



Autorité de certification et d'horodatage

Politique de certification de l'AC YOUSIGN SAS - QUALIFIED SIGNATURE CA

Exporté le 09/03/2021

Créateur : Florent Eudeline - 05/05/2020

Dernier changement : Kevin Dubourg - 11/09/2020

Diffusion : C1 - Public

Ce document est la propriété exclusive de YOUSIGN.

Sommaire:

1 -	Historiques des évolutions	11
2 -	Introduction	12
2.1 -	Présentation générale	12
2.2 -	Identification du document.....	12
2.3 -	Entités intervenant dans l'IGC.....	12
2.3.1 -	Autorités de certification	12
2.3.2 -	Autorités d'enregistrement	13
2.3.3 -	Opérateur de Services de Certification (OSC).....	13
2.3.4 -	Porteurs de certificats.....	13
2.3.5 -	Utilisateurs de certificats.....	13
2.4 -	Usage des certificats	13
2.4.1 -	Domaines d'utilisation applicables.....	13
2.4.2 -	Bi-clés et certificats d'AC et de composantes.....	13
2.4.3 -	Domaines d'utilisation interdits.....	14
2.5 -	Gestion de la PC	14
2.5.1 -	Entité gérant la PC et la DPC.....	14
2.5.2 -	Point de contact.....	14
2.6 -	Définitions et acronymes.....	14
2.6.1 -	Acronymes.....	14
2.6.2 -	Définitions	15
2.7 -	Références documentaires.....	17
3 -	Responsabilités concernant la mise à disposition des informations devant être publiées.....	18
3.1 -	Entités chargées de la mise à disposition des informations.....	18
3.2 -	Informations devant être publiées.....	18
3.3 -	Délais et fréquences de publication.....	18
3.4 -	Contrôle d'accès aux informations publiées	18
4 -	Identification et authentification	19
4.1 -	Nommage	19
4.1.1 -	Types de noms	19

4.1.2 -	Nécessité d'utilisation de noms explicites	20
4.1.3 -	Pseudonymisation des porteurs	20
4.1.4 -	Règles d'interprétation des différentes formes de nom	20
4.1.5 -	Unicité des noms.....	20
4.1.6 -	Identification, authentification et rôle des marques déposées	20
4.2 -	Validation initiale de l'identité	20
4.2.1 -	Méthode pour prouver la possession de la clé privée	20
4.2.2 -	Validation de l'identité d'un organisme	20
4.2.3 -	Validation de l'identité d'un individu.....	21
4.2.4 -	Informations non vérifiées du porteur.....	22
4.2.5 -	Validation de l'autorité du demandeur.....	22
4.3 -	Identification et validation d'une demande de renouvellement des clés	22
4.3.1 -	Identification et validation pour un renouvellement courant.....	22
4.3.2 -	Identification et validation pour un renouvellement après révocation.....	22
4.4 -	Identification et validation d'une demande de révocation	22
5 -	Exigences opérationnelles sur le cycle de vie des certificats.....	22
5.1 -	Demande de certificat.....	22
5.1.1 -	Origine d'une demande de certificat	22
5.1.2 -	Processus et responsabilités pour l'établissement d'une demande de certificat.....	23
5.2 -	Traitement d'une demande de certificat.....	23
5.2.1 -	Exécution des processus d'identification et de validation de la demande	23
5.2.2 -	Acceptation ou rejet de la demande	23
5.2.3 -	Durée d'établissement du certificat.....	23
5.3 -	Délivrance du certificat.....	23
5.3.1 -	Actions de l'AC concernant la délivrance du certificat.....	23
5.3.2 -	Notification par l'AC de la délivrance du certificat au porteur	24
5.4 -	Acceptation du certificat	24
5.4.1 -	Démarche d'acceptation du certificat	24
5.4.2 -	Publication du certificat	24
5.4.3 -	Notification par l'AC aux autres entités de la délivrance du certificat	24
5.5 -	Usages de la bi-clé et du certificat	24
5.5.1 -	Utilisation de la clé privée et du certificat par le porteur	24
5.5.2 -	Utilisation de la clé publique et du certificat par l'utilisateur du certificat	24
5.6 -	Renouvellement d'un certificat.....	24

5.7 -	Délivrance d'un nouveau certificat suite au changement de la bi-clé	25
5.8 -	Modification du certificat	25
5.9 -	Révocation et suspension des certificats.....	25
5.9.1 -	Causes possibles d'une révocation	25
5.9.1.1 -	Certificats des porteurs.....	25
5.9.1.2 -	Certificats d'une composante de l'AC	25
5.9.2 -	Origine d'une demande de révocation	26
5.9.2.1 -	Certificats de porteurs	26
5.9.2.2 -	Certificats d'une composante de l'IGC.....	26
5.9.3 -	Procédure de traitement d'une demande de révocation	26
5.9.3.1 -	Révocation d'un certificat porteur	26
5.9.3.2 -	Révocation d'un certificat d'une composante de l'IGC.....	27
5.9.4 -	Délai accordé au porteur pour formuler la demande de révocation	27
5.9.5 -	Délai de traitement par l'AC d'une demande de révocation	27
5.9.5.1 -	Révocation d'un certificat porteur	27
5.9.5.2 -	Révocation d'un certificat d'une composante de l'IGC.....	28
5.9.6 -	Exigences de vérification de la révocation par les utilisateurs de certificats	28
5.9.7 -	Fréquence d'établissement des LCR.....	28
5.9.8 -	Délai maximum de publication d'une LCR	28
5.9.9 -	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats.....	28
5.9.10 -	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats	28
5.9.11 -	Autres moyens disponibles d'information sur les révocations	28
5.9.12 -	Exigences spécifiques en cas de compromission de la clé privée	28
5.9.13 -	Suspension des certificats.....	29
5.10 -	Fonction d'information sur l'état des certificats.....	29
5.10.1 -	Caractéristiques opérationnelles.....	29
5.10.2 -	Disponibilité de la fonction	29
5.11 -	Fin de la relation entre le porteur et l'AC	29
5.12 -	Séquestre de clé et recouvrement	29
6 -	Mesures de sécurité non techniques.....	29
6.1 -	Mesures de sécurité physique	29
6.1.1 -	Situation géographique et construction des sites	29
6.1.2 -	Accès physique.....	29
6.1.3 -	Alimentation électrique et climatisation	30

6.1.4 -	Vulnérabilité aux dégâts des eaux.....	30
6.1.5 -	Prévention et protection incendie	30
6.1.6 -	Conservation des supports.....	30
6.1.7 -	Mise hors service des supports.....	30
6.1.8 -	Sauvegardes hors site	30
6.2 -	Mesures de sécurité procédurales	30
6.2.1 -	Rôles de confiance	30
6.2.2 -	Nombre de personnes requises par tâche	31
6.2.3 -	Identification et authentification pour chaque rôle.....	31
6.2.4 -	Rôles exigeant une séparation des attributions.....	32
6.3 -	Mesures de sécurité vis-à-vis du personnel	32
6.3.1 -	Qualifications, compétences et habilitations requises.....	32
6.3.2 -	Procédures de vérification des antécédents	32
6.3.3 -	Exigences en matière de formation initiale	32
6.3.4 -	Exigences et fréquence en matière de formation continue.....	32
6.3.5 -	Fréquence et séquence de rotation entre différentes attributions.....	32
6.3.6 -	Sanctions en cas d'actions non autorisées.....	32
6.3.7 -	Exigences vis-à-vis du personnel des prestataires externes.....	33
6.3.8 -	Documentation fournie au personnel.....	33
6.4 -	Procédure de constitution des données d'audit.....	33
6.4.1 -	Type d'évènements à enregistrer.....	33
6.4.2 -	Fréquence de traitement des journaux d'évènements	34
6.4.3 -	Période de conservation des journaux d'évènements.....	34
6.4.4 -	Protection des journaux d'évènements.....	34
6.4.5 -	Procédure de sauvegarde des journaux d'évènements.....	34
6.4.6 -	Système de collecte des journaux d'évènements	34
6.4.7 -	Notification de l'enregistrement d'un évènement au responsable de l'évènement.....	34
6.4.8 -	Évaluation des vulnérabilités	34
6.5 -	Archivage des données	35
6.5.1 -	Types de données à archiver	35
6.5.2 -	Période de conservation des archives	35
6.5.3 -	Protection des archives	35
6.5.4 -	Procédure de sauvegarde des archives	35
6.5.5 -	Exigences d'horodatage des données	36




