yousign

Politique de certification des certificats de cachet serveur émis par l'AC YOUSIGN SAS - SIGN3 CA

v1.0.4 | Diffusion : C1 - Public

HISTORIQUE DES VERSIONS			
Version	**Objet de la modification**	**Date**	**Auteur**
1.0.4	Ajout d'un paragraphe précisant que l'entité sujette dispose de 30 jours après la vérification initiale de l'identité des personnes physiques pour obtenir son certificat (section Validation initiale de l'identité)	22 juin 2026	Fiona BOUVIER
1.0.3	Ajout de l'OID 01.2.250.1.302.1.24.1.0 pour l'émission des certificats qualifiés de cachet électronique (sections Présentation générale et Identification du document) Mise à jour de la définition de l'abonné (section Définitions) Ajout du nommage des certificats de test (section Types de noms) Mise à jour des informations non vérifiées pour le RCC (section Informations non vérifiées du RCC) Ajout des exigences complémentaires pour les services qualifiés (sections Exigences spécifiques en cas de compromission de la clé privée, Procédures de remontée et de traitement des incidents et des compromissions, Procédures de reprise en cas de compromission de la clé privée d'une composante, Vérification de la génération des paramètres des bi-clés et de leur qualité, Niveau de qualification du module cryptographique et des dispositifs de création de signature et Annexes sur les exigences de sécurité du module cryptographique de l'AC) Mise à jour de la durée de conservation des archives (sections Période de conservation des archives et Archivage des clés publiques)	15 mai 2025	Tony BELOT Tony DUFOUR

	Ajout des champs “qcStatments” pour les certificats qualifiés (section Certificats de cachet)		
1.0.2	Changement de la taille de clé de 2048 vers 3072 bits pour les certificats de cachet (sections tailles des clés et certificats de cachet)	31 oct. 2024	Etienne SELLAN
1.0.1	Précision relative aux personnes disposant d’un accès au dossier d’enregistrement, susceptibles de demander la révocation d’un certificat (section origine d'une demande de révocation) Prise en compte du cas d’une demande de révocation incomplète ou d’un demandeur non authentifié dans le délai de traitement (section délai de traitement par l'AC d'une demande de révocation)	28 juin 2024	Jean VERRONS
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)	13 juil. 2023	Tony Belot

	• 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 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

1.1. Présentation générale

La société Youtrust est un PSCE 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`

1.2. Identification du document

Le présent document correspond à la PC de l'AC « YOUSIGN SAS - SIGN3 CA » pour les services de délivrance des certificats suivants :

- OID `1.2.250.1.302.1.18.1.0` pour l'émission des certificats de cachet électronique LCP de la norme ETSI 319 411-1 pour lesquels l'enregistrement est réalisé à distance. Les certificats de cachet électronique sont exclusivement à destination de personnes morales.
- OID `1.2.250.1.302.1.24.1.0` pour l'émission des certificats qualifiés de cachet électronique QCP-l de la norme ETSI 319 411-2 pour lesquels l'enregistrement est réalisé en face à face physique ou équivalent. Les certificats qualifiés de cachet électronique sont exclusivement à destination de personnes

morales. Ces certificats sont conformes à la norme ETSI 319 411-2 au niveau QCP-l et sont qualifiés, au sens du règlement eIDAS par l'ANSSI.

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. La société Youtrust peut toutefois demander un certificat pour elle-même en suivant la procédure nominale.

1.3.2. Autorités d'enregistrement

L'AE a pour rôle de vérifier les identités, tel que décrit à la section « Validation initiale de l'identité ».

L'AE de l'AC est opérée par un service interne à Youtrust.

1.3.3. Responsables de certificats de cachets

La notion de RCC est définie à la section « Définitions ».

1.3.4. 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

La présente PC traite des bi-clés et des certificats émis à la demande d'un RCC, afin que des entités puissent sceller électroniquement des données, c'est à dire créer un cachet électronique sur ces données, dans le cadre d'échanges dématérialisés avec les catégories d'utilisateurs de certificats identifiées à la section « Entités intervenant dans l'IGC ». Un tel cachet électronique apporte une preuve de l'authenticité et de l'intégrité des données.

