographique de l'IGC.

Les conditions de génération des bi-clés et des certificats, ainsi que les mesures de sécurité à respecter sont précisées aux sections « Mesures de sécurité non

techniques » et « Mesures de sécurité techniques », notamment la séparation des rôles de confiance dans la section « Mesures de sécurité procédurales ».

[1.2.250.1.302.1.19.1.0]
L'AC produit le certificat sur la base de la CSR transmise par l'AE et le fournit en main propre au responsable de l'unité d'horodatage.

4.3.2. Notification par l'AC de la délivrance du certificat

Pas de notification au porteur.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
L'acceptation d'un certificat émis par l'AC est tacite dès la signature effectuée via le service de signature. Avant cette utilisation, le porteur peut refuser la génération du certificat en interrompant le processus de signature. Si la bi-clé avait déjà été générée, cette dernière est détruite de manière automatique par un processus technique. L'AC conserve une trace de l'acceptation (action de la signature) du certificat par le porteur. Cette acceptation sera horodatée.

[1.2.250.1.302.1.19.1.0]
L'acceptation du certificat est réalisée par le responsable de l'unité d'horodatage qui reçoit et vérifie immédiatement le certificat. En cas de refus, le responsable de l'unité d'horodatage demande la révocation du certificat. La vérification et l'acceptation sont consignées dans le script de cérémonie de clés de l'unité d'horodatage.

4.4.2. Publication du certificat

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]

L'AC ne publie pas les certificats des porteurs émis. Les certificats sont accessibles dans chaque document signé.

[1.2.250.1.302.1.19.1.0]
Le certificat est publié par l'AH avant son utilisation, conformément aux dispositions prévues dans la PH.

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

L'AC informe l'AE de l'émission du certificat.

4.5. Usages de la bi-clé et du certificat

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

La clé privée et le certificat ne peuvent être utilisés que dans le cadre prévu à la section « Usage des certificats ».

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
Le certificat étant éphémère, la clé privée n'est utilisée que dans le cadre de l'opération de signature. La clé privée correspondante est détruite à la fin de ce processus.

[1.2.250.1.302.1.19.1.0]
Les clés privées des unités d'horodatage ne sont utilisables que pour signer les contremarques produites par les unités d'horodatage.

[1.2.250.1.302.1.20.1.0]
Les clés privées du service OCSP ne sont utilisables que pour signer les jetons OCSP produits par les répondeurs OCSP.

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

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
Les certificats de signature sont utilisés pour vérifier la validité des signatures réalisées sur le service de signature.

[1.2.250.1.302.1.19.1.0]
Les certificats des UH sont utilisés pour vérifier la validité des jetons d'horodatage (des dispositions sont prévues dans la PH).

[1.2.250.1.302.1.20.1.0]
Les certificats OCSP sont utilisés pour vérifier la validité des jetons OCSP produits.

4.6. Renouvellement d'un certificat

Conformément à la [RFC3647], la notion de renouvellement de certificat correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent, y compris la clé publique.

Dans le cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. L'AC générant les bi-clés garantit qu'un certificat correspondant à une bi-clé existante ne peut pas être renouvelé au sens de la [RFC3647].

4.6.1. Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2. Origine d'une demande de renouvellement

Sans objet.

4.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet.

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

Sans objet.

4.6.5. Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6. Publication du nouveau certificat

Sans objet.

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

Sans objet.

4.7. Délivrance d'un nouveau certificat suite au changement de la bi-clé

Conformément à la [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat liée à la génération d'une nouvelle bi-clé.

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

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]

Les certificats de signature sont des certificats éphémères et ne peuvent pas être révoqués. Une nouvelle bi-clés et un nouveau certificat sont générés pour chaque nouvelle invitation à signer.

[1.2.250.1.302.1.19.1.0]
Les bi-clés des unités d'horodatage, et les certificats correspondants, seront renouvelés au minimum à une fréquence de 3 ans.

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

La délivrance d'un nouveau certificat provient des origines décrites à la section « Demande de certificat ».

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

Cf. section « Traitement d'une demande de certificat » et « Actions de l'AC concernant la délivrance du certificat ».

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

Cf. section « Notification par l'AC de la délivrance du certificat ».

4.7.5. Démarche d'acceptation du nouveau certificat

Cf. section « Démarche d'acceptation du certificat ».

4.7.6. Publication du nouveau certificat

Cf. section « Publication du certificat ».

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

Cf. section « Notification par l'AC aux autres entités de la délivrance du certificat ».

4.8. Modification du certificat

Les certificats de signature sont des certificats éphémères et ne peuvent pas être révoqués.

Pour modifier un certificat, il faudra faire une nouvelle demande auprès de l'AC en respectant le processus de demande initiale. Les actions réalisées par l'AC sont décrites dans les sections « Révocation et suspension des certificats » et « Délivrance d'un nouveau certificat suite au changement de la bi-clé ».

4.8.1. Causes possibles de modification d'un certificat

Sans objet.

4.8.2. Origine d'une demande de modification d'un certificat

Sans objet.

4.8.3. Procédure de traitement d'une demande de modification d'un certificat

Sans objet.

4.8.4. Notification de l'établissement du certificat modifié

Sans objet.

4.8.5. Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6. Publication du certificat modifié

Sans objet.

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

Sans objet.

4.9. Révocation et suspension des certificats

4.9.1. Causes possibles d'une révocation

4.9.1.1. Certificats de porteur

[1.2.250.1.302.1.17.1.0]

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

La révocation de ces certificats n'est pas possible, le porteur ou l'AE(D) pouvant toutefois informer l'AC d'un incident concernant le certificat comme par exemple une erreur dans le nom du porteur ou l'usurpation d'une identité (voir Identification et validation d'une demande de révocation).

[1.2.250.1.302.1.19.1.0]

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance, soit parce qu'elle en a été informée, soit parce qu'elle obtient l'information au cours d'une de ses vérifications, le certificat concerné doit être révoqué :

- les informations figurant dans le certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- les obligations découlant des CGU ou de la PC, ou les modalités applicables d'utilisation du certificat n'ont pas été respectées ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ou dans le certificat ;
- les données d'activation sont suspectées de compromission, compromises, perdues, volées ou révoquées ;
- la clé privée du certificat est suspectée de compromission, compromise, perdue, ou volée ;
- une personne autorisée demande la révocation du certificat ;

- un certificat de la chaîne de certification (ACP ou ACI) est révoqué, entraînant de fait la révocation de tous les certificats émis par cette AC.

4.9.1.2. Certificats d'une composante de l'AC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC, y compris un certificat d'AC pour la génération de certificats et de LCR ou LAR :

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant la composante.

4.9.2. Origine d'une demande de révocation

4.9.2.1. Certificats de porteur

[1.2.250.1.302.1.19.1.0]

Les personnes qui peuvent demander la révocation d'un certificat sont les suivantes :

- le porteur ;
- l'AC émettrice du certificat ou l'une de ses composantes.

4.9.2.2. Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Révocation d'un certificat de porteur

[1.2.250.1.302.1.19.1.0]

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites à la section « Identification et validation d'une demande de révocation ».

Les informations suivantes doivent figurer dans la demande de révocation de certificat :

- l'identité du demandeur de la révocation ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (nom distinctif) ;
- la cause de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation sera diffusée au minimum via une LCR signée par une entité désignée par l'AC.

Le demandeur de la révocation sera informé de l'opération de révocation et de son résultat, que le certificat ait été révoqué ou non. De plus, si le porteur du certificat n'est pas le demandeur, il sera également informé de la révocation effective de son certificat.