6.5.6 -	Système de collecte des archives.....	36
6.5.7 -	Procédures de récupération et de vérification des archives	36
6.6 -	Changement de clé d'AC.....	36
6.7 -	Reprise suite à la compromission et sinistre	36
6.7.1 -	Procédures de remontée et de traitement des incidents et des compromissions.....	36
6.7.2 -	Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données).....	37
6.7.3 -	Procédures de reprise en cas de compromission de la clé privée d'une composante.....	37
6.7.4 -	Capacités de continuité d'activité suite à un sinistre	37
6.8 -	Fin de vie de l'IGC	37
6.8.1 -	Transfert d'activité ou cessation d'activité affectant une composante de l'IGC.....	38
6.8.2 -	Cessation d'activité affectant l'AC	38
7 -	Mesures de sécurité techniques	38
7.1 -	Génération et installation de bi-clés	39
7.1.1 -	Génération des bi-clés	39
7.1.1.1 -	Clés d'AC	39
7.1.1.2 -	Clés des porteurs.....	39
7.1.2 -	Transmission de la clé privée à son propriétaire.....	39
7.1.3 -	Transmission de la clé publique à l'AC	39
7.1.4 -	Transmission de la clé publique de l'AC aux utilisateurs de certificats	39
7.1.5 -	Tailles des clés.....	40
7.1.6 -	Vérification de la génération des paramètres des bi-clés et de leur qualité.....	40
7.1.7 -	Objectifs d'usage de la clé	40
7.2 -	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques.....	40
7.2.1 -	Standards et mesures de sécurité pour les modules cryptographiques	40
7.2.2 -	Contrôle de la clé privée par plusieurs personnes	40
7.2.2.1 -	Clés d'AC	40
7.2.2.2 -	Clés porteur	40
7.2.3 -	Séquestre de la clé privée.....	41
7.2.4 -	Copie de secours de la clé privée	41
7.2.4.1 -	Clés d'AC	41
7.2.4.2 -	Clés porteur	41
7.2.5 -	Archivage de la clé privée	41
7.2.6 -	Transfert de la clé privée vers / depuis le module cryptographique.....	41

7.2.7 -	Stockage de la clé privée dans un module cryptographique	41
7.2.8 -	Méthode d'activation de la clé privée	42
7.2.8.1 -	Clés d'AC	42
7.2.8.2 -	Clés porteur	42
7.2.9 -	Méthode de désactivation de la clé privée	42
7.2.10 -	Méthode de destruction des clés privées	42
7.2.11 -	Niveau de qualification du module cryptographique et des dispositifs de création de signature.....	42
7.3 -	Autres aspects de la gestion des bi-clés.....	42
7.3.1 -	Archivage des clés publiques	42
7.3.2 -	Durées de vie des bi-clés et des certificats	43
7.4 -	Données d'activation	43
7.4.1 -	Génération et installation des données d'activation	43
7.4.1.1 -	Clés de l'AC	43
7.4.1.2 -	Clés des porteurs.....	43
7.4.2 -	Protection des données d'activation	43
7.4.2.1 -	Clés de l'AC	43
7.4.2.2 -	Clés des porteurs.....	43
7.4.3 -	Autres aspects liés aux données d'activation.....	43
7.5 -	Mesures de sécurité des systèmes informatiques.....	43
7.5.1 -	Exigences de sécurité technique spécifiques aux systèmes informatiques	43
7.5.2 -	Niveau de qualification des systèmes informatiques	44
7.6 -	Mesures de sécurité liées au développement des systèmes	44
7.6.1 -	Mesures liées à la gestion de la sécurité	44
7.6.2 -	Niveau d'évaluation sécurité du cycle de vie des systèmes	44
7.7 -	Mesures de sécurité réseau	44
7.8 -	Horodatage Système de datation	44
8 -	Profil des certificats et des LCR	45
8.1 -	Profils de certificats	45
8.1.1 -	Certificats de l'ACR.....	45
8.1.2 -	Certificats de l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA »	47
8.1.3 -	Certificats éphémère de signature	49
8.1.4 -	Certificats du service OCSP	51
8.2 -	Liste de Certificats Révoqués	53
8.3 -	Répondeur OCSP.....	53

8.3.1 -	Requêtes OCSP.....	53
8.3.2 -	Réponses OCSP	54
9 -	Audit de conformité et autres évaluations	54
9.1 -	Fréquences et ou circonstances des évaluations.....	55
9.2 -	Identités qualifications des évaluateurs.....	55
9.3 -	Relations entre évaluateurs et entités évaluées	55
9.4 -	Sujets couverts par les évaluations.....	55
9.5 -	Actions prises suite aux conclusions des évaluations.....	55
10 -	Autres problématiques métiers et légales.....	55
10.1 -	Tarifs	55
10.1.1 -	Tarifs pour la fourniture ou le renouvellement de certificats.....	55
10.1.2 -	Tarifs pour accéder aux certificats	55
10.1.3 -	Tarifs pour accéder aux LCR et au répondeur OCSP	56
10.1.4 -	Politique de remboursement	56
10.2 -	Responsabilité financière	56
10.2.1 -	Couverture par les assurances	56
10.2.2 -	Autres ressources.....	56
10.2.3 -	Couverture et garantie concernant les entités utilisatrices.....	56
10.3 -	Confidentialité des données professionnelles	56
10.3.1 -	Périmètre des informations confidentielles	56
10.3.2 -	Informations hors du périmètre des informations confidentielles	56
10.3.3 -	Responsabilités en termes de protection des informations confidentielles	56
10.4 -	Protection des données personnelles	57
10.4.1 -	Politique de protection des données personnelles	57
10.4.2 -	Informations à caractère personnel.....	57
10.4.3 -	Informations à caractère non personnel	57
10.4.4 -	Responsabilité en termes de protection des données à caractères personnelles	57
10.4.5 -	Notification et consentement d'utilisation des données personnelles	57
10.4.6 -	Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives	57
10.4.7 -	Autres circonstances de divulgation d'informations personnelles.....	57
10.5 -	Droits sur la propriété intellectuelle et industrielle	57
10.6 -	Interprétations contractuelles et garanties.....	58
10.6.1 -	Autorités de Certification.....	58

10.6.2 -	Service d'enregistrement	58
10.6.3 -	Porteurs de certificats.....	58
10.6.4 -	Utilisateurs de certificats.....	59
10.6.5 -	Autres participants.....	59
10.7 -	Limite de garantie	59
10.8 -	Limite de responsabilité	59
10.9 -	Indemnités	59
10.10 -	Durée et fin anticipée de validité de la PC	59
10.10.1 -	Durée de validité	59
10.10.2 -	Fin anticipée de validité.....	59
10.10.3 -	Effets de la fin de validité et clauses restant applicables	60
10.11 -	Amendements à la PC	60
10.11.1 -	Procédures d'amendements	60
10.11.1.1 -	Décision	60
10.11.1.2 -	Réalisation.....	60
10.11.2 -	Mécanisme et période d'information sur les amendements.....	60
10.11.3 -	Circonstances selon lesquelles l'OID doit être changé	60
10.12 -	Dispositions concernant la résolution de conflits.....	61
10.13 -	Juridictions compétentes.....	61
10.14 -	Conformité aux législations et réglementations	61
10.15 -	Dispositions diverses	61
10.15.1 -	Accord global.....	61
10.15.2 -	Transfert d'activités	61
10.15.3 -	Conséquences d'une clause non valide.....	61
10.15.4 -	Application et renonciation	61
10.15.5 -	Force majeure	61
10.15.6 -	Autres dispositions.....	61
11 -	Annexe 1 Exigences de sécurité du module cryptographique de l'AC	62
11.1 -	Exigences sur les objectifs de sécurité.....	62
11.2 -	Exigences sur la certification	62
12 -	Annexe 2 Exigences de sécurité du dispositif du système de signature.....	62
12.1 -	Exigences sur les objectifs de sécurité.....	62
12.2 -	Exigences sur la certification	63

1 - Historiques des évolutions

Version	Objet de la révision	Date	Auteur
1.0.2	Corrections documentaires suite à l'audit Uniformisation terminologique	 5 nov. 2020	Florent Eudeline
1.0.1	Modification mise en page	 18 août 2020	Florent Eudeline
1.0.0	Création du document	 25 sept. 2018	Antoine Louiset

2 - Introduction

2.1 - Présentation générale

La société Yousign est un Prestataire de Service de Certification Electronique (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 - QUALIFIED SIGNATURE CA ». Ce document regroupe l'ensemble des engagements et des pratiques de Yousign dans le cadre du déploiement et de l'exploitation de l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA », tant sur les plans techniques qu'organisationnels.