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 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 Adresse de messagerie : 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	-

Acronyme	Signification	Traduction
ACP	Autorité de Certification Primaire	-
AE	Autorité d'Enregistrement	-
CGU	Conditions Générales d'Utilisation	-
DCP	Déclaration des Pratiques de Certification	-
DN	Distinguished Name	Nom distinctif
HSM	Hardware Security Module	Module cryptographique
IGC	Infrastructure de Gestion de Clés	-
LAR	Liste des certificats d'Autorités de Certification Révoqués	-
LCR	Liste des Certificats Révoqués	-
OID	Object Identifier	Identifiant d'objet
PC	Politique de Certification	-
PSCE	Prestataire de Services de Certification Électronique	-
RCC	Responsable du Certificat de Cachet	-
RSA	Rivest Shamir Adelman	-
URL	Uniform Resource Locator	Localisateur uniforme de ressource

1.6.2. Définitions

Terme	Signification
Abonné	[1.2.250.1.302.1.18.1.0] L'abonné est une personne morale cliente de la société Youtrust. Un lien contractuel existe entre l'abonné et la société Youtrust. [1.2.250.1.302.1.24.1.0] L'abonné est la personne morale Youtrust.
Autorité d'Enregistrement	Autorité responsable de la vérification des identités.

Terme	Signification
Autorité d'Horodatage	Autorité responsable de la gestion d'un service d'horodatage.
Autorité de Certification	Au sein d'un PSCE, une AC a en charge, au nom et sous la responsabilité de ce PSCE, 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 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.
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 peut être le PSCE lui-même ou une entité externe liée au PSCE 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

Terme	Signification
	certification électronique et en conformité avec la ou les PC qu'elle s'est engagée à respecter.
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.
Entité sujette	L'entité sujette est la personne morale pour laquelle le certificat a été émis. Cette personne morale est représentée par un représentant légal, enregistré par l'AE. Le DN du certificat permet d'identifier cette entité.
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 RCC de la fonction de génération des éléments secrets du RCC.
Fonction de génération des éléments secrets du RCC	Cette fonction génère la bi-clé du RCC.
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 RCC et/ou aux utilisateurs de certificats, hors informations d'état des certificats.
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
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 cachet et réaliser des opérations cryptographiques.
Personne autorisée	Il s'agit d'une personne autre que le RCC qui est autorisée par la PC de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du RCC (demande de révocation, de renouvellement, etc.). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du RCC.
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 RCC et les utilisateurs de certificats.
Prestataire de Services de Certification Électronique	Un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des RCC et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles).
Responsable du Certificat de Cachet	Le RCC est la personne physique qui est responsable de la protection des données d'activation de la clé privée correspondant au certificat de l'entité sujette. Le RCC est par défaut un responsable légal de l'entité sujette. Il peut alternativement être une personne nommée par un représentant légal de l'entité sujette. Dans ce dernier cas, le RCC peut être hiérarchiquement

Terme	Signification
	rattaché à l'entité sujette, ou rattaché à une autre entité avec laquelle un lien contractuel ou réglementaire existe. Le RCC peut être amené à changer en cours de validité du certificat (départ du RCC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.) sans remettre en cause la validité du certificat.
Service de cachet Yousign	Le service de cachet Youtrust est une application fournie par Youtrust permettant à un abonné, après utilisation des données d'activation, d'utiliser la clé privée correspondant à la clé publique qui est dans le certificat d'une entité sujette. Le service de cachet Youtrust est le seul système autorisé sur lequel les données d'activation des clés privées peuvent être utilisées.
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 ces CGU. 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 de cachet sont conformes à la norme [X.509]. Les certificats de cachet seront identifiés par un DN conforme aux spécifications de la norme [X.501].

Nom du champ	Description	Obligatoire
CN	CommonName Raison sociale, éventuellement suffixée d'un nom libre désignant le service interne à l'entité sujette auquel le certificat est rattaché	Oui
serialNumber	serialNumber Date et heure de lancement de la génération du certificat	Oui
O	Organization Raison sociale de l'entité sujette	Oui
OI	OrganizationIdentifier Champ contenant l'identifiant de l'entité sujette structuré conformément aux exigences de la norme ETSI 319 412-1	Oui
OU	OrganisationUnit Numéro d'identification unique de l'entité sujette	Non

Nom du champ	Description	Obligatoire
C	`Country` Pays du siège social de l'entité sujette	Oui

Les certificats de test émis par l'AC `YOUSIGN SAS - SIGN3 CA` sont identifiables par la mention du mot « TEST » dans la valeur de l'attribut CN.

3.1.2. Nécessité d'utilisation de noms explicites

Le DN choisi pour désigner les services de création de cachet dans les certificats doit être explicite. L'identification de l'entité sujette à laquelle ce service est rattaché est obligatoire.

3.1.3. Pseudonymisation des services de création de cachet

Sans objet.