L'opération est enregistrée dans les journaux d'évènements.

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

En cas de révocation d'un des certificats de la chaîne de certification, l'AC doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés (disposant d'un certificat non révoqué ni expiré) que leurs certificats ne sont plus valides, en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Afin de faciliter la révocation du certificat de l'AC, celle-ci est signée par une autorité supérieure racine.

4.9.4. Délai accordé pour formuler la demande de révocation

[1.2.250.1.302.1.19.1.0]

Dès que le porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

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

4.9.5.1. Révocation d'un certificat de porteur

[1.2.250.1.302.1.19.1.0]

Par nature, une demande de révocation doit être traitée en urgence. La fonction de gestion des révocations est disponible 24h/24h 7j/7j.

Toute demande de révocation d'un certificat de porteur sera traitée dans un délai inférieur à 24h, ce délai s'entend entre la réception de la demande de révocation et la mise à disposition de l'information de révocation auprès des utilisateurs.

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

La révocation d'un certificat d'une composante de l'IGC doit être effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat.

La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la LCR de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

La révocation d'un certificat de signature de l'AC (signature de certificats et de LCR / LAR) sera effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

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

L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Il pourra utiliser la dernière LCR publiée par l'AC afin de vérifier le statut de révocation du certificat. L'utilisateur doit aussi vérifier le statut de révocation des AC de la chaîne de certification en utilisant pour chacune la dernière LAR émise par l'AC de niveau supérieur.

4.9.7. Fréquence d'établissement des LCR

Les LCR de l'AC YOUSIGN SAS SIGN3 CA ont une durée de validité de 7 jours. Une nouvelle LCR est générée au moins une fois par période glissante de 4 jours, soit 3 jours avant l'expiration de la LCR en cours. En cas d'échec de génération, le processus est automatiquement réitéré jusqu'à succès.

4.9.8. Délai maximum de publication d'une LCR

Les LCR sont publiées le plus rapidement possible après leur génération, ce délai de publication sera de trente (30) minutes maximum.

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

L'AC met à disposition un service OCSP de vérification en ligne de la révocation des certificats. Le service OCSP prend en compte sans délai la révocation des certificats. L'information fournie par le service OCSP est donc toujours la plus à jour, un délai maximum de 24h peut s'écouler avant que la LCR n'indique une révocation déjà remontée par une réponse OCSP.

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

Les utilisateurs de certificats peuvent utiliser librement le service OCSP ou les LCR en fonction de leur contexte et de leurs capacités.

4.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet.

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

Pour les certificats, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, outre les exigences de la section « Révocation et suspension des certificats », la révocation suite à une compromission de la clé privée fera l'objet d'une information diffusée clairement sur le site Internet www.youtrust.com. De plus, en cas de compromission de la clé privée de l'AC, l'AC s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé. La révocation d'une AC est publiée par Youtrust dans la LAR émise par l'AC de niveau supérieur, conformément aux engagements stipulés à la section « Responsabilités concernant la mise à disposition des informations devant être publiées ».

4.9.13. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC.

4.9.14. Origine d'une demande de suspension

Sans objet.

4.9.15. Procédure de traitement d'une demande de suspension

Sans objet.

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

Sans objet.

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

4.10.1. Caractéristiques opérationnelles

Youtrust fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'ACP), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR et l'état du certificat de l'ACP.

Les LCR / LAR sont publiées à l'adresse spécifiée dans la section « Entités chargées de la mise à disposition des informations », et à l'adresse contenue dans les certificats émis.

Le service OCSP (limité au statut de révocation des certificats de porteurs) est disponible à l'adresse spécifiée dans la section « Entités chargées de la mise à disposition des informations » qui est aussi contenue dans les certificats émis.

4.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24h, 7j/7j.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4h et un taux de disponibilité annuel de 99,9%.

4.10.3. Dispositifs optionnels

La présente PC ne formule pas d'exigence spécifique sur le sujet.

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

[1.2.250.1.302.1.17.1.0]

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

Le porteur obtient à chaque demande un certificat éphémère de signature pour lequel il peut, même après expiration, informer l'AC d'un incident, comme par exemple une erreur dans le nom du porteur ou l'usurpation d'une identité (voir Identification et validation d'une demande de révocation).

[1.2.250.1.302.1.19.1.0]

Sans objet, le porteur et l'AC sont internes à Youtrust.

4.12. Séquestre de clé et recouvrement

L'AC ne séquestre aucune clé privée.

4.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

5. Mesures de sécurité non techniques

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

Les sites d'hébergement des services de certification Youtrust sont situés dans des locaux sécurisés.

5.1.2. Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès aux locaux des différentes composantes de l'IGC sont contrôlés. Les personnes devront s'authentifier et disposer des droits nécessaires pour accéder physiquement et logiquement à l'ensemble des ressources et fonctionnalités de l'IGC.

5.1.3. Alimentation électrique et climatisation

Des systèmes de protection de l'alimentation électrique et de la climatisation sont mis en œuvre afin d'assurer la continuité des services délivrés.
Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et/ou constructeurs.

5.1.4. Vulnérabilité aux dégâts des eaux

L'hébergement est réalisé dans une zone non inondable.

5.1.5. Prévention et protection incendie

Les moyens de prévention et de protection contre les incendies mis en œuvre par l'IGC permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC, en matière de disponibilité.

5.1.6. Conservation des supports

Des sauvegardes des supports sont réalisées quotidiennement. Les sites dans lesquels sont conservées les sauvegardes sont protégés contre les risques d'incendies et d'inondation. De plus, les accès physiques et logiques sont protégés et soumis à une gestion des droits et à une authentification forte.
S'il y a utilisation de documents papiers, ou de supports amovibles tels qu'un CD, une clé USB de stockage, un disque dur externe ou une carte à puce, ceux-ci seront conservés dans un coffre-fort uniquement accessible par des personnes habilitées.
Des procédures de gestion protègent les supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

L'AE(D) et ses opérateurs sont responsables de la conservation des documents constitutifs des dossiers d'enregistrement, sous forme papier ou numérique. Ils mettent en œuvre des mesures de sécurité afin de garantir la disponibilité, la confidentialité et l'intégrité de ces données.
L'AE(D) et ses opérateurs sont également responsables de garantir la traçabilité de ces données notamment en établissant un lien non équivoque entre la demande de certificat et la vérification de l'identité du futur porteur.

5.1.7. Mise hors service des supports

La mise hors service des différents supports varie en fonction de leur nature. En ce qui concerne les documents papiers, les CD, les clés USB de stockage, les cartes à puce, ils seront broyés en fin de vie (fin d'utilisation ou obsolescence). Les supports de stockage seront vidés, puis détruits. Les HSM seront mis hors service en suivant les directives du constructeur.

5.1.8. Sauvegardes hors site

Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, disposent d'une sauvegarde hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.). Les fonctions de sauvegarde et de restauration seront effectuées par des administrateurs autorisés conformément aux mesures de sécurité procédurales.
Les sauvegardes hors sites sont conservées dans un environnement sécurisé en accès physique et logique, et sécurisé contre les risques d'incendie et d'inondation.

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance

Le Comité technique Youtrust met en œuvre les rôles suivants :

- **Responsable de sécurité** : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre

connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats.

- **Responsable d'application** : Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
  Le responsable d'application gère les autorisations en fonction des rôles, et délivre les données d'authentification.
- **Ingénieur système** : Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur** : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- **Auditeur système** : Personne désignée dont le rôle est de procéder de manière régulière à l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

En plus de ces rôles de confiance au sein de l'IGC, une AC distingue en tant que rôle de confiance, les rôles de porteurs de parts de secrets d'IGC. Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés.