L'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA » ne peut être utilisée que pour :

- produire des certificats qualifiés de signature éphémères ;
- produire des Listes des Certificats Révoqués (LCR) ;
- produire des certificats pour son répondeur OCSP.

Les certificats qualifiés de signature sont exclusivement à destination de personnes physiques, en lien ou non avec une personne morale.

Ces certificats sont conformes à la norme ETSI 319 411-2 au niveau QCP-n (voir [EN_319411-2]) et sont qualifiés, au sens du règlement eIDAS [EIDAS], par l'ANSSI.

La chaîne de certification est la suivante :

- AC Racine : « YOUSIGN SAS - ROOT2 CA »
 - AC Émettrice : « YOUSIGN SAS - QUALIFIED SIGNATURE CA »

2.2 - Identification du document

L'identifiant de ce document est :

- OID : 1.2.250.1.302.1.11.1.0, pour l'émission des certificats qualifiés de signature éphémères,

L'OID peut 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.

2.3 - Entités intervenant dans l'IGC

2.3.1 - Autorités de certification

La notion d'Autorité de Certification (AC) telle qu'utilisée dans la présente PC est définie au chapitre [Définitions et acronymes](#) ci-dessous.

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,...) et s'appuie pour cela sur une infrastructure technique : une Infrastructure de Gestion de Clés (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. L'AC maintient une analyse de risques sur le périmètre des services de certification qu'elle propose. Le Comité de Direction Technique de l'AC décide de la stratégie de gestion des risques, valide et suit les plans d'actions correspondants.

L'Autorité de Certification est la société « YOUSIGN SAS » qui assure l'ensemble des fonctions.

2.3.2 - Autorités d'enregistrement

L'Autorité d'Enregistrement (AE) a pour rôle de vérifier l'identité du futur porteur de certificat. L'AE est opérée par un service interne de Yousign.

2.3.3 - Opérateur de Services de Certification (OSC)

Yousign opère lui-même ses différents services. Yousign fait héberger son infrastructure chez deux fournisseurs d'hébergement tiers (OVH et TELEHOUSE).

2.3.4 - Porteurs de certificats

Le porteur de certificat est une personne physique, qui peut être enregistrée en son nom propre ou en lien avec une personne morale. Dans ce dernier cas, ce lien est vérifié lors de la validation d'identité du porteur. La personne morale peut être une entreprise ou une administration.

Si le porteur de certificat signe au nom et pour le compte d'une personne morale, il déclare avoir le pouvoir d'engager juridiquement cette personne morale dans le cadre de l'opération pour laquelle le processus de signature électronique est mis en œuvre.

Le porteur respecte les obligations qui lui incombent, définies dans la présente PC et résumées dans les CGU qu'il doit accepter avant l'utilisation de son certificat.

2.3.5 - Utilisateurs de certificats

Un utilisateur désigne une personne physique ou un service en ligne amené à vérifier la validité d'un certificat ainsi que son lien avec les données signées.

Les utilisateurs exploitent les informations contenues dans le certificat, ainsi que celle mises à disposition en ligne par l'AC, afin de vérifier sa validité (révocation, date de validité, ...).

Les utilisateurs doivent respecter les obligations qui leur incombent, telles que définies dans la présente PC, en particulier au [Interprétations contractuelles et garanties](#).

2.4 - Usage des certificats

2.4.1 - Domaines d'utilisation applicables

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

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

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

2.4.2 - Bi-clés et certificats d'AC et de composantes

Cette PC comporte également des exigences concernant les bi-clés et certificats de l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA ».

L'AC génère et signe différents types d'objets : certificats et LCR. Pour signer ces objets, l'AC dispose d'une bi-clé, dont le certificat correspondant est rattaché à une AC de niveau supérieur (voir la hiérarchie [Présentation générale](#)).

La signature des réponses OCSP est réalisée par un certificat spécifique émis par l'AC (voir ci-dessous).

Les bi-clés et certificats de l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA » ne sont utilisés que pour la signature

de certificats, de LCR et uniquement à cette fin. Ils ne sont notamment jamais utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

L'AC produit aussi des certificats destinés exclusivement au scellement des réponses OCSP de son service. Ces certificats sont différenciés des certificats des porteurs clients du service de signature par un identifiant de politique spécifique (OID : 1.2.250.1.302.1.12.1.0, voir au §7.1.4). Le processus de gestion du certificat OCSP suit une procédure interne qui n'est pas détaillée dans cette PC.

2.4.3 - Domaines d'utilisation interdits

Tout domaine d'application qui n'est pas prévu dans le chapitre précédent [Usage des certificats](#), est interdit. De plus, les usages du certificat doivent être en conformité avec la législation et la réglementation.

2.5 - Gestion de la PC

2.5.1 - Entité gérant la PC et la DPC

La société Yousign SAS est responsable de la PC.

Yousign organise un Comité de Direction Technique comprenant des membres de la direction de Yousign, des experts fonctionnels et techniques. Le Comité de Direction Technique a la responsabilité de la validation de la PC, de sa qualification et de sa mise en œuvre.

Le Comité de Direction Technique prend en charge la mise en place et le suivi de l'infrastructure technique opérationnelle. Il 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.

Les modalités de modification de présent document sont détaillées au chapitre [Amendements à la PC2](#).

2.5.2 - Point de contact

Toute demande relative à la présente PC est à adresser à :

Gestion de l'AC Yousign

Yousign SAS

8 allée Henri Pigis

14000 CAEN

Adresse de messagerie : contact@yousign.fr

2.6 - Définitions et acronymes

2.6.1 - Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

ACAutorité de Certification

ACIAutorité de Certification Intermédiaire

ACRAutorité de Certification Racine

AEAutorité d'Enregistrement

ANSSIAgence Nationale de la Sécurité des Systèmes d'information

CGU Conditions Générales d'Utilisation

DNDistinguished Name

DPCDéclaration des Pratiques de Certification

eIDAS electronic IDentification, Authentication and trust Services

HSMHardware Security Module (module cryptographique)

IDS Intrusion Detection System

IGC Infrastructure de Gestion de Clés
LAR Liste des certificats d'AC Révoqués
LCR Liste des Certificats Révoqués
OCSP Online Certificate Status Protocol
OID Object Identifier
OSC Opérateur de Service de Certification
PC Politique de Certification
PSCE Prestataire de Services de Certification Électronique
RSAR Rivest Shamir Adelman
SMS Short Message Service
URL Uniform Resource Locator
VPN Virtual Private Network

2.6.2 - Définitions

Les termes utilisés dans la présente PC sont les suivants :

Autorité d'enregistrement - Cf. chapitre [Entités intervenant dans l'IGC2](#)

Autorité d'horodatage - Autorité responsable de la gestion d'un service d'horodatage.

Autorité de certification (AC) - Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre 1.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

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 ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Certificat de signature éphémère - Certificat électronique de signature, valide pour quelques minutes seulement, émis à la volée par l'AC pour une transaction initiée par le porteur et comportant une ou plusieurs signatures.

Clé privée - clé de la bi-clé asymétrique d'une entité ou d'un porteur.

Clé publique - clé de la bi-clé asymétrique d'une entité ou d'un porteur qui peut être rendue publique.

Code d'authentification - code permettant d'authentifier un porteur pour valider une signature.

Comité de Direction Technique - le comité de direction technique est un comité interne à Yousign qui est en charge du bon fonctionnement de l'IGC Yousign.

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 (DPC) - Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux porteurs et en conformité avec la ou les politiques de certification 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.

Fonction de génération des certificats - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du porteur de la fonction de génération des éléments secrets du porteur.

Fonction de génération des éléments secrets du porteur - Cette fonction génère la bi-clé du porteur.

Fonction de gestion des révocations - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction de publication - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats.

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).

Infrastructure de gestion de clés (IGC) - 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.

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 porteurs et réaliser des opérations cryptographiques.