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 RCC les informations et documents démontrant la légitimité de son CN. A défaut, le RCC 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

La création d'un certificat pour une entité sujette nécessite les identifications suivantes par l'AE :

- identification de l'entité sujette (personne morale) ;
- identification du représentant légal (personne physique) de l'entité sujette ;
- identification du RCC (personne physique), si celui-ci est différent du représentant légal ;
- identification de l'entité du RCC (personne morale), si celle-ci est différente de l'entité sujette.

À l'issue de la vérification initiale de l'identité d'une personne physique, l'entité sujette 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.

3.2.1. Méthode pour prouver la possession de la clé privée

La clé privée est entièrement gérée, stockée et protégée par Youtrust. Youtrust met en œuvre des moyens techniques et organisationnels afin d'assurer que la clé privée ne soit logiquement associée qu'à l'entité du RCC et ne puisse être utilisée que par cette entité. Celle-ci devra s'authentifier à l'aide d'une clé d'API sur un canal HTTPs auprès des services de Youtrust. L'accès à la clé d'API est réservé au propriétaire et aux administrateurs déclarés sur les services de Youtrust.

En aucun cas Youtrust pourra utiliser cette clé pour son propre usage.

3.2.2. Validation de l'identité d'un organisme

Cf. section « Validation de l'identité d'individu ».

3.2.3. Validation de l'identité d'un individu

3.2.3.1. Enregistrement d'un RCC pour un certificat de cachet à émettre

Le RCC doit faire une demande formelle envoyée auprès de l'AE. Le dossier d'enregistrement doit contenir l'ensemble des éléments listés ci-dessous :

- une demande de certificat, datée de moins de 3 mois, signée par le RCC et comportant le nom du service de création de cachet concerné par cette demande ;
- tout document, vérifiable et daté de moins de 3 mois, attestant de l'existence de l'entité sujette et comportant son numéro d'identification unique ;
- tout document, daté de moins de 3 mois, attestant de la qualité du représentant légal de l'entité sujette ;
- un document officiel d'identité en cours de validité d'un représentant légal de l'entité sujette ;
- dans le cas où le RCC n'est pas un représentant légal de l'entité sujette :
    - un mandat, daté de moins de 3 mois, désignant le RCC comme étant habilité à être RCC pour le service de création de cachet pour lequel le certificat de cachet doit être délivré. Ce mandat doit être signé par un représentant légal de l'entité sujette et co-signé, pour acceptation, par le RCC ;
    - un document officiel d'identité en cours de validité du RCC ;
- dans le cas où le RCC n'appartient pas hiérarchiquement à l'entité sujette, tout document, vérifiable et daté de moins de 3 mois, attestant de l'existence de l'entité du RCC et comportant son numéro d'identification unique ;
- les CGU signées électroniquement par l'ensemble des parties.

Le formulaire de demande de certificat comporte :

- les informations d'identification de l'entité du RCC si celle-ci est différente de l'entité sujette ;
- les informations d'identification du représentant légal de l'entité sujette, ainsi que du RCC si celui-ci n'est pas confondu avec le représentant légal de l'entité sujette ;

- les points de contact ultérieurs qui pourraient être utiles à l'AC afin de planifier, réaliser et valider les opérations de renouvellement et de révocation des certificats de cachet ;
- les références au certificat de cachet concerné par la demande et les informations devant figurer dans ce certificat ;
- les références à l'organisation sur le produit Youtrust pour laquelle le certificat de cachet doit être autorisé ;
- l'information, l'acceptation et l'engagement explicites de chacune des parties quant à leurs obligations respectives.

L'AE effectue les opérations suivantes :

- vérification de la complétude du formulaire ;
- vérification de la signature électronique du formulaire par le représentant légal de l'entité sujette et le cas échéant par le RCC ;
- vérification de la recevabilité et de la cohérence des pièces justificatives produites ;
- vérification de la cohérence des informations portées dans le formulaire avec les pièces justificatives ;
- vérification de la signature électronique des CGU par l'ensemble des parties.

3.2.3.2. Enregistrement d'un nouveau RCC pour un certificat de cachet déjà émis

Dans le cas de changement d'un RCC en cours de validité d'un certificat de cachet, le nouveau RCC doit être enregistré en tant que tel par l'AE en remplacement de l'ancien RCC. L'enregistrement du nouveau RCC (personne physique) représentant une entité nécessite l'identification de ce RCC et la vérification de son habilitation.