Toutes les personnes opérant un rôle de confiance au sein de l'IGC en seront notifiées, et accepteront ce rôle grâce à la signature d'un accord d'acceptation du rôle. Le responsable d'application procédera alors à la formation et la sensibilisation de la personne obtenant un rôle de confiance.

Les fonctions de l'IGC sont soumises à une gestion d'accès en fonction des rôles. Un système d'authentification forte est mis en place.

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

Les opérateurs d'enregistrement de l'AE(D) ont un rôle de confiance d'opérateur d'enregistrement des porteurs. Ils sont nommés et enrôlés par l'AE(D), dans le cadre d'un processus d'habilitation décrit au chapitre Qualifications, compétences et habilitations requises.

L'authentification des opérateurs de l'AE(D) au système d'information de l'AE(D) doit reposer sur une politique d'authentification définie par l'AE(D) et satisfaisant aux exigences de sécurité de l'IGC.

5.2.2. Nombre de personnes requises par tâche

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.
Pour des raisons de sécurité, il est demandé de répartir les fonctions sensibles sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC (cf. chapitre Mesures de sécurité techniques).

5.2.3. Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Néanmoins il y a une séparation obligatoire de ces rôles : responsable de sécurité et ingénieur système.

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

5.3.1. Qualifications, compétences et habilitations requises

Tout le personnel amené à travailler au sein de composantes de l'IGC est soumis à une clause de confidentialité.
Le personnel amené à travailler au sein de l'IGC, occupera un poste correspondant à ses compétences professionnelles. Le personnel occupant un rôle de confiance devra posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.
Toutes les personnes intervenant dans des rôles de confiance de l'IGC sont informées :

- de leurs responsabilités relatives aux services de l'IGC ;
- des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

5.3.2. Procédures de vérification des antécédents

Youtrust s'assure de l'honnêteté de son personnel amené à travailler au sein de la composante en mettant en œuvre des moyens respectant le cadre légal et les réglementations en vigueur.
Ces personnes ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. Elles devront remettre à Youtrust une copie du bulletin n°3 de leur casier judiciaire. Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflits d'intérêts préjudiciables à l'impartialité de leurs tâches.
Ces vérifications seront menées préalablement à l'affectation à un rôle de confiance.

5.3.3. Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

5.3.4. Exigences et fréquence en matière de formation continue

Le personnel concerné sera informé et disposera d'une formation adéquate préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6. Sanctions en cas d'actions non autorisées

Les sanctions et procédures disciplinaires associées sont définies dans des documents opposables communiqués aux personnels concernés.

5.3.7. Exigences vis-à-vis des prestataires externes

Le personnel des prestataires externes intervenant sur une composante de l'AC doit également respecter les exigences du présent chapitre Mesures de sécurité vis-à-vis du personnel. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

Lors de la sélection d'un prestataire externe, l'AC s'assure que le prestataire choisi répond aux besoins en conformité et en sécurité décrits dans la présente PC, au travers d'un processus de sélection de fournisseur documenté.

5.3.8. Documentation fournie au personnel

Le personnel dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, il doit lui être remis la ou les politique(s) de sécurité l'impactant.

5.4. Procédure de constitution des données d'audit

5.4.1. Type d'évènements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre de l'IGC, celle-ci journalise les événements tels que décrits ci-dessous, sous forme électronique. La journalisation est automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements sont recueillis, par des moyens électroniques et/ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les actions de maintenance et de changements de la configuration des systèmes, qui sont journalisées dans un document électronique et/ou papier signé et horodaté ;
- les changements apportés au personnel, qui sont journalisés dans un document électronique et/ou papier signé et horodaté;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...), qui sont journalisées dans un document électronique et/ou papier signé et horodaté.

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment :

- enregistrement d'un futur porteur ;
- réception d'une demande de certificat (initiale et renouvellement) ;
- validation / rejet d'une demande de certificat ;
- événements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- génération des certificats des porteurs;
- publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- réception d'une demande de révocation ;
- validation / rejet d'une demande de révocation ;
- génération puis publication des LCR.

Chaque enregistrement d'un événement dans un journal doit contenir au minimum les champs suivants :

- type de l'événement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'événement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) ;
- résultat de l'événement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements.
De plus, en fonction du type de l'événement, chaque enregistrement devra également contenir les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'événement ;
- toute information caractérisant l'événement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'événement.

5.4.2. Fréquence de traitement des journaux d'évènements

Cf. chapitre Procédure de constitution des données d'audit ci-dessous.

5.4.3. Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins un (1) mois. Ils sont également archivés simultanément pour une période indiquée dans le chapitre Période de conservation des archives.

5.4.4. Protection des journaux d'évènements

Sur site, les journaux d'évènements ne sont rendus accessibles qu'au personnel de confiance. De plus, ceux-ci ne sont accessibles qu'en lecture. Afin de garantir l'intégrité des journaux, ceux-ci seront signés électroniquement quotidiennement. L'archivage se fait dans un système d'archivage à vocation probatoire.

5.4.5. Procédure de sauvegarde des journaux d'évènements

L'ensemble des journaux d'événements sont sauvegardés quotidiennement.

5.4.6. Système de collecte des journaux d'évènements

La collecte des journaux d'événements se fait au travers d'un système d'archivage à vocation probatoire.

5.4.7. Notification de l'enregistrement d'un évènement au responsable de l'événement

Aucune notification n'est délivrée suite à l'enregistrement d'un événement.

5.4.8. Évaluation des vulnérabilités

Youtrust procède ou fait procéder à une analyse des vulnérabilités. Pour ce faire, plusieurs éléments sont analysés :

- une analyse des accès physiques, afin de détecter toute intrusion non autorisée ;
- une analyse complète des journaux d'événements en vue d'une détection en échec d'événement ou d'opération est réalisée en continue. Le personnel disposant d'un rôle de confiance est notifié par mail lorsqu'une anomalie est détectée ;
- une analyse automatique via un outil de gestion des vulnérabilités. Un scan hebdomadaire est effectué et un rapport envoyé au personnel disposant d'un rôle de confiance.

5.5. Archivage des données

5.5.1. Types de données à archiver

Des dispositions en matière d'archivage sont mises en place par l'ACP. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.
Les données à archiver sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les certificats, LAR et LCR tels qu'émis ou publiés ;
- les engagements signés par le responsable du Comité de Direction Technique ;
- les journaux d'évènements des différentes entités de l'IGC, incluant en particulier les événements relatifs au cycle de vie des certificats et des clés pour les porteurs et les AC ;
- les dossiers d'enregistrements ;
- les dossiers de preuve de vérification d'identité ;
- les attestations de vérification d'identité ;
- la trace d'acceptation du certificat par le porteur.

5.5.2. Période de conservation des archives

Dossiers d'enregistrement

Tout dossier d'enregistrement accepté sera archivé pour les besoins de fourniture de la preuve de la certification dans des procédures légales.

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.19.1.0]
[1.2.250.1.302.1.20.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]

Les dossiers d'enregistrement sont conservés pour une durée de 10 ans.

La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du porteur.
Au cours de cette durée d'opposabilité des documents, le dossier d'enregistrement doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.
Ce dossier doit permettre de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]

Dans le cas où des documents sont conservés au format papier, des mesures de sécurité physique spécifiques doivent être mises en place (dégradation, incendie, accès, vol et perte).