Opérateur de Service de Certification – entité en charge d'assurer la mise en œuvre et le maintien en conditions opérationnelles des services nécessaires au fonctionnement de l'AC.

Personne autorisée - Il s'agit d'une personne autre que le porteur qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, ...). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du porteur.

Politique de certification (PC) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Porteur - La personne physique identifiée dans le certificat et qui est la seule personne autorisée à utiliser la clé privée correspondant à la clé publique qui est dans le certificat.

Prestataire de services de certification électronique (PSCE) - 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 porteurs 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).

Système de signature Yousign – Le système de signature Yousign est une application fournie par Yousign permettant à un porteur d'utiliser la clé privée correspondant à la clé publique qui est dans le certificat qui l'identifie en vue de réaliser des signatures électroniques de données et d'autoriser la signature de ces données par d'autres utilisateurs. C'est le seul système autorisée à accéder aux clés privées des porteurs. Pour pouvoir utiliser leur clé privée, les porteurs doivent s'authentifier via un Code d'authentification.

Utilisateur de certificat - Cf. chapitre [Entités intervenant dans l'IGC2](#).

2.7 - Références documentaires

<p>[<ac:structured-macro ac:name="anchor" ac:schema-version="1" ac:macro-id="077c3c55-a26d-4a2c-becb-5931dcac92b8"><ac:parameter ac:name="">ANSSI_DELIV_CERT</ac:parameter></ac:structured-macro>ANSSI_DELIV_CERT]</p>	<p>Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.1 du 3 janvier 2017 https://www.ssi.gouv.fr/uploads/2016/06/eidas_delivrance-certificats-qualifies_v1.1_anssi.pdf</p>
<p>[ANSSI_PSCO]</p>	<p>Prestataires de services de confiance qualifiés – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.2 du 5 juillet 2017 https://www.ssi.gouv.fr/uploads/2017/01/eidas_psc-qualifies_v1.2_anssi.pdf</p>
<p>[EN_319401]</p>	<p>ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.02.01_60/en_319401v020201p.pdf</p>
<p>[EN_319411-2]</p>	<p>ETSI EN 319 411-2 V2.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.02.02_60/en_31941102v020202p.pdf</p>
<p>[GDPR]</p>	<p>Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 – Règlement Général de Protection des Données https://www.cnil.fr/fr/reglement-europeen-protection-donnees</p>

[EIDAS]	Règlement (UE) 2014/910 du Parlement européen et du Conseil du 23 juillet 2014 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32014R0910
---------	---

3 - Responsabilités concernant la mise à disposition des informations devant être publiées

3.1 - Entités chargées de la mise à disposition des informations

Yousign a mis en place une page regroupant les publications à l'adresse suivante :

<https://yousign.com/documentation-technique-des-certifications/>

3.2 - Informations devant être publiées

Yousign publie les informations suivantes :

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

Les PC et les certificats sont accompagnés d'une empreinte (algorithme SHA256) permettant d'en vérifier l'intégrité.

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

3.3 - 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 contenant l'OID correspondant ;
- Les LCR sont publiées quotidiennement, les LAR annuellement.
- Les certificats d'AC sont publiés suite à leur émission et avant toute signature d'un certificat final.
- Les CGU Yousign sont publiées suite à chaque mise à jour.

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 Yousign décide des différentes parties (clients, utilisateurs, sous-traitants de la fourniture du service, organismes de contrôle...) 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.

3.4 - Contrôle d'accès aux informations publiées

Toutes les informations publiées indiquées ci-dessus, sont publiques et ne sont accessibles qu'en lecture. L'accès en modification aux données publiées est restreint aux équipes internes Yousign 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 Yousign qui est conforme aux exigences réglementaires en vigueur.

4 - Identification et authentification

4.1 - Nommage

4.1.1 - Types de noms

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

Les certificats des porteurs sont conformes à la norme [X.509]. L'AC émettrice et le porteur des certificats sont identifiés par un « *Distinguished Name* » (DN) conforme aux spécifications de la norme [X.501] et du règlement eIDAS (voir [EIDAS]).

Les DN sont construits de la façon suivante :

Attribut	Description	Présence
CN	<i>commonName</i> : Nom et prénom du porteur	Oui
SN	<i>surname</i> : Nom du porteur	Oui
GN	<i>givenName</i> : Prénom du porteur	Oui
OI	<i>organizationIdentifier</i> : Identifiant de l'entité avec laquelle le porteur est en lien, selon la syntaxe eIDAS : NTRFR-<numéro de SIREN>	Uniquement en cas de lien avec une personne morale
OU	<i>organizationUnit</i> : Identifiant de l'entité avec laquelle le porteur est en lien, selon la syntaxe RGS : 0002 <numéro de SIREN>	
O	<i>organizationName</i> : Nom de l'entité avec laquelle le porteur est en lien	
C	<i>countryName</i> : Pays de l'autorité d'enregistrement de Yousign., toujours égal à FR (France)	Oui
serialNumber	<i>serialNumber</i> : Date et l'heure de lancement de la génération du certificat.	Oui

Les certificats de test émis par l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA » sont identifiables immédiatement par l'ajout du préfixe « TEST – » dans la valeur de l'attribut CN, par exemple :

CN = TEST – Jean DUPONT,...

En dehors de cette spécificité, les certificats de tests émis par l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA » suivent les mêmes processus que les certificats de production nominale.

4.1.2 - Nécessité d'utilisation de noms explicites

Les noms contenus dans les certificats sont explicites.

4.1.3 - Pseudonymisation des porteurs

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

4.1.4 - Règles d'interprétation des différentes formes de nom

Les éléments contenus dans le chapitre [Nommage2](#) fournissent les explications permettant d'interpréter correctement les différentes formes de nom.

4.1.5 - Unicité des noms

Pour assurer l'unicité des noms, le DN du sujet du certificat contient un champ « *serialNumber* » correspondant à la date et à l'heure de lancement de la génération du certificat. Ceci garantit qu'un DN utilisé pour un porteur ne sera jamais réassigné à un autre porteur pendant toute la durée de vie de l'AC.

4.1.6 - Identification, authentification et rôle des marques déposées

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

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

4.2 - Validation initiale de l'identité

La validation initiale de l'identité du porteur est réalisée lors d'un face à face physique auprès de l'AE, dans une phase d'enregistrement du porteur.

Le porteur obtient au cours de cet enregistrement un moyen d'identification lui permettant de s'authentifier fortement pour déclencher par la suite une signature électronique.

4.2.1 - Méthode pour prouver la possession de la clé privée

Sans objet puisque le porteur ne génère pas sa propre clé.

La clé privée du porteur est entièrement gérée, stockée et protégée par l'IGC Yousign qui s'assure qu'elle reste sous le contrôle exclusif de son porteur.

4.2.2 - Validation de l'identité d'un organisme

Sans objet.

4.2.3 - Validation de l'identité d'un individu

La validation initiale de l'identité du porteur est réalisée par l'AE lors d'un face à face physique. Le porteur y remet un dossier d'enregistrement complété et comprenant :

- Le formulaire de demande de certificat, signé par le porteur et datée de moins de 3 mois ;
- Les conditions générales d'utilisation en vigueur signées par le porteur ;
- Un justificatif d'identité du porteur en cours de validité parmi les justificatifs suivants :
 - la carte d'identité,
 - le passeport,
 - la carte de séjour ;
- Uniquement pour une demande en lien avec une personne morale :
 - pour une entreprise, toute pièce, valide lors de la demande de certificat, attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;
 - pour une entreprise, tout document signé par le responsable légal et attestant de la qualité du signataire à faire une demande de certificat pour le compte de son entreprise ;
 - pour une administration, une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative ;
 - pour une entreprise ou une administration, le formulaire de demande de certificat doit être signé par un représentant légal de la personne morale en plus de la signature du porteur.