Le représentant légal de l'entité sujette doit faire une demande formelle envoyée auprès de l'AE. Le dossier d'enregistrement doit contenir l'ensemble des éléments listés ci-dessous :

- le formulaire de demande de changement de RCC, daté de moins de 3 mois, signé par un représentant légal de l'entité sujette ;
- tout document, daté de moins de 3 mois, attestant de la qualité du représentant légal de l'entité sujette ;

- un document officiel d'identité en cours de validité d'un représentant légal de l'entité sujette ;
- dans le cas où le RCC n'est pas un représentant légal de l'entité sujette :
    - un mandat, daté de moins de 3 mois, désignant le RCC comme étant habilité à être RCC pour le service de création de cachet pour lequel le certificat de cachet doit être délivré. Ce mandat doit être signé par un représentant légal de l'entité sujette et co-signé, pour acceptation, par le RCC ;
    - un document officiel d'identité en cours de validité du RCC ;
- dans le cas où le RCC n'appartient pas hiérarchiquement à l'entité sujette, tout document, vérifiable et daté de moins de 3 mois, attestant de l'existence de l'entité du RCC et comportant son numéro d'identification unique ;
- les CGU signées électroniquement par l'ensemble des parties.

Le formulaire de demande de changement de RCC comporte :

- les informations d'identification de l'entité du RCC si celle-ci est différente de l'entité sujette ;
- les informations d'identification du représentant légal de l'entité sujette, ainsi que du RCC si celui-ci n'est pas confondu avec le représentant légal de l'entité sujette ;
- les références au certificat de cachet concerné par la demande et les informations devant figurer dans ce certificat ;
- l'information, l'acceptation et l'engagement explicites de chacune des parties quant à leurs obligations respectives.

L'AE effectue les opérations suivantes :

- vérification de la complétude du formulaire ;
- vérification de la signature électronique du formulaire par le représentant légal de l'entité sujette et le cas échéant par le RCC ;
- vérification de la recevabilité et de la cohérence des pièces justificatives produites ;
- vérification de la cohérence des informations portées dans le formulaire avec les pièces justificatives ;
- vérification de la signature électronique par l'ensemble des parties des CGU.

3.2.4. Informations non vérifiées du RCC

L'adresse de messagerie et le numéro de téléphone du RCC sont déclaratifs. Youtrust ne procède pas à la vérification de ces données.

3.2.5. Validation de l'autorité du demandeur

La demande est réalisée par le RCC qui est le représentant légal de l'entité sujette, ou à défaut dispose d'un mandat signé par ce dernier.

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

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

3.3.2. Identification et validation pour un renouvellement après révocation

L'identification et la validation de l'identité du RCC pour un renouvellement après révocation correspond à une nouvelle demande 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

La demande de révocation d'un certificat pourra se faire par courriel par l'entité sujette, le RCC, ou toute autre personne autorisée. Le demandeur doit compléter le formulaire

de demande de révocation. A réception, un opérateur de révocation s'assure des autorisations du demandeur conformément à la procédure suivante :

- Si le demandeur a fourni un secret de révocation, l'opérateur de révocation le vérifie. Si le secret de révocation est correct, l'opérateur de révocation procède à la révocation du certificat ;
- Si le demandeur n'a pas fourni de secret de révocation, ou si ce dernier est incorrect, l'opérateur de révocation appelle le demandeur et lui pose une série de 2 questions aléatoires liées à son identité présumée et dont les réponses se trouvent dans le dossier d'enregistrement ;
- Si le demandeur est injoignable par téléphone, l'opérateur de révocation génère un secret aléatoire et le transmet aux points de contact listés dans le dossier d'enregistrement. L'opérateur de révocation attend ensuite la fourniture de ce secret par le demandeur.

L'opérateur de révocation vérifie les réponses apportées par le demandeur. Si celles-ci sont correctes, l'opérateur de révocation procède à la révocation du certificat. Dans tous les cas, l'opérateur de révocation notifie les points de contact listés dans le dossier d'enregistrement du succès ou de l'échec de l'opération de révocation.

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

La demande de certificat provient par défaut d'un représentant légal de l'entité sujette, qui endosse le rôle de RCC. Ce représentant légal peut alternativement nommer un RCC, faisant ou non partie de la même structure juridique.

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

Le dossier d'enregistrement doit contenir les informations et pièces justificatives listées à la section « Validation initiale de l'identité » et est établi par le RCC, soit directement,

soit à partir des éléments fournis par l'entité sujette. Le dossier est transmis à l'AE par voie électronique. L'AE s'assure de disposer d'une information permettant de contacter le RCC.