Certificats, LAR et LCR émis par l'AC

Les certificats de porteur et d'AC, ainsi que les LCR / LAR produites, doivent être archivés pendant au moins 5 années après leur expiration.

Journaux d'événements

Les journaux d'événements traités au chapitre Procédure de constitution des données d'audit seront archivés pendant 17 ans après leur génération. L'archivage se fera dans un milieu sécurisé, permettant de garantir l'intégrité des données au cours du temps.

5.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, seront :

- protégées en intégrité ;
- accessibles seulement aux personnes autorisées ;
- pourront être relues et exploitées pendant toute la durée de l'archivage.

Dans le cadre d'un transfert ou d'une cessation d'activité, l'ensemble des archives peuvent être confiées à un tiers chargé d'en assurer, pour la durée initialement prévue, la disponibilité et la protection dans les termes décrits dans ce paragraphe.

5.5.4. Procédure de sauvegarde des archives

L'archivage est réalisé soit de manière automatique, soit de manière manuelle par du personnel autorisé. L'archivage est réalisé hors site dans un environnement sécurisé d'archivage à vocation probatoire. Des sauvegardes des archives sont réalisées quotidiennement sur des sites distants.

5.5.5. Exigences d'horodatage des données

Chaque événement contient la date et l'heure précise de réalisation. Les archives quotidiennes sont horodatées via un procédé cryptographique.

5.5.6. Système de collecte des archives

Les systèmes de collecte des archives de Youtrust sont internes.

5.5.7. Procédures de récupération et de vérification des archives

Les archives peuvent être récupérées dans un délai maximum de 2 jours ouvrés. Seules les personnes occupant un rôle de confiance peuvent réaliser les opérations de récupération et de vérification des archives.

5.6. Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela, la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.
Au regard de la date de fin de validité de ce certificat, son renouvellement sera demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.
Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée sera utilisée pour signer des certificats.
Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7. Reprise suite à la compromission et sinistre

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

L'IGC Youtrust a mis en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.
Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la

compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de l'IGC. Le responsable du Comité de Direction Technique doit en être informé immédiatement. Il devra alors traiter l'anomalie. S'il estime que l'incident a un niveau de gravité important, il demandera une révocation immédiate du certificat. Si celle-ci a lieu, il publiera l'information de révocation du certificat dans la plus grande urgence, voire immédiatement. Il le fera via le site public de Youtrust, via une notification par courrier électronique à l'ensemble des clients.
Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors le responsable du Comité de Direction Technique publiera l'information via le site public et notifiera par courrier électronique l'ensemble des clients de Youtrust. Tous les certificats concernés seront alors révoqués.

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

L'hébergeur de Youtrust dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC, des engagements de l'AC dans sa propre PC notamment en ce qui concerne les fonctions liées à la publication et / ou la révocation des certificats.
Youtrust dispose d'une procédure permettant de réinitialiser l'environnement logiciel.
Ce plan sera testé au minimum une fois tous les 2 ans.

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

La compromission d'une clé d'infrastructure ou de contrôle d'une composante est traitée dans le plan de continuité de la composante (cf. chapitre Reprise suite à la compromission et sinistre) en tant que sinistre.
Dans le cas de compromission d'une clé d'AC, le certificat correspondant sera immédiatement révoqué : cf. chapitre Révocation et suspension des certificats.
En outre, l'AC respecte les engagements suivants :

- indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

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

L'IGC Youtrust dispose des moyens nécessaires permettant d'assurer la continuité des activités en conformité avec les exigences de la présente PC et de la PC de l'AC (cf. chapitre Reprise suite à la compromission et sinistre).

5.8. Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.
L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.
Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.
La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

5.8.1. Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC :

- met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats de porteurs et des informations relatives aux certificats) ;
- assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LAR et LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC. À défaut, les applications de l'Administration refuseront les certificats émis par des AC dont

les LCR en cours de validité ne seraient plus accessibles, même si le certificat de porteur est encore valide ;

- dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire.

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

En cas de fin de vie d'une AED, celle-ci :

- informe l'AC avec un préavis de six (6) mois minimum ;
- supprime les habilitations de tous les opérateurs AED à la date d'arrêt d'activité ;
- arrête l'enregistrement de nouveaux porteurs auprès de l'AC ;
- rappelle aux opérateurs AED la nécessité de poursuivre l'archivage des dossiers de preuves d'identité sur la durée initialement prévue.

Youtrust supprime les habilitations des serveurs et de l'AED à la date d'arrêt d'activité.

5.8.2. Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité sera progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LAR / LCR conformément aux engagements pris dans sa PC.

L'AC prend les dispositions suivantes en cas de cessation de service :

- la notification des entités affectées ;
- le transfert de ses obligations à d'autres parties ;
- la gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC prendra les dispositions suivantes :

- s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;

- prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- révoquer son certificat ;
- révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- informer (par exemple par récépissé) tous les porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant ;
- mettre fin aux contrats en vigueur avec les prestataires et les sous-traitants participant aux processus de gestion des certificats, ou supprimer leurs habilitations devenues obsolètes après la fin de vie de l'AC.

6. Mesures de sécurité techniques

6.1. Génération des bi-clés

6.1.1. Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (cf. chapitre Mesures de sécurité non techniques). Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre Annexes sur les exigences de sécurité du module cryptographique de l'AC ci-dessous pour le niveau de sécurité considéré.
La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre Mesures de sécurité procédurales), dans le cadre de « cérémonies de clés ». Ces cérémonies se déroulent suivant la procédure préalablement définie et validée par le responsable du Comité de Direction Technique.
L'initialisation de l'IGC et/ou la génération des clés de signature d'AC s'accompagne de la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.
Suite à leur génération, les parts de secrets sont remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Elles sont stockées sur une carte à puce. Un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur.

La cérémonie des clés est réalisée par deux personnes internes à Youtrust occupant des rôles de confiance. De plus, un témoin valide la bonne mise en œuvre de la cérémonie.

6.1.2. Clés des porteurs

La génération des clés des porteurs doit être effectuée dans un environnement sécurisé (cf. chapitre Mesures de sécurité non techniques).
Les bi-clés des porteurs doivent être générées directement dans le dispositif de création de signature. Ce dispositif est un module cryptographique conforme aux exigences du chapitre Annexes.

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
Youtrust met en œuvre des moyens techniques et organisationnels afin d'assurer que la clé privée ne sera utilisée que par le porteur. En aucun cas Youtrust ne pourra utiliser cette clé pour son propre usage ou pour le compte d'une autre personne que le porteur.

[1.2.250.1.302.1.19.1.0]
[1.2.250.1.302.1.20.1.0]
Les clés privées des unités d'horodatage et du service OCSP sont générés par leur responsable d'application respectif, à l'intérieur du matériel cryptographique de l'infrastructure IGC.

6.2. Transmission de la clé privée à son propriétaire

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
La clé privée n'est pas transmise au porteur.

[1.2.250.1.302.1.19.1.0]
[1.2.250.1.302.1.20.1.0]
Sans objet, la bi-clé est générée par le propriétaire.

6.3. Transmission de la clé publique à l'AC

La clé publique du porteur est transmise techniquement à l'AC suite au processus de génération de la bi-clé, dans le module cryptographique. Cela est fait à travers un message au format PKCS#10 signé par la clé privée de serveur.

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

La clé publique des AC est enveloppée dans un certificat signé par l'AC racine. Sa diffusion s'accompagne de l'empreinte numérique du certificat ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC.
La clé publique de l'AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) pourront aisément être récupérées par les utilisateurs de certificats, via l'interface publique (cf. chapitre Entités chargées de la mise à disposition des informations).