Le formulaire de demande comporte :

- Le type de certificat demandé ;
- Les nom et prénom du porteur, tels qu'ils apparaissent sur la pièce d'identité présentée avec le dossier ;
- Des informations issues de la pièce d'identité présentée : type, numéro, date de validité, autorité émettrice ;
- L'adresse de messagerie électronique du porteur ;
- Un numéro de téléphone pour joindre le porteur ;
- L'acceptation explicite par le porteur de ses obligations ;
- L'engagement d'exactitude des informations du formulaire, et en particulier celles qui seront reprises dans le certificat ;
- Le consentement du porteur à la conservation par l'AC des informations du dossier d'enregistrement et de gestion de ses clés de signature ;

L'AE effectue les opérations suivantes lors du face à face :

- Vérification de la complétude et de la signature par le futur porteur du formulaire de demande ;
- Vérification de la signature par le futur porteur des conditions générales d'utilisation du service de signature ;
- Validation de l'identité du futur porteur par contrôle de l'original de la pièce d'identité ;
- Vérification de la cohérence des informations portées dans le formulaire de demande avec la pièce d'identité ;
- Pour le cas demande en lien avec une personne morale
 - Vérification de la validité des pièces justificatives supplémentaires ;
 - Vérification de la signature par la personne morale de la demande.

La vérification de l'adresse de messagerie du porteur est effectuée durant le processus de création de compte du porteur sur le service Yousign.

Une fois ces contrôles effectués avec succès, l'AE date et signe le formulaire puis enregistre le demandeur dans l'IGC.

Cet enregistrement déclenche le processus d'attribution du moyen d'identification électronique qui permettra, par la suite, au porteur de s'authentifier pour effectuer une signature électronique à la volée avec Yousign.

L'enrôlement du porteur pour ce moyen d'identification se fait en face à face avec l'AE afin de garantir l'identité

associée à ce moyen.

L'AE archive le formulaire de demande, les CGU ainsi qu'une copie recto/verso du titre d'identité. Le porteur obtient une copie du formulaire et des conditions générales d'utilisation.

4.2.4 - Informations non vérifiées du porteur

Sans objet.

4.2.5 - Validation de l'autorité du demandeur

Sans objet.

4.3 - Identification et validation d'une demande de renouvellement des clés

4.3.1 - Identification et validation pour un renouvellement courant

Une nouvelle bi-clé et un nouveau certificat sont générés à chaque demande de signature.

Pendant une durée de 3 ans après la date d'enregistrement auprès de l'AE, le porteur utilise le moyen d'authentification qui lui a été fourni à l'enregistrement pour déclencher un processus de signature et obtenir un certificat éphémère spécifique à chaque transaction.

Au-delà de cette période, le porteur doit obligatoirement renouveler son enregistrement auprès de l'AE, selon le processus spécifié au chapitre [Validation initiale de l'identité](#)². Son moyen d'authentification est renouvelé à cette occasion.

4.3.2 - Identification et validation pour un renouvellement après révocation

Après une révocation, l'identification et la validation de l'identité du porteur doivent être réalisées selon le processus initial, spécifié au chapitre [Validation initiale de l'identité](#)². Son moyen d'authentification est renouvelé à cette occasion. Aucun nouveau certificat à la volée ne peut être émis avant la réalisation de ce nouvel enregistrement.

4.4 - Identification et validation d'une demande de révocation

La demande de révocation d'un certificat doit être réalisée par le porteur lui-même.

L'identité du porteur est vérifiée par l'AE qui traite la demande via :

- une série de deux questions aléatoires concernant cette identité ;
- une confirmation par un autre canal que celui utilisé pour la demande.

5 - Exigences opérationnelles sur le cycle de vie des certificats

5.1 - Demande de certificat

5.1.1 - Origine d'une demande de certificat

La demande de certificat est toujours réalisée par le futur porteur.

5.1.2 - Processus et responsabilités pour l'établissement d'une demande de certificat

L'enregistrement et la validation initiale d'identité sont décrits au chapitre [Validation initiale de l'identité](#) : Le dossier de demande est établi directement par le futur porteur. Celui-ci prend rendez-vous auprès de l'AE afin de déposer ce dossier et valider son identité par un face à face physique. Il obtient un moyen d'identification électronique pour pouvoir déclencher une signature électronique à la volée. Le porteur doit disposer d'un compte sur le service de signature Yousign, créé préalablement ou pendant la phase de validation initiale d'identité. Suite à cette vérification initiale, une demande de certificat est émise lorsque le porteur réalise une nouvelle transaction de signature. Le porteur doit s'authentifier fortement avec le moyen d'identification obtenu à l'enregistrement initial pour que la demande soit envoyée à l'AC.

La réalisation du processus d'authentification par le porteur est sous la responsabilité du fournisseur du moyen d'identification électronique partenaire de Yousign. En cas de succès, une preuve d'authentification, valable pour la transaction en cours, est générée.

La demande de certificat transmise à l'AC comprend au minimum le nom et le prénom du porteur ainsi que la preuve d'authentification du porteur.

5.2 - Traitement d'une demande de certificat

5.2.1 - Exécution des processus d'identification et de validation de la demande

Le porteur doit s'authentifier fortement avec le moyen d'identification qui lui a été remis par l'AC. Suite à cette authentification, le porteur peut déclencher le processus de signature.

L'AC sur la base de l'authentification forte réussie par le porteur peut déterminer quelles sont les informations d'identité à porter dans le certificat.

Le processus de signature permet de vérifier la validité de la preuve d'authentification et l'habilitation du signataire à recevoir un certificat de signature à la volée. En particulier, lorsque le porteur a réalisé une demande de révocation ou si son moyen d'authentification a été compromis ou est suspecté de compromission, il ne peut plus obtenir de certificat avant d'avoir renouvelé son enregistrement selon les mêmes modalités que l'enregistrement initial.

Lorsque ces contrôles sont réalisés avec succès, l'AC est en mesure de générer une nouvelle bi-clé et un nouveau certificat.

5.2.2 - Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AC retourne une erreur au système de signature en décrivant si possible l'erreur survenue.

5.2.3 - Durée d'établissement du certificat

Le certificat est émis immédiatement par l'AC une fois la demande acceptée.

5.3 - Délivrance du certificat

5.3.1 - Actions de l'AC concernant la délivrance du certificat

Suite à l'acceptation de la demande, l'AC déclenche les processus de génération et de préparation des différents éléments du porteur : la bi-clé du porteur, ainsi que le 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 clés et des certificats et les mesures de sécurité mises en œuvre sont précisées aux chapitres [Mesures de sécurité non techniques3](#)- et [Mesures de sécurité techniques3](#)- ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre [Mesures de sécurité procédurales3](#)).

5.3.2 - Notification par l'AC de la délivrance du certificat au porteur

L'AC n'envoie pas notification spécifique au porteur, c'est le processus de signature qui indique l'avancement de la procédure au signataire.

5.4 - Acceptation du certificat

5.4.1 - Démarche d'acceptation du certificat

L'acceptation d'un certificat émis par l'AC est tacite dès lors que le porteur valide la création de la signature dans le système de signature Yousign. Cette disposition est portée à la connaissance du porteur dans les conditions générales d'utilisations du service, acceptées explicitement lors de l'enregistrement.

Avant cette validation, le porteur peut refuser la génération du certificat en interrompant le processus de signature. Si la bi-clé avait déjà été générée, cette dernière est détruite de manière automatique par un processus technique.

5.4.2 - Publication du certificat

L'AC ne publie pas les certificats de signature des porteurs. Néanmoins les certificats sont insérés dans les documents signés, ce qui permet au porteur de le consulter et aux utilisateurs de vérifier la signature.

5.4.3 - Notification par l'AC aux autres entités de la délivrance du certificat

Sans objet.

5.5 - Usages de la bi-clé et du certificat

5.5.1 - Utilisation de la clé privée et du certificat par le porteur

La clé privée et le certificat associé ne sont utilisés que dans le cadre du processus de signature Yousign.

5.5.2 - Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Le certificat du porteur sert uniquement à l'utilisateur à la vérification de la validité de la signature d'un document signé par le porteur. Les obligations spécifiées au [Interprétations contractuelles et garanties2](#) doivent être respectées.

5.6 - Renouvellement d'un certificat

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 des porteurs, garantit qu'un certificat correspondant à une bi-clé existante ne peut pas être renouvelé au sens du [RFC3647].

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

Se référer au [Demande de certificat](#).

5.8 - Modification du certificat

Sans objet.