4.2. Traitement d'une demande de certificat

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

Les identités des personnes physiques, des personnes morales et le contenu du dossier d'enregistrement sont vérifiés conformément aux exigences de la section « Validation initiale de l'identité ».

Une fois ces contrôles effectués avec succès, l'AE enregistre la demande dans l'IGC, puis l'AC réalise les opérations techniques décrites à la section « Délivrance du certificat ». Enfin, l'AE génère un formulaire synthétisant les opérations réalisées et archive le dossier d'enregistrement.

4.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le demandeur en justifiant le rejet.

4.2.3. Durée d'établissement du certificat

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.

4.3. Délivrance du certificat

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

Suite aux vérifications réalisées par l'AE, l'AC déclenche les processus de génération de la bi-clé, ainsi que du certificat associé.

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 ».

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

Une fois la bi-clé et le certificat générés, et le service de cachet Youtrust activé, le RCC en sera informé via courrier électronique. Un formulaire synthétisant les opérations réalisées, comportant le certificat généré, lui est communiqué.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'acceptation d'un certificat émis par l'AC est tacite dès l'envoi du certificat au RCC par Youtrust.

Le RCC peut refuser le certificat auprès de l'AE en demandant sa révocation.

4.4.2. Publication du certificat

L'AC ne publie pas les certificats de cachet émis. Le certificat est accessible dans chaque document signé ou dans le formulaire de synthèse des opérations réalisées lors du traitement du dossier d'enregistrement.

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

La clé privée et le certificat ne peuvent être utilisés que dans le cadre de l'utilisation du service de cachet Youtrust par l'entité sujette et le service applicatif désignés lors de la demande de certificat. Toute autre utilisation est strictement interdite.

Cette restriction d'utilisation de la clé privée et du certificat associé est assurée par un mécanisme d'authentification, réalisée via une clé d'API associée à l'entité pour laquelle le certificat a été émis. L'utilisation de la clé privée et du certificat est conditionnée à la validation de cette authentification par le service de cachet Youtrust.

4.5.2. Utilisation de la clé publique et du certificat

Cf. section précédente.

4.6. Renouvellement d'un certificat

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

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

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des serveurs, et les certificats correspondants, seront renouvelés au minimum à une fréquence de 3 ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la

révocation du certificat du serveur telle que documentée à la section « Révocation et suspension des certificats ».

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

La délivrance d'un nouveau certificat de cachet liée à la génération d'une nouvelle bi-clé ne pouvant être réalisée qu'après la révocation du certificat actuel, toute délivrance d'un tel 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 RCC 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

Pour modifier un certificat, il faudra révoquer celui-ci puis faire une nouvelle demande auprès de l'AC. 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 cachet

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 ;
- une nouvelle version des CGU ou de la PC est publiée et n'a pas été acceptée, soit par l'entité du RCC, soit par l'entité sujette, dans les délais annoncés par Youtrust ;
- la relation commerciale entre Youtrust et l'entité du RCC a pris fin, soit dans son intégralité, soit sur le service de cachet Youtrust ;
- la relation commerciale entre l'entité du RCC et l'entité sujette a pris fin, soit dans son intégralité, soit dans le cadre du service exploitant le service de cachet Youtrust ;
- un certificat de la chaîne de certification (ACP ou ACI) le certificat de l'AC est révoqué, entraînant de fait la révocation de tous les certificats de cachet 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 cachet

Les personnes / entités qui peuvent demander la révocation d'un certificat de cachet sont les suivantes :

- le RCC ;
- un représentant légal de l'entité sujette ;
- toute personne autorisée par le RCC et disposant du secret de révocation ou d'un accès au dossier d'enregistrement ;
- l'AC émettrice du certificat ou l'une de ses composantes (AE).

Nota : le RCC doit être informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat.

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 cachet

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, le RCC, le responsable légal de l'entité sujette ainsi que les points de contacts listés dans le dossier d'enregistrement du certificat concerné seront informés de l'opération de révocation et de son résultat, que le certificat ait été révoqué ou non.

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 RCC, des responsables légaux des entités sujettes ainsi que des points de contacts listés dans les dossiers d'enregistrement des certificats concernés 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

Dès que l'entité sujette ou son représentant légal, l'entité du RCC ou le RCC 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 cachet

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 cachet 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.

Dans le cas où la demande de révocation est incomplète ou que le demandeur ne peut pas être authentifié, le délai de traitement peut être prolongé et ne commencera qu'à compter de la réception de tous les éléments nécessaires à la révocation.

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 LAR 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 de cachet 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 de cachet. 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 sont générées a minima toutes les 24 heures.