6.5. Tailles des clés

Les clés d'AC auront ces caractéristiques :

- Algorithme utilisé : RSA.
- Taille minimale des clés : 4096 bits.

Les clés des certificats de signature devront avoir ces caractéristiques :

- Algorithme utilisé : RSA.
- Taille minimale des clés :
  - 2048 bits avant le 4 avr. 2024
  - 3072 bits à compter du 4 avr. 2024.

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

L'équipement de génération des bi-clés de l'AC et des porteurs est un module cryptographique garantissant la robustesse des clés générées.
Les bi-clés ne peuvent être générées que sur un module conforme à cette exigence, ou d'un niveau cryptographique et sécuritaire supérieur.

6.7. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR (cf. chapitre Usage des certificats).
L'utilisation d'une clé privée du porteur et du certificat associé est strictement au service de signature (cf. chapitre Usage des certificats).

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

6.8.1. Standards et mesures de sécurité pour les modules cryptographiques

Les modules cryptographiques, utilisés par l'AC et les serveurs, pour la génération et la mise en œuvre de leurs clés de signature, sont des modules cryptographiques répondant aux exigences du chapitre Annexes sur les exigences de sécurité du module cryptographique de l'AC ci-dessous. Youtrust utilise des HSM certifiés et s'assure de leur sécurité, physique et logicielle. Youtrust héberge ce matériel dans des zones d'accès contrôlées et protégées contre les pannes électriques, les inondations ainsi que les incendies.
Youtrust s'assure de la sécurité des HSM lors de leur mise en place, lors de la cérémonie des clés, lors de leur utilisation, et ce jusqu'à leur fin de vie.

6.8.2. Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature des AC est assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets. Il y a 2 porteurs de secrets pour chaque AC, qui se voient remettre ces secrets sur carte à puce lors de la cérémonie des clés. Nous utilisons une méthode N-M.

Le contrôle de la clé privée d'un porteur est sous son contrôle exclusif.

6.8.3. Séquestre de la clé privée

Les clés privées d'AC et des certificats de porteurs ne sont pas séquestrées.

6.8.4. Copie de la clé privée

Les clés privées d'AC font l'objet de copies de secours.

[1.2.250.1.302.1.19.1.0]
[1.2.250.1.302.1.20.1.0]
Les clés privées des services applicatifs font l'objet de copies de secours.

Lorsqu'une clé privée fait l'objet d'une copie, la copie est soit stockée dans un module cryptographique conforme aux exigences de la section « Annexes sur les exigences de sécurité du module cryptographique de l'AC », soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement utilisé offre alors un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuie sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées ne soient à aucun moment en clair en dehors du module cryptographique. Le contrôle des opérations de chiffrement / déchiffrement doit être conforme aux exigences de la section « Contrôle de la clé privée par plusieurs personnes ».
Lorsque la copie de secours est réalisée hors module cryptographique, les clés privées sont encapsulées (wrap) à l'intérieur du module cryptographique avant toute exportation, au moyen d'un algorithme et d'une longueur de clé offrant un niveau de sécurité équivalent ou supérieur à celui de la clé protégée. L'opération de déchiffrement (unwrap) ne peut être effectuée qu'au sein d'un module cryptographique de qualification équivalente. Les modalités opérationnelles de ces opérations sont décrites dans la procédure interne applicable.

6.8.5. Archivage de la clé privée

Les clés privées ne sont jamais archivées.

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

Le transfert vers / depuis le module cryptographique ne se fait que sous forme chiffrée, conformément aux exigences du chapitre Copie de la clé privée.

6.8.7. Stockage de la clé privée dans un module cryptographique

Le stockage des clés privées est réalisé dans un module cryptographique répondant aux exigences du chapitre Annexes ci-dessous pour le niveau de sécurité considéré.
Cependant, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences du chapitre Copie de secours de la clé privée.
Youtrust met les moyens en place afin de garantir que les clés privées ne sont pas compromises pendant leur stockage ou leur transport.

Dans le cadre du service de signature à distance, les bi-clés des porteurs sont pré-générées dans le module cryptographique. La clé privée est immédiatement encapsulée au sein du module cryptographique et n'en sort que sous forme chiffrée. Ce mécanisme d'encapsulation offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique. La clé privée n'est déchiffrée qu'à l'intérieur du module cryptographique, le temps de la transaction de signature, puis immédiatement détruite. La remise de la bi-clé au porteur s'effectue par l'émission d'un certificat liant son identité à la clé publique correspondante. Aucun matériel cryptographique privé n'est transmis au porteur.

6.8.8. Méthode d'activation de la clé privée

L'activation des clés privées d'AC se fera dans un module cryptographique et sera contrôlée via des données d'activation tel que décrit dans la section « Données d'activation ». Pour l'AC, les porteurs de secrets devront être présents afin de réaliser l'activation.

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

L'activation de la clé privée du porteur est liée au processus de signature réalisé par le porteur.

L'identification et l'authentification du porteur réussies permettent la génération de la clé privée correspondante et son activation est immédiate.

[1.2.250.1.302.1.19.1.0]

[1.2.250.1.302.1.20.1.0]

L'activation des clés privées des unités d'horodatage ou des serveurs OCSP se fera dans un module cryptographique et sera contrôlée via des données d'activation (cf. section Données d'activation).

6.8.9. Méthode de désactivation de la clé privée

La désactivation des clés privées dans le module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

La désactivation des clés privées des certificats de porteurs est automatique en fin de création de signature et correspond techniquement à la destruction de la clé privée dans le module cryptographique.

Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans la section « Annexes sur les exigences de sécurité du module cryptographique de l'AC » pour le niveau de sécurité considéré.

6.8.10. Méthode de destruction des clés privées

En fin de vie d'une clé privée d'AC ou de porteurs, normale ou anticipée (révocation), cette clé sera systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

[1.2.250.1.302.1.17.1.0]

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

Les clés privées des porteurs sont automatiquement détruites à la fin du processus de signature. Une fois détruites, les clés privées ne sont de fait plus utilisables.

[1.2.250.1.302.1.19.1.0]
[1.2.250.1.302.1.20.1.0]
La destruction des clés privées en fin de vie est de la responsabilité du responsable de l'application concernée. Il se coordonne avec le Comité de Direction Technique et les porteurs de secrets afin de garantir l'intégrité des matériels cryptographiques.

6.8.11. Niveau de qualification du module cryptographique et des dispositifs de création de signature

Cf. Exigences sur la certification.

6.9. Autres aspects de la gestion des bi-clés

6.9.1. Archivage des clés publiques

Les clés publiques des AC sont archivées pendant 5 ans après l'expiration des certificats correspondants.

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

Les bi-clés et les certificats des AC doivent avoir une durée de vie au maximum de 10 ans. La fin de validité d'un certificat d'AC doit être postérieure à la fin de vie des certificats de porteurs qu'elle émet.

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
Les certificats des porteurs ont une durée de validité de 15 minutes. Les clés privées correspondantes ont une durée de vie équivalente à la durée du processus de signature.

[1.2.250.1.302.1.19.1.0]

Les certificats ont une durée de validité de 3 ans.

[1.2.250.1.302.1.20.1.0]
Les certificats OCSP ont une durée de validité de 5 ans.

6.10. Données d'activation

6.10.1. Génération et installation des données d'activation

6.10.1.1. Clés de l'AC

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se fait lors de la phase d'initialisation et de personnalisation de ce module. Les données d'activation sont stockées sur des cartes à puce. Ces cartes sont fournies aux porteurs de secrets qui doivent les stocker de manière sécurisée, en les protégeant contre le vol, la détérioration, et l'utilisation non autorisée.