5.9 - Révocation et suspension des certificats

5.9.1 - Causes possibles d'une révocation

5.9.1.1 - Certificats des porteurs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur :

- les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le porteur n'a pas respecté ses obligations découlant de la PC de l'AC ou des CGU correspondantes ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ;
- la personne morale en lien avec le porteur demande la révocation, par exemple en cas de fin de la relation avec celui-ci ;
- la clé privée du porteur est suspectée de compromission, est compromise ou, est perdue (éventuellement les données d'activation associées) ;
- le moyen d'authentification du porteur pour autoriser une transaction de signature a été compromis ou suspecté de compromission ;
- la fin programmée d'utilisation de l'algorithme de condensat mis en œuvre ;
- Le certificat de l'AC a été révoqué ;
- La cessation d'activité de l'AC.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

S'agissant de certificats émis à la volée à partir du dossier d'enregistrement initial, il est possible que le porteur ne dispose pas de certificat en cours de validité au moment où l'un des événements cités ci-dessus se produit. Dans ce cas, et tant que son accès à la fonction de signature Yousign est valide, le porteur a l'obligation de faire une demande de révocation dans les mêmes conditions que s'il avait un certificat valide ce qui bloquera toute nouvelle émission de certificat avant la réalisation d'un nouvel enregistrement.

5.9.1.2 - 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 / 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 (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Fin programmée d'utilisation de l'algorithme de condensat mis en œuvre ;

- cessation d'activité de l'entité opérant la composante.

5.9.2 - Origine d'une demande de révocation

5.9.2.1 - Certificats de porteurs

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

- le porteur du certificat ;
- pour le cas d'un certificat émis en lien avec une personne morale, le représentant légal de la société ou le signataire de la demande de certificat représentant la personne morale ;
- l'AC émettrice du certificat ou l'une de ses composantes (AE).

5.9.2.2 - 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. Dans ce cas, une demande de révocation est formulée et signée par le responsable du Comité de Direction Technique. Cette demande inclue obligatoirement les informations du certificat à révoquer et la raison de la révocation.

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

5.9.3 - Procédure de traitement d'une demande de révocation

5.9.3.1 - Révocation d'un certificat porteur

Les exigences d'identification et de validation d'une demande de révocation, effectuée par la fonction de gestion des révocations, sont décrites au chapitre [Identification et validation d'une demande de révocation2](#).

La demande doit être faite par téléphone ou par courriel, par l'une des personnes identifiées au chapitre [Révocation et suspension des certificats](#) :

- Révocation via téléphone : le demandeur contacte Yousign par téléphone et demande la révocation d'un certificat. Afin de s'assurer de l'identité du demandeur, une série de deux questions lui est posée. Ces questions sont fondées sur les informations en possession de Yousign. La validation de la demande est effective après la réception d'une confirmation obtenue via un courrier électronique.
- Révocation par courriel : le demandeur contacte Yousign par message électronique et demande la révocation d'un certificat. Afin de s'assurer de l'identité du demandeur, Yousign prend contact avec le demandeur par téléphone et pose une série de 2 questions aléatoires concernant son identité. Ces questions sont fondées sur les informations en possession de Yousign. La validation de la demande est effective après cette confirmation par téléphone.

Les coordonnées de Yousign pour effectuer une révocation de certificat sont indiquées sur le site Yousign : <https://www.yousign.com>

Les informations suivantes doivent être données dans la demande de révocation de certificat :

- l'identité du porteur ;
- si le porteur possède un certificat valide au moment de la demande, une information permettant de le retrouver rapidement et sans erreur (n° de série, date de délivrance...);
- la cause de révocation.

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

par l'AC.

Le demandeur de la révocation sera informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le porteur du certificat n'est pas le demandeur, il sera également informé de la révocation effective de son certificat.

Dans le cas où la demande de révocation concerne un certificat qui a expiré au moment du traitement de la demande par Yousign, un mail sera retourné au porteur lui indiquant que :

- la révocation ne peut avoir lieu du fait du statut expiré du certificat ;
- de par ce statut expiré, le certificat ne peut plus être utilisé dans une transaction de signature ;
- un nouvel enregistrement auprès d'une AE est nécessaire afin de retrouver la faculté de signer via un nouveau certificat émis à la volée.

Lorsque la demande de révocation ne concerne pas un certificat spécifique (par exemple en cas de compromission du moyen d'identification entre deux transactions de signature), un mail sera retourné au porteur lui indiquant que :

- sa demande a été prise en compte et qu'aucune nouvelle signature ne sera permise avec son moyen d'identification actuel ;
- un nouvel enregistrement auprès d'une AE est nécessaire afin de retrouver la faculté de s'authentifier et de signer.

5.9.3.2 - Révocation d'un certificat d'une composante de l'IGC

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

Cela ne concerne que les certificats finaux encore en cours de validité au moment de la révocation du certificat d'AC.

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

5.9.4 - Délai accordé au porteur pour formuler la demande de révocation

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

Une demande de révocation n'est recevable que durant la durée de vie du certificat électronique, qui est de quelques minutes pour un certificat éphémère. Au-delà de cette période, le certificat est expiré et il n'est plus possible de le révoquer.

5.9.5 - Délai de traitement par l'AC d'une demande de révocation

5.9.5.1 - Révocation d'un certificat porteur

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 porteur sera traitée :

- Si le certificat n'a pas expiré au moment du traitement de la révocation, et
- dans un délai inférieur à 24h, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

5.9.5.2 - 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 évènement 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 liste de révocation 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.

5.9.6 - Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur 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 ou le service OCSP.

5.9.7 - Fréquence d'établissement des LCR

Les LCR sont générées, à minima, toutes les 24h.

5.9.8 - Délai maximum de publication d'une LCR

Les LCR sont publiées le plus rapidement possible après leurs établissements. Au maximum le délai de publication sera de 30 minutes.

Le service OCSP prend en compte sans délai la révocation des certificats.

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

Voir [Fonction d'information sur l'état des certificats](#).

5.9.10 - Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Voir [Révocation et suspension des certificats](#).

5.9.11 - Autres moyens disponibles d'information sur les révocations

Sans objet.

5.9.12 - Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de porteur, 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 du chapitre [Révocation et suspension des certificats](#) ci-dessus, la révocation suite à une compromission de la clé privée fera l'objet d'une information diffusée clairement sur le site Internet www.yousign.fr. 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.

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.

5.9.13 - Suspension des certificats

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

5.10 - Fonction d'information sur l'état des certificats

5.10.1 - Caractéristiques opérationnelles

Yousign 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 le chapitre [Entités chargées de la mise à disposition des informations](#)², et à l'adresse contenue dans les certificats émis.

Le service OCSP est disponible à l'adresse <http://ocsp.yousign.fr>, qui est aussi indiquée dans les certificats émis.

5.10.2 - Disponibilité de la fonction

La fonction d'information sur l'état des certificats (LCR et OCSP) 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%.

5.11 - Fin de la relation entre le porteur et l'AC

En cas de fin de relation contractuelle entre l'AC et le porteur avant la fin de la période de validité du certificat, pour une raison ou pour une autre, le certificat du porteur est révoqué et l'AC ne délivrera pas de nouveau certificat au porteur.

5.12 - Séquestre de clé et recouvrement

Les clés privées des porteurs sont exclusivement des clés de signature, elles ne sont pas séquestrées.

Les clés privées d'AC et des composantes de l'IGC ne sont pas séquestrées.

6 - Mesures de sécurité non techniques

Les exigences présentées dans ce chapitre respectent le RGS et résultent de l'analyse de risques et de la stratégie de gestion de risques définie par le Comité de Direction Technique de Yousign.

6.1 - Mesures de sécurité physique

6.1.1 - Situation géographique et construction des sites

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

6.1.2 - 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 doivent s'authentifier et disposer des droits nécessaires pour accéder physiquement et logiquement à l'ensemble des ressources et

fonctionnalités de l'IGC.

Tous les accès physiques sont tracés (enregistrement vidéo et surveillance de l'ouverture des baies).

6.1.3 - 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.

6.1.4 - Vulnérabilité aux dégâts des eaux

L'hébergement est réalisé dans une zone non inondable.

6.1.5 - 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.

6.1.6 - 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.

S'il y a utilisation de documents papiers, ou de supports amovibles telles 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 accessible par le porteur autorisé.

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.

6.1.7 - 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.

6.1.8 - 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 événement 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 protégées contre les risques d'incendies et d'inondation.