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 30 minutes maximum.

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

Sans objet.

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

Sans objet.

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 de cachet, 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 ».

[1.2.250.1.302.1.24.1.0]
Conformément aux obligations réglementaires sur les prestataires de service de confiance européens, l'organe de contrôle national sera informé de la compromission d'une clé privée de l'AC dans les 24 (vingt-quatre) heures.

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'AC Racine), 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'AC Racine.

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.

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 l'abonné et l'AC

En cas de fin de relation contractuelle entre l'AC et l'abonné avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

De plus, l'AC doit révoquer un certificat de cachet pour lequel il n'y a plus de RCC explicitement identifié.

4.12. Séquestre de clé et recouvrement

Les clés privées d'AC ne sont pas séquestrées. De plus, les clés privées des certificats de cachet ne sont pas séquestrées. Bien qu'elles soient stockées dans le module cryptographique de l'IGC Youtrust en vue de leur utilisation, ceci ne doit pas être considéré comme du séquestre.

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.

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.

- **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.

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. Identification et authentification pour chaque rôle

Toutes les personnes opérant un rôle de confiance au sein de l'IGC Youtrust doivent obtenir une autorisation préalable. Toutes les fonctions de l'IGC sont soumises à un contrôle des autorisations basé sur une authentification forte.

Le responsable d'application gère les autorisations. Il devra gérer la liste des

autorisations en fonction des rôles. De plus, il devra assigner à chaque personne le bon rôle. Enfin, c'est également lui qui délivrera les données d'authentification au personnel. Il délivrera un certificat d'authentification.
Chaque attribution d'un rôle à un membre du personnel de l 'IGC doit être notifiée par écrit. Ce rôle doit être clairement mentionné et décrit dans sa fiche de poste.

5.2.4. 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 vis-à-vis de Youtrust.
Le personnel amené à travailler au sein de l 'IGC Youtrust, occupera un poste correspondant à ses compétences professionnelles. Le personnel occupant un rôle de confiance (responsable de sécurité, responsable d'application, ingénieur système ou auditeur système) devra posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.
L'AC informe toutes les personnes intervenant dans des rôles de confiance de l'IGC :

- de ses 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 le règlement intérieur et la charte informatique fournie à l'ensemble des employés de Youtrust. Celles-ci sont plus ou moins importantes en fonction de l'impact que peut avoir une action non autorisée.

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

Aucun prestataire externe ne peut disposer d'un rôle de confiance au sein de l'IGC Youtrust. Si un prestataire externe doit intervenir sur une composante de l'IGC, ceci doit être fait avec l'accord préalable du responsable de sécurité, et sous sa supervision. Toutes les interventions réalisées doivent être journalisées.

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 RCC,...), 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 :

- 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 RCC ;
- transmission des certificats aux RCC ;
- 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 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 ;

- la trace d'acceptation du certificat par le RCC.

5.5.2. Période de conservation des archives

Dossiers d'enregistrement

Tout dossier d'enregistrement accepté sera archivé 10 ans pour les besoins de fourniture de la preuve de la certification dans des procédures légales.

La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du RCC.

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.

Certificats, LAR et LCR émis par l'AC

Les certificats de cachet et d'AC, ainsi que les LCR / LAR produites, doivent être archivés pendant au moins 10 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 RCC 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.

[1.2.250.1.302.1.24.1.0]
Conformément aux obligations réglementaires sur les prestataires de service de confiance européens, l'organe de contrôle national sera informé de tout incident de sécurité touchant l'AC et ses services dans les 24 (vingt-quatre) heures.

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.

[1.2.250.1.302.1.18.1.0]

- informer tous les RCC ;

[1.2.250.1.302.1.24.1.0]

- informer l'organe de contrôle national dans les vingt-quatre heures (cf. chapitre Reprise suite à la compromission et sinistre).

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

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 RCC 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 serveurs

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

6.2. Transmission de la clé privée à son propriétaire

La clé privée n'est pas transmise au serveur. Elle est stockée par l'IGC au sein d'un module cryptographique.

6.3. Transmission de la clé publique à l'AC

La clé publique du RCC 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 cachet devront avoir ces caractéristiques :

- Algorithme utilisé : RSA.
- Taille minimale des clés :
  - 2048 bits avant le 23 avr. 2024
  - 3072 bits à compter du 23 avr. 2024

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

L'équipement de génération de bi-clés est un module cryptographique conforme aux exigences du chapitre Annexe Exigences de sécurité du module cryptographique de l'AC, paramétré et exploité conformément aux préconisations de son fournisseur, ce qui garantit la qualité des bi-clés générées.