6.10.1.2. Clés des certificats de porteurs

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
Les données d'activation du porteur sont générées par :

- le magic link lui permettant d'accéder au processus de signature ;
- le code d'authentification saisi préalablement à l'opération de signature.

[1.2.250.1.302.1.19.1.0]
[1.2.250.1.302.1.20.1.0]

Comme pour l'AC, les données d'activation sont stockées sur des cartes à puce et sous la responsabilité de porteurs de secrets.

6.10.2. Protection des données d'activation

6.10.2.1. Clés de l'AC

Le porteur de secret a la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des données d'activation des clés d'AC.

6.10.2.2. Clés des certificats de porteurs

[1.2.250.1.302.1.17.1.0]
[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
Les éléments d'activation sont propres aux porteurs et ne sont valables que pour un processus de signature précis.

[1.2.250.1.302.1.19.1.0]
[1.2.250.1.302.1.20.1.0]
La protection des données d'activation est de la responsabilité des porteurs de secret.

6.10.3. Autres aspects liés aux données d'activation

Sans objet.

6.11. Mesures de sécurité des systèmes informatiques

6.11.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

L'IGC met en place une série de mesures et de moyens permettant de garantir un haut niveau de sécurité :

- authentification forte des utilisateurs du système avec une gestion des rôles par utilisateur;
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- mise en place d'antivirus et d'antimalware ;
- protection du réseau.

6.11.2. Niveau de qualification des systèmes informatiques

Sans objet.

6.12. Mesures de sécurité liées au développement des systèmes

6.12.1. Mesures liées à la gestion de la sécurité

Tous les développements impactants l'IGC sont documentés et réalisés via un processus de manière à en assurer la qualité.
La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau sont documentées et contrôlées.
De plus, un cloisonnement entre les environnements de développement, de test, de pré-production et de production est opéré pour assurer une mise en production de qualité.

6.12.2. Niveau d'évaluation sécurité du cycle de vie des systèmes

Toute évolution significative d'un système d'une composante de l'IGC doit être testée et validée avant déploiement. Ces opérations sont réalisées par du personnel de confiance.

6.13. Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles et ports nécessaires au fonctionnement de chaque composante au sein de l'IGC.
Les communications avec des entités externes sont protégées par une authentification mutuelle préalable.
Les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont auditées régulièrement en vue de vérifier leur conformité.

6.14. Horodatage

L'ensemble des éléments archivés sont horodatés.

7. Profil des certificats et des LCR

7.1. Profils de certificats

Les certificats respectent le format décrit par la [RFC5280].

7.1.1. Certificats de l'ACP

Champs de base	Valeur
Version	2
Numéro de série	*Défini par l'outil*
Signature	SHA256WithRSA
Emetteur	CN=YOUSIGN SAS - ROOT2 CA, OU=794513986, O=YOUSIGN SAS, L=CAEN, ST=CALVADOS, C=FR
Validité	*20 ans*
Subject	CN=YOUSIGN SAS - ROOT2 CA, OU=794513986, O=YOUSIGN SAS, L=CAEN, ST=CALVADOS, C=FR
Longueur des clefs de l'AC	*4096 bits*

Champs d'extension	Obligatoire	Critique	Valeur
Authority Key Identifier	Oui	Non	Hash sha1 de la clé publique du certificat

Subject Key Identifier	Oui	Non	Hash sha1 de la clé publique du certificat
Key Usage	Oui	Oui	`Key_CertSign, Crl_Sign`
CRL Distribution Points	Oui	Non	http://crl.yousign.fr/yousignsasroot2ca.crl http://crl2.yousign.fr/yousignsasroot2ca.crl http://crl3.yousign.fr/yousignsasroot2ca.crl
Basic Constraints	Oui	Oui	`CA:true`

7.1.2. Certificats de l'AC « YOUSIGN SAS - SIGN3 CA »

Champs de base	**Valeur**
Version	*2*
Numéro de série	*Défini par l'outil*
Signature	`SHA256WithRSA`

Issuer	`CN=YOUSIGN SAS - ROOT2 CA,`
	`OU=794513986,`
	`O=YOUSIGN SAS,`
	`L=CAEN,`
	`ST=CALVADOS,`
	`C=FR`

Validity	*10 ans*

Subject	`CN=YOUSIGN SAS - SIGN3 CA,`
	`OU=794513986,`
	`O=YOUSIGN SAS,`
	`L=CAEN,`
	`ST=CALVADOS,`
	`C=FR`

Longueur des clefs de l'AC	*4096 bits*

Champs d'extension	**Obligatoire**	**Critique**	**Valeur**

Authority Key Identifier	Oui	Non	Hash SHA-1 de la clé publique de l'ACP
Subject Key Identifier	Oui	Non	Hash SHA-1 de la clé publique de l'AC
Key Usage	Oui	Oui	`Key_CertSign`, `Crl_Sign`
CRL Distribution Points	Oui	Non	http://crl.yousign.fr/crl/yousignsasroot2ca.crl http://crl2.yousign.fr/crl/yousignsasroot2ca.crl http://crl3.yousign.fr/crl/yousignsasroot2ca.crl
Basic Constraints	Oui	Oui	`CA:true`

7.1.3. Certificats de personnes physiques

[1.2.250.1.302.1.17.1.0]

Champs de base	**Valeur**
Version	2
Numéro de série	Défini par l'outil et comprenant une part aléatoire
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS - SIGN3 CA, OU=794513986, O=YOUSIGN SAS, L=CAEN, ST=CALVADOS, C=FR
Validity	15 minutes
Subject	Se reporter au à la section types de noms
Longueur des clefs	2048 bits avant le Apr 4, 2024 3072 bits après le Apr 4, 2024

Champs d'extension	**Obligatoire (O/N)**	**Critique (O/N)**	**Valeur**
Authority Key Identifier	O	N	Hash SHA-1 de la clé publique de l'ACI SIGN3

Subject Key Identifier	O	N	Hash SHA-1 de la clé publique du certificat
Key Usage	O	O	Non Repudiation
Extended Key Usage	O	N	MS Document Signing Adobe PDF Signing
Certificate Policies	O	N	1.2.250.1.302.1.17.1.0 http://yousign.fr/fr/public/document
CRL Distribution Points	O	N	http://crl.yousign.fr/crl/yousignsassign3ca.crl http://crl2.yousign.fr/crl/yousignsassign3ca.crl http://crl3.yousign.fr/crl/yousignsassign3ca.crl
Basic Constraints	O	O	CA:false
Authority Information Access	O	N	Certificat autorité : http://crl.yousign.fr/yousignsassign3ca.crt http://crl2.yousign.fr/yousignsassign3ca.crt http://crl3.yousign.fr/yousignsassign3ca.crt Répondeur OCSP : http://ocsp.yousign.fr

[1.2.250.1.302.1.22.1.0]

[1.2.250.1.302.1.23.1.0]

Champs de base	**Valeur**
Version	2
Numéro de série	Défini par l'outil et comprenant une part aléatoire
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS - SIGN3 CA, OU=794513986, O=YOUSIGN SAS, L=CAEN, ST=CALVADOS, C=FR
Validity	15 minutes
Subject	Se reporter au à la section types de noms
Longueur des clefs	3072 bits