6.2 - Mesures de sécurité procédurales

6.2.1 - Rôles de confiance

Le Comité technique Yousign 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'événements 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 (AC ou AE ou OCSP) 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.
- **Officier d'enregistrement** : il s'agit de personnes en charge de traiter les dossiers de demande de certificats. Ces personnes sont formées à la validation des justificatifs fournis par le demandeur notamment les justificatifs d'identité.
- **Officier de révocation** : il s'agit de personnes en charge de traiter les demandes de révocation formulées par les porteurs.
- **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.
- **Exploitant** : 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'événements 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 porteur 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 (bi-facteur) est mis en place.

6.2.2 - 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](#)).

6.2.3 - Identification et authentification pour chaque rôle

Toutes les personnes opérant un rôle de confiance au sein de l'IGC Yousign 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 de la sécurité 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 (authentification bi-facteur). 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.

6.2.4 - 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.

6.3 - Mesures de sécurité vis-à-vis du personnel

6.3.1 - 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 Yousign.

Le personnel amené à travailler au sein de l'IGC Yousign, 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.

6.3.2 - Procédures de vérification des antécédents

Yousign 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 Yousign une copie du bulletin n°3 de leur casier judiciaire. Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches. Ces vérifications seront menées préalablement à l'affectation à un rôle de confiance.

6.3.3 - 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.

6.3.4 - 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.

Le personnel est régulièrement (annuellement) formé aux pratiques à l'état de l'art de la sécurité informatique et est formé à la gestion et à la remontée des incidents de sécurité.

6.3.5 - Fréquence et séquence de rotation entre différentes attributions

La présente PC ne formule aucune exigence sur le sujet.

6.3.6 - 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 Yousign. Celles-ci sont plus ou moins importantes en fonction de l'impact que peut avoir une action non autorisée.

6.3.7 - 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 Yousign. Si un prestataire externe doit intervenir sur une composante de l'IGC, ceci est fait avec l'accord préalable du responsable de sécurité, et sous sa supervision. Toutes les interventions réalisées sont journalisées.

6.3.8 - 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 lui est remis la ou les politique(s) de sécurité l'impactant.

6.4 - Procédure de constitution des données d'audit

6.4.1 - 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 évènements 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 ;
- traces d'activité (*logs*) des pare-feux et des routeurs ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

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

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

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

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

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

- type de l'évènement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement (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'évènement (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'évènement, 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'évènement ;
- toute information caractérisant l'évènement (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'évènement.

6.4.2 - Fréquence de traitement des journaux d'évènements

Cf. chapitre ci-dessous.

6.4.3 - Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au maximum 90 jours. Ils sont archivés au minimum sous un délai de 3 mois.

6.4.4 - Protection des journaux d'évènements

Sur site, les journaux d'évènements ne sont rendus accessibles qu'au personnel de confiance.

6.4.5 - Procédure de sauvegarde des journaux d'évènements

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

6.4.6 - Système de collecte des journaux d'évènements

La collecte des journaux d'évènements se fait au travers d'un système de centralisation des logs.

6.4.7 - Notification de l'enregistrement d'un évènement au responsable de l'évènement

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

6.4.8 - Évaluation des vulnérabilités

Yousign 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 lors qu'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.

6.5 - Archivage des données

6.5.1 - Types de données à archiver

Des dispositions en matière d'archivage sont mises en place par l'AC. 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 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 ;
- les dossiers d'enregistrement ;
- la trace d'acceptation du certificat par le porteur.

6.5.2 - Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est 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 est portée à la connaissance du porteur dans les conditions générales d'utilisation du service.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat peut être présenté par l'AC en cas de sollicitation par les autorités habilitées. Ce dossier permet de retrouver l'identité réelle des personnes physiques désignées dans les certificats émis par l'AC.

Certificats, LAR et LCR émis par l'AC

Les certificats de porteurs et d'AC, ainsi que les LCR / LAR produites, sont archivés pendant au moins 7 années après leur expiration.

Journaux d'évènements

Les journaux d'évènements traités au chapitre [Procédure de constitution des données d'audit2](#) sont archivés pendant 17 ans. L'archivage est réalisé dans un environnement sécurisé, permettant de garantir l'intégrité des données au cours du temps.

6.5.3 - Protection des archives

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

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

6.5.4 - Procédure de sauvegarde des archives

L'archivage est réalisé soit de manière automatique, soit de manière manuelle par du personnel autorisé. L'archivage est chiffré en AES256 puis envoyé hors site dans un environnement sécurisé. Ces archives sont dupliquées sur plusieurs datacenters distincts afin de garantir leur disponibilité.

6.5.5 - Exigences d'horodatage des données

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

Les composants en charge de la fonction de révocation sont synchronisés quotidiennement avec une source de temps UTC.

6.5.6 - Système de collecte des archives

Les systèmes de collecte des archives de Yousign sont internes.

6.5.7 - 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.

6.6 - 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 du certificat de l'AC doit toujours 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 plus longue durée de vie des certificats signés par la clé privée correspondante. Ce délai sera au minimum de trois mois avant l'expiration du certificat de l'AC.

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.

6.7 - Reprise suite à la compromission et sinistre

6.7.1 - Procédures de remontée et de traitement des incidents et des compromissions

L'IGC Yousign 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'évènement 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 Yousign, via une notification par courrier électronique à l'ensemble des clients.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors le responsable du Comité de Direction Technique publiera l'information via le site public et notifiera par courrier électronique l'ensemble des clients de Yousign. Tous les certificats concernés seront alors révoqués.

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.

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

L'hébergeur de Yousign 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. Yousign dispose d'une procédure permettant de réinitialiser l'environnement logiciel. Ce plan est testé au minimum une fois tous les 2 ans.

6.7.3 - 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 :

- informer tous les porteurs
- indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.
- Informer l'organe de contrôle national dans les vingt-quatre heures (voir [Reprise suite à la compromission et sinistre](#))

6.7.4 - Capacités de continuité d'activité suite à un sinistre

L'IGC Yousign 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](#)).

6.8 - 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.

L'AC communiquera au point de contact identifié sur <http://ssi.gouv.fr>, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC communiquera à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet événement. L'AC tiendra informée l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

6.8.1 - 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 des porteurs et des informations relatives aux certificats).
- Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LAR et LCR, maintien du service OCSP), 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 du porteur est encore valide.
- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire.

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

7 - Mesures de sécurité techniques

Les exigences présentées dans ce chapitre respectent le RGS et résultent de l'analyse de risques et de la stratégie de gestion de risques définie par le Comité de Direction Technique de Yousign.

7.1 - Génération et installation de bi-clés

7.1.1 - Génération des bi-clés

7.1.1.1 - Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé. Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre [Annexe 1 _ Exigences de sécurité du module cryptographique de l'AC](#).

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 [Révocation et suspension des certificats](#)), 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 Yousign occupant des rôles de confiance. De plus, un témoin valide la bonne mise en œuvre de la cérémonie.

7.1.1.2 - Clés des porteurs

La génération des clés des porteurs est effectuée dans un environnement sécurisé. Les bi-clés des porteurs sont générées directement dans le dispositif de création de signature conforme aux exigences du chapitre [Annexe 1 _ Exigences de sécurité du module cryptographique de l'AC1](#)- ci-dessous.

Ce dispositif est détenu et opéré par Yousign.

7.1.2 - Transmission de la clé privée à son propriétaire

La clé privée de signature du porteur n'est pas transmise à son propriétaire. Les modalités de protection et de gestion de cette clé privée sont détaillées dans [Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques](#).

7.1.3 - Transmission de la clé publique à l'AC

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

7.1.4 - 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 exposée au chapitre [Entités chargées de la mise à disposition des informations](#).

7.1.5 - Tailles des clés

Les clés d'AC ont ces caractéristiques :

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

Les clés des certificats porteurs et OCSP ont ces caractéristiques :

- Algorithme utilisé : RSA.
- Taille minimale des clés : 2048 bits.

7.1.6 - 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 1_ 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.

7.1.7 - Objectifs d'usage de la clé

L'utilisation des clés privées d'AC, des porteurs et des certificats associés est strictement limitée aux usages précisés en [Usage des certificats](#).

7.2 - Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

7.2.1 - Standards et mesures de sécurité pour les modules cryptographiques

Les modules cryptographiques, utilisés par l'AC et les porteurs, pour la génération et la mise en œuvre de leurs clés de signature, sont des modules cryptographiques répondant aux exigences du chapitre [Annexe 1_ Exigences de sécurité du module cryptographique de l'AC](#) ci-dessous. Yousign utilise des HSM qualifiés et s'assure de leur sécurité, physique et logicielle. Yousign héberge ce matériel dans des zones d'accès contrôlées et protégées contre les pannes électriques, les inondations ainsi que les incendies.