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 de serveur et du certificat associé est strictement au service de cachet de données (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 du RCC est sous contrôle exclusif. Youtrust ne dispose pas des éléments permettant d'accéder et d'utiliser la clé privée d'un serveur durant le processus de signature. Le processus technique garantit que seule la clé privée générée pour le serveur durant le processus de signature est utilisée.

6.8.3. Séquestre de la clé privée

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

6.8.4. Copie de la clé privée

Les clés privées d'AC font l'objet de copies de secours.
Les clés privées des certificats de cachet peuvent faire l'objet de copies.

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 ».

6.8.5. Archivage de la clé privée

Les clés privées d'AC et de serveurs ne sont jamais archivées.

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

La génération des clés privées d'AC et de serveurs se fait dans le module cryptographique.
Le transfert vers / depuis le module cryptographique ne se fait que pour la génération des copies de sauvegardes. Ceci se fait 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 d'AC et de serveurs est réalisé dans un module cryptographique répondant aux exigences du chapitre Annexes ci-dessous pour le niveau de sécurité considéré.
Cependant, dans le cas des copies de secours, 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 d'AC ne sont pas compromises pendant leur stockage ou leur transport.

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.

L'activation de la clé privée des certificats de cachet est décrite dans la section « Méthode pour prouver la possession de la clé privée ».

6.8.9. Méthode de désactivation de la clé privée

La désactivation des clés privées d'AC 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 cachet est automatique en fin de création du cachet et correspond techniquement à la destruction de la clé privée déchiffrée 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 serveur, normale ou anticipée (révocation), cette clé sera systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

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

Les modules cryptographiques utilisés par Youtrust sont des modules validés FIPS 140-2.

[1.2.250.1.302.1.24.1.0]
Les modules cryptographiques utilisés par Youtrust sont des modules qualifiés au niveau renforcé par l'ANSSI.

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 10 ans.

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 cachet qu'elle émet.

Les bi-clés et les certificats de cachet doivent avoir une durée de vie au maximum de 3 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 cachet

Les données d'activation sont constituées des clés d'API, dont la génération et l'utilisation sont décrites à la section « Méthode pour prouver la possession de la clé privée ».

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 cachet

Le RCC a la responsabilité d'assurer la confidentialité des données d'activation des clés des certificats de cachet.

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 réalisés par Youtrust et impactant 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, Youtrust opère un cloisonnement entre les environnements de développement, de test, de pré-production et de production. Ceci permet d'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

Les AC soumises à la présente PC, sont des AC en ligne. Elles n'ont pas d'accès en entrée ou en sortie au réseau public. Les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé.

6.14. Horodatage Système de datation

L 'AC « YOUSIGN SAS - SIGN3 CA » réalise un horodatage sur l'ensemble des éléments archivés.

7. Profil des certificats et des LCR

7.1. Profils de certificats

Les certificats respectent le format décrit par la RFC 5280.

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	
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

7.1.2. 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	
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 cachet

[1.2.250.1.302.1.18.1.0]

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 23 avr. 2024* *3072 bits à compter du 23 avr. 2024*

Champs d'extension	Obligatoire	Critique	Valeur
Authority Key Identifier	Oui	Non	*Hash SHA-1 de la clé publique de l'AC*
Subject Key Identifier	Oui	Non	*Hash SHA-1 de la clé publique du certificat*
Key Usage	Oui	Oui	`Non Repudiation, Digital Signature`

Extended Key Usage	Oui	Non	MS Document Signing (1.3.6.1.4.1.311.10.3.12), PDF Signing (1.2.840.113583.1.1.5)
Certificate Policies	Oui	Non	1.2.250.1.302.1.18.1.0
CRL Distribution Points	Oui	Non	http://crl.yousign.fr/crl/yousignsassign3ca.crl http://crl2.yousign.fr/crl/yousignsassign3ca.crl http://crl3.yousign.fr/crl/yousignsassign3ca.crl
Basic Constraints	Oui	Oui	CA:false
Authority Information Access	Oui	Non	*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

[1.2.250.1.302.1.24.1.0]