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	Hash SHA-1 de la clé publique de l'ACI SIGN3
Subject Key Identifier	O	N	Hash SHA-1 de la clé publique du certificat
Key Usage	O	O	Non Repudiation
Extended Key Usage	O	N	MS Document Signing Adobe PDF Signing
Certificate Policies	O	N	1.2.250.1.302.1.22.1.0 ou 1.2.250.1.302.1.23.1.0 http://yousign.fr/fr/public/document
CRL Distribution Points	O	N	http://crl.yousign.fr/crl/yousignsassign3ca.crl http://crl2.yousign.fr/crl/yousignsassign3ca.crl http://crl3.yousign.fr/crl/yousignsassign3ca.crl
Basic Constraints	O	O	CA:false
Authority Information Access	O	N	Certificat autorité : http://crl.yousign.fr/yousignsassign3ca.crt http://crl2.yousign.fr/yousignsassign3ca.crt http://crl3.yousign.fr/yousignsassign3ca.crt Répondeur OCSP : http://ocsp.yousign.fr
ext-etsi-valassured-ST-certs	O	N	0.4.0.194121.2.1

7.1.4. Certificats des Unités d'Horodatage

[1.2.250.1.302.1.19.1.0]

Champs de base	Valeur
Version	2
Numéro de série	Défini par l'outil et comprenant une part aléatoire

Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS - SIGN3 CA, OU=794513986, O=YOUSIGN SAS, L=CAEN, ST=CALVADOS, C=FR
Validity	3 ans
Subject	Se reporter à la section types de noms
Longueur des clefs	2048 bits avant le 28 août 2024 3072 bits à compter du 28 août 2024

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	Hash SHA-1 de la clé publique de l'ACI SIGN3
Subject Key Identifier	O	N	Hash SHA-1 de la clé publique du certificat
Key Usage	O	O	Digital Signature
Extended Key Usage	O	O	id-kp-timeStamping
Certificate Policies	O	N	1.2.250.1.302.1.19.1.0 http://yousign.fr/fr/public/document
CRL Distribution Points	O	N	http://crl.yousign.fr/yousignsassign3ca.crl http://crl2.yousign.fr/yousignsassign3ca.crl http://crl3.yousign.fr/yousignsassign3ca.crl
Basic Constraints	O	O	CA:false
Authority Information Access	O	N	Certificat autorité : http://crl.yousign.fr/yousignsassign3ca.crt http://crl2.yousign.fr/yousignsassign3ca.crt http://crl3.yousign.fr/yousignsassign3ca.crt Répondeur OCSP : http://ocsp.yousign.fr

Remarque : les certificats d'unité d'horodatage sont émis selon le niveau NCP+ de la norme ETSI 319 411-1. Ces certificats ne sont pas qualifiés au sens eIDAS, ce qui reste compatible avec la qualification eIDAS du service d'horodatage.

7.1.5. Certificats du service OCSP

[1.2.250.1.302.1.20.1.0]

Champs de base	Valeur
Version	2
Numéro de série	Défini par l'outil et comprenant une part aléatoire
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS - SIGN3 CA, OU=794513986, O=YOUSIGN SAS, L=CAEN, ST=CALVADOS, C=FR
Validity	5 ans
Subject	Se reporter à la section types de noms
Longueur des clefs	2048 bits avant le 30 oct. 2024 3072 bits à compter du 30 oct. 2024

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	Hash SHA-1 de la clé publique de l'ACI SIGN3
Subject Key Identifier	O	N	Hash SHA-1 de la clé publique du certificat
Key Usage	O	O	Digital Signature
Extended Key Usage	O	N	id-kp-OCSPSigning
Certificate Policies	O	N	1.2.250.1.302.1.20.1.0 http://yousign.fr/fr/public/document
id-ocsp-nocheck	O	N	NULL
Basic Constraints	O	O	CA:false

CRL Distribution Points	O	N	http://crl.yousign.fr/yousignsassign3ca.crl http://crl2.yousign.fr/yousignsassign3ca.crl http://crl3.yousign.fr/yousignsassign3ca.crl
Authority Information Access	O	N	Certificat autorité : http://crl.yousign.fr/yousignsassign3ca.crt http://crl2.yousign.fr/yousignsassign3ca.crt http://crl3.yousign.fr/yousignsassign3ca.crt

7.2. Liste de Certificats Révoqués

Les listes de certificats révoqués respectent le format décrit par la [RFC5280].

Champs de base	**Valeur**
Version	1
Signature	SHA256WithRSA
Emetteur	CN=YOUSIGN SAS - SIGN3 CA, OU=794513986, O=YOUSIGN SAS, L=Caen, ST=Calvados, C=FR
Validité	*7 jours*
Prochaine mise à jour	*Date de la CRL + 1 jour*
Liste des certificats révoqués	*Pour chaque certificat :* *Numéro de série, date de la révocation*

Champs d'extension	**Obligatoire**	**Critique**	**Valeur**

Authority Key Identifier	Oui	Non	Hash SHA-1 de la clé publique de l'AC
CRL Number	Oui	Non	Défini par l'outil

7.3. Jetons OCSP

7.3.1. Requêtes OCSP

Les requêtes OCSP acceptées sont celles qui respectent le format décrit par la [RFC6960].

Le service OCSP ignore la signature si elle est présente.

Les requêtes attendues sont de la forme :

Champ	Commentaires	Valeur attendue
version	Version de la requête	0 (version 1)
requestorName	Nom de l'émetteur de la requête	Valeur absente ou ignorée
requestList **- reqCert** **-** **singleRequestExtensions**	Liste des certificats à vérifier	Un ou plusieurs identifiants de certificats sont acceptés. La valeur des extensions est ignorée
requestExtensions	Extensions	Seule l'extension Nonce est prise en compte, les autres sont ignorées

Les algorithmes d'empreinte acceptés pour les identifiants de certificats sont SHA-1, SHA-256, SHA-384 et SHA-512.

7.3.2. Réponses OCSP

Les réponses OCSP respectent le format décrit par la [RFC6960]. Elles sont signées par le service sauf si une erreur s'est produite (requête rejetée ou échec de traitement).

Les réponses sont de la forme BasicOCSPResponse :

Champ	Commentaires	Valeur
version	Version de la requête	0 (version 1)
responderID	Nom du répondeur	Hash de la clé publique du répondeur

producedAt	Heure de production de la réponse	Heure de production à la seconde près
responses **- certID** **- certStatus** **- revocationDate** **- thisUpdate**	Statut des certificats identifiés dans la requête	Le statut du certificat est le statut actuel du certificat (thisUpdate est la date courante). La date de révocation est fournie le cas échéant, mais pas la raison de révocation
responseExtensions	Extension Nonce	L'extension Nonce fournie par un émetteur est renvoyée dans la réponse
	Extension Archive CutOff	Date de début de validité de l'AC. Cette extension est disponible uniquement dans les réponses OCSP pour les certificats expirés

8. Audit de conformité et autres évaluations

8.1. Fréquences et ou circonstances des évaluations

Un contrôle de conformité est réalisé lors de la mise en service du système et suite à toute modification significative. De plus, un audit sera réalisé au moins tous les ans.

8.2. Identités et qualifications des évaluateurs

Les audits sont réalisés en interne par du personnel de Youtrust ou bien sous la forme d'une prestation auprès d'acteurs spécialistes de la sécurité des systèmes d'information et ayant des compétences reconnues dans le domaine de la signature électronique.
Dans le cadre d'obtention de certifications des services de l'IGC, l'audit de certification est réalisé par une société externe dûment accréditée.

8.3. Relations entre évaluateurs et entités évaluées

Les contrôleurs sont indépendants et impartiaux dans leur missions d'évaluation, qu'ils fassent partie du personnel interne ou qu'il s'agisse de prestataires externes.