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	*3072 bits*

Champs d'extension	Obligatoire	Critique	Valeur
Authority Key Identifier	Oui	Non	*Hash SHA-1 de la clé publique de l'AC*
Subject Key Identifier	Oui	Non	*Hash SHA-1 de la clé publique du certificat*
Key Usage	Oui	Oui	`Non Repudiation, Digital Signature`
Extended Key Usage	Oui	Non	`MS Document Signing (1.3.6.1.4.1.311.10.3.12), PDF Signing (1.2.840.113583.1.1.5)`
Certificate Policies	Oui	Non	`1.2.250.1.302.1.24.1.0 URL de publication : http://yousign.fr/fr/public/document`
CRL Distribution Points	Oui	Non	`http://crl.yousign.fr/crl/yousignsassign3ca.crl` `http://crl2.yousign.fr/crl/yousignsassign3ca.crl` `http://crl3.yousign.fr/crl/yousignsassign3ca.crl`
Basic Constraints	Oui	Oui	`CA:false`
Authority Information Access	Oui	Non	*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`
qcStatements	O	N	esi4- qcStatement-1 = id-etsi-qcsQcCompliance esi4- qcStatement-6 = id-etsi-qct-eseal

7.2. Liste de Certificats Révoqués

Les listes de certificats révoqués respectent le format décrit par la RFC 5280.

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

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. 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.

8.2. Identités qualifications des évaluateurs

Les contrôleurs sont des employés de la société Youtrust. Youtrust s'engage à mandater des personnes disposant des compétences en sécurité requises pour auditer et vérifier la conformité du système.

8.3. Relations entre évaluateurs et entités évaluées

Les contrôleurs sont des membres internes de Youtrust.

8.4. Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) 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 présenteront pour approbation au Comité de Direction Technique la liste des composantes et procédures qui seront auditées.

8.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : "réussite", "échec", "à confirmer". Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.

- En cas de résultat "à confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

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

L'accès aux LCR 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 :

- la partie non-publique de la DPC de l'AC ;
- les clés privées de l'AC, des composantes et des certificats de cachet ;
- les données d'activation associées aux clés privées d'AC et de serveurs ;
- tous les secrets de l'IGC ;
- les journaux d'évènements des composantes de l'IGC ;
- les dossiers d'enregistrement ;
- les causes de révocations, sauf accord explicite du RCC.

9.3.2. Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3. Responsabilités en termes de protection des informations confidentielles

Youtrust applique des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre Périmètre des informations confidentielles. Youtrust s'engage à respecter 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 s'engage 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).

9.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- les causes de révocation des certificats de cachet (qui sont considérées comme confidentielles sauf accord explicite du RCC) ;
- le dossier d'enregistrement du RCC ;
- les données d'activation de la clé privée.

9.4.3. Informations à caractère non personnel

Sans objet.

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

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

9.4.5. Notification et consentement d'utilisation des données personnelles

Le RCC est informé que la délivrance de certificats électroniques suppose la mise en œuvre par Youtrust de traitements de données à caractère personnel auquel le RCC consent. Le RCC est informé que la communication de ses données est obligatoire et nécessaire pour prendre en compte sa demande. Le RCC dispose d'un droit d'accès aux données le concernant auprès du DPO de Youtrust, à l'adresse dpo@yousign.com.

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les RCC à l'AC ne sont pas divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du RCC, décision judiciaire ou autre autorisation légale.

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

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

9.4.7. 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 (par exemple : logiciels, pages Web, bases de données, textes originaux, ...) est sanctionnée par le Code de la propriété intellectuelle.
L'entité détient tous les droits de propriété intellectuelle sur les informations personnelles contenues dans les certificats de cachet émis par l'AC et dont il est propriétaire.

9.6. Interprétations contractuelles et garanties

L'AC garantit 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 RCC.

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

L'AC contrôlera que tout projet de modification de sa PC reste conforme aux exigences de la présente PC. En cas de changement important, l'AC 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 sur son site internet. 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 RCC, 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 de Caen.

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. Accord global

Sans objet.

9.14.2. Transfert d'activités

Sans objet.

9.14.3. Conséquences d'une clause non valide

Sans objet.

9.14.4. Application et renonciation

Sans objet.

9.14.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français.

9.14.6. Autres dispositions

Sans objet.

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 serveurs, répond aux exigences de sécurité suivantes :

- garantir que la génération des bi-clés des certificats de cachet 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 cachet ;
- 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.

[1.2.250.1.302.1.24.1.0]

Le module cryptographique est déployé selon les préconisations de sa cible de sécurité pour la qualification du matériel. La communication avec le module cryptographique est réalisée sur un canal chiffré après authentification mutuelle.

10.2. Exigences sur la certification

Le module cryptographique utilisé par Youtrust dispose d'une certification FIPS 140-2.

[1.2.250.1.302.1.24.1.0]

Le module cryptographique utilisé par Youtrust est qualifié au niveau renforcé par l'ANSSI.