8.4. Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC ou sur l'ensemble de l'architecture de l'IGC et visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).
Pour ce faire, les auditeurs formalisent un plan d'audit qui sera présenté au Comité de Direction Technique.

8.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rédige des fiches d'écarts catégorisant ceux-ci en écarts mineurs ou majeurs. D'autres catégories peuvent exister mais ne sont pas obligatoires.
En cas d'écart, l'AC présente un plan d'action corrective qui peut être validé par l'équipe d'audit. Les actions correctives sont ensuite implémentées dans un délai adapté au niveau de l'écart et à la complexité du plan d'action.
Éventuellement un contre-audit est réalisé pour confirmer la levée des écarts.

9. Autres problématiques métiers et légales

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

Sans objet.

9.1.2. Tarifs pour accéder aux certificats

Sans objet.

9.1.3. Tarifs pour accéder aux LCR et répondeur OCSP

L'accès aux LCR et au répondeur OCSP est gratuit.

9.1.4. Politique de remboursement

Sans objet.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

Youtrust certifie qu'elle est titulaire d'une police d'assurance garantissant sa responsabilité civile professionnelle. Elle s'engage à maintenir en vigueur cette police d'assurance pendant toute la durée de son activité professionnelle.

9.2.2. Autres ressources

Sans objet.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- l'ensemble des documents n'ayant pas vocation à être partagés publiquement ;
- tous les secrets de l'IGC incluant les clés privées et leurs données d'activation ;
- les journaux d'évènements des composantes de l'IGC ;
- les dossiers d'enregistrement ;
- les dossiers de preuves ;
- les causes de révocations, sauf accord explicite du porteur.

9.3.2. Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3. Responsabilités en termes de protection des informations confidentielles

Des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre Périmètre des informations confidentielles sont appliquées et tiennent compte de la législation et la réglementation en vigueur sur le territoire français.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

Youtrust et les tiers mentionnés dans la présente Politique de certification s'engagent à respecter la législation et la réglementation en vigueur en matière de protection de données à caractère personnel, et en particulier le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (dit le règlement général sur la protection des données ou RGPD).

Les rôles de Youtrust et de ces tiers, les traitements de données personnelles ainsi que les modalités d'exercice de droits des personnes concernées par les traitements de données personnelles ayant lieu dans le cadre de la présente Politique de certification sont décrits l'Accord de protection des données ainsi que dans la Politique de confidentialité de Youtrust.

9.4.2. Responsabilité en termes de protection des données à caractère personnel

Se reporter à la législation et réglementation en vigueur sur le territoire français.

9.4.3. Notification et consentement d'utilisation des données personnelles

Le porteur est informé que la délivrance de certificats électroniques suppose la mise en œuvre par Youtrust de traitements de données à caractère personnel auquel le porteur consent. Le porteur est informé que la communication de ses données est obligatoire et nécessaire pour prendre en compte sa demande. Le porteur dispose notamment d'un droit d'accès aux données le concernant auprès du DPO de Youtrust via le formulaire disponible au lien suivant https://yousign.app/privacy-requests?lang=fr.
Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne sont pas divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

[1.2.250.1.302.1.22.1.0]
[1.2.250.1.302.1.23.1.0]
Le porteur est informé que son enregistrement auprès d'une AE(D) nécessite la création d'un dossier d'enregistrement conservé par l'AE(D). Le porteur peut exercer ses droits auprès de l'AE(D).
Si une le porteur contacte directement Youtrust pour exercer l'un de ses droits, Youtrust s'engage à renvoyer le porteur vers l'AE(D) dans les plus brefs délais afin que ce dernier puisse donner suite à sa demande. Youtrust pourra assister le Responsable de traitement à donner aux demandes dans la mesure où cela est raisonnablement nécessaire, mais l'AE(D) est seul responsable des réponses à ces demandes.

9.4.4. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Se reporter à la législation et réglementation en vigueur sur le territoire français.

9.4.5. Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5. Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par Youtrust sont protégés par la législation et réglementation en vigueur. Les utilisateurs ne disposent d'aucun droit de propriété intellectuelle sur les différents éléments mis en œuvre par Youtrust pour assurer son IGC.
La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctifs, droits d'auteur est sanctionnée par le Code de la propriété intellectuelle.

9.6. Interprétations contractuelles et garanties

Youtrust et ses tiers garantissent le respect des engagements décrits dans la présente politique. Les obligations des différentes parties sont rappelées dans les CGU du service.

9.7. Limite de responsabilité

Youtrust ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme des données d'authentification, des certificats, des LCR, ainsi que de tout autre équipement ou logiciel mis à disposition.

Youtrust décline sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le porteur.

En tout état de cause, Youtrust ne saurait être redevable du paiement de dommages et intérêts, de quelque nature qu'ils soient, directs, matériels, commerciaux, financiers ou moraux, en raison de l'exécution de la présente Politique de Certification.

9.8. Indemnités

Sans objet.

9.9. Durée et fin anticipée de validité de la PC

9.9.1. Durée de validité

La PC de l'AC doit rester en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.9.2. Fin anticipée de validité

Cette PC reste en application jusqu'à la publication d'une nouvelle version.

9.9.3. Effets de la fin de validité et clauses restant applicables

Sans objet.

9.10. Amendements à la PC

9.10.1. Procédures d'amendements

Youtrust contrôlera que tout projet de modification de sa PC reste conforme aux exigences de la présente PC. En cas de changement important, Youtrust pourra faire appel à une expertise technique externe, si elle le juge nécessaire.

9.10.2. Mécanisme et période d'information sur les amendements

Lors de tout changement important de la PC impactant les porteurs ou les utilisateurs des certificats, Youtrust informera les parties impactées au travers d'un communiqué publié par voie électronique. Si besoin, une communication par courrier postal pourra être réalisée.

9.10.3. Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple,

augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.
En particulier, l'OID de la PC de l'AC doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC) intervient dans les exigences de la présente PC applicable à la famille de certificats considérée.

9.11. Dispositions concernant la résolution de conflits

En cas de litige entre les parties découlant de l'interprétation, l'application et/ou l'exécution du contrat et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée aux tribunaux compétents dans le ressort de la Cour d'appel de Paris.

9.12. Juridictions compétentes

Se rapporter au chapitre Dispositions concernant la résolution de conflits.

9.13. Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, les règlements européens eIDAS et RGPD.
Les pratiques du service de délivrance de certificats de l'AC sont non discriminatoires.
Dans la mesure du possible, l'AC respecte les standards d'accessibilité pour rendre ses services accessibles à tous les utilisateurs, y compris ceux en situation de handicap.

9.14. Dispositions diverses

9.14.1. Interprétation

Sans objet.

9.14.2. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus au sens de l'article 1218 du Code civil et de la jurisprudence des tribunaux français.

10. Annexes sur les exigences de sécurité du module cryptographique de l'AC

10.1. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR), ainsi que, pour la génération des bi-clés de porteurs, répond aux exigences de sécurité suivantes :

- garantir que la génération des bi-clés des certificats de porteurs est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des certificats de porteurs;
- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- est capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- est capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration ;
- si le module cryptographique de l'AC détecte des tentatives d'altérations physiques, celui-ci entrera dans un état sûr ;

- le module cryptographique est la propriété de Youtrust.

10.2. Exigences sur la certification

Le module cryptographique utilisé par Youtrust dispose d'une certification FIPS 140-2 level 3 et est qualifié est niveau renforcé par l'ANSSI.