Yousign 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.

7.2.2 - Contrôle de la clé privée par plusieurs personnes

7.2.2.1 - Clés d'AC

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 3 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 de contrôle « M of N » : un quorum de 2 personnes parmi 3 est nécessaire pour autoriser une opération sur les clés.

7.2.2.2 - Clés porteur

La clé privée du porteur est sous son contrôle exclusif :

- Le processus technique garantit que la clé privée générée pour le porteur durant une transaction de signature est la seule à pouvoir être utilisée et ne peut être utilisée par aucun autre processus ;

- Le personnel Yousign ne dispose pas des éléments permettant d'accéder et d'utiliser la clé privée d'un porteur durant le processus de signature ;
- La mise en œuvre de la clé privée est liée à l'authentification forte préalable du porteur sur le portail Yousign. Cette authentification se fait via le moyen remis dans le cadre de la phase d'identification décrite au paragraphe [Validation initiale de l'identité](#).

7.2.3 - Séquestre de la clé privée

Les clés privées des AC et des porteurs ne font pas l'objet de séquestre.

7.2.4 - Copie de secours de la clé privée

7.2.4.1 - Clés d'AC

Les clés privées d'AC font l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences du chapitre [Annexe 1 _ Exigences de sécurité du module cryptographique de l'AC1](#)- ci-dessous, 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 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 d'AC ne soient à aucun moment en clair en dehors du module cryptographique.

7.2.4.2 - Clés porteur

Les clés privées des porteurs ne font pas l'objet de copie de secours.

7.2.5 - Archivage de la clé privée

Les clés privées d'AC et des porteurs ne sont jamais archivées.

7.2.6 - Transfert de la clé privée vers / depuis le module cryptographique

La génération des clés privées d'AC et des porteurs se fait dans le module cryptographique. Le transfert vers / depuis le module cryptographique ne se fait que pour la génération des copies de sauvegardes des clés d'AC. Ceci se fait sous forme chiffrée, conformément aux exigences du chapitre [Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques](#).

7.2.7 - Stockage de la clé privée dans un module cryptographique

Le stockage des clés privées d'AC est réalisé dans un module cryptographique répondant aux exigences des chapitres [Annexe 1 _ Exigences de sécurité du module cryptographique de l'AC](#) et [Annexe 2 _ Exigences de sécurité du dispositif du système de signature](#). Cependant, dans le cas de leurs copies de secours, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences du chapitre [Exigences sur la certification](#).

Yousign met les moyens en place afin de garantir que les clés privées du matériel cryptographique ne sont pas compromises pendant leur stockage ou leur transport.

7.2.8 - Méthode d'activation de la clé privée

7.2.8.1 - Clés d'AC

L'activation des clés privées d'AC se fera dans un module cryptographique et sera contrôlée via des données d'activation (cf. chapitre [Données d'activation](#)). Pour l'AC, les porteurs de secrets devront être présents afin de réaliser l'activation.

7.2.8.2 - Clés porteur

La clé privée d'un porteur est active à partir du moment de sa génération. La génération de la bi-clé ne peut avoir lieu qu'après authentification forte du porteur, la clé privée n'est générée et activée que si cette authentification a réussi.

7.2.9 - Méthode de désactivation de la clé privée

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

Ces conditions de désactivation répondent aux exigences définies dans le chapitre [Annexe 1 _ Exigences de sécurité du module cryptographique de l'AC](#) pour le niveau de sécurité considéré.

La clé privée d'un porteur n'est pas désactivée mais directement détruite à la fin de son utilisation (voir [Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques](#)).

7.2.10 - Méthode de destruction des clés privées

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

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

7.2.11 - Niveau de qualification du module cryptographique et des dispositifs de création de signature

Les modules cryptographiques utilisés par Yousign satisfont aux critères d'évaluation de l'ANSSI exposés dans [ANSSI_PSCO].

7.3 - Autres aspects de la gestion des bi-clés

7.3.1 - Archivage des clés publiques

Voir [Archivage des données](#).

7.3.2 - 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 des porteurs qu'elle émet. Les clés de signatures de l'AC auront une durée de vie de maximum 10 ans.

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

7.4 - Données d'activation

7.4.1 - Génération et installation des données d'activation

7.4.1.1 - Clés de l'AC

Les clés de l'AC sont générées et conservées dans un module cryptographique matériel de l'infrastructure de l'IGC. La génération et l'installation des données d'activation du module cryptographique 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.

7.4.1.2 - Clés des porteurs

Les données d'activation du porteur sont générées par le moyen d'identification électronique qui lui est remis durant son enregistrement initial.

7.4.2 - Protection des données d'activation

7.4.2.1 - Clés de l'AC

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

7.4.2.2 - Clés des porteurs

Les éléments d'activation sont propres aux porteurs et ne sont valables que pour un processus de signature précis. Le porteur doit reprendre son authentification pour chaque transaction de signature.

7.4.3 - Autres aspects liés aux données d'activation

Sans objet.

7.5 - Mesures de sécurité des systèmes informatiques

7.5.1 - 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 ;
- Revue périodique des habilitations des personnels sur les systèmes informatiques ;
- Surveillance continue afin de détecter toute tentative d'accès aux systèmes informatiques ;
- Veille sécurité assurant l'application régulière des correctifs de sécurité des systèmes informatiques, et la prise en compte des vulnérabilités critiques dans un délai de 48 heures.
- Politique de durcissement des systèmes informatiques ;
- Protection du réseau ;

7.5.2 - Niveau de qualification des systèmes informatiques

Sans objet.

7.6 - Mesures de sécurité liées au développement des systèmes

7.6.1 - Mesures liées à la gestion de la sécurité

Tous les développements réalisés par Yousign 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, Yousign 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.

7.6.2 - Niveau d'évaluation sécurité du cycle de vie des systèmes

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

7.7 - Mesures de sécurité réseau

Les AC soumises à la présente PC, sont des AC en ligne déployées dans un environnement physiquement sécurisé et périodiquement audités. Des dispositifs de protection du réseau (pare-feux, solutions de détection d'intrusion (IDS), VPN) contribuent à la sécurité du réseau. Les flux non explicitement autorisés sont interdits par défaut.

Le réseau d'administration des systèmes informatiques est logiquement séparé du réseau d'exploitation. Des postes d'administration, sécurisés spécifiquement, sont dédiés à l'administration système.

La redondance des accès sur les services exposés sur Internet est assurée.

La configuration des équipements réseau est périodiquement auditée. Des tests d'intrusion sont réalisés de façon périodique.

7.8 - Horodatage Système de datation

Un horodatage est réalisé sur l'ensemble des éléments archivés.

Voir [Archivage des données](#).

8 - Profil des certificats et des LCR

8.1 - Profils de certificats

8.1.1 - Certificats de l'ACR

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	20 ans
Subject	CN=YOUSIGN SAS - ROOT2 CA, OU=794513986, O=YOUSIGN SAS, L=CAEN, ST=CALVADOS, C=FR
Longueur des clés de l'AC	4096 bits

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	Hash sha1 de la clé publique du certificat
Subject Key Identifier	O	N	Hash sha1 de la clé publique du certificat
Key Usage	O	O	Key_CertSign CrL_Sign
CRL Distribution Points	O	N	http://crl.yousign.fr/crl/yousignsasroot2ca.crl http://crl2.yousign.fr/crl/yousignsasroot2ca.crl http://crl3.yousign.fr/crl/yousignsasroot2ca.crl

Basic Constraints	O	O	CA:true Longueur de chemin : aucune
--------------------------	---	---	--

8.1.2 - Certificats de l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE 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 – QUALIFIED SIGNATURE CA, OU=0002 794513986, O=YOUSIGN SAS, OI=NTRFR-794513986, C=FR
Longueur des clés de l'AC	4096 bits

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	Hash SHA-1 de la clé publique de l'AC Racine
Subject Key Identifier	O	N	Hash SHA-1 de la clé publique du certificat
Key Usage	O	O	Key_CertSign Crl_Sign
CRL Distribution Points	O	N	http://crl.yousign.fr/crl/yousignsasroot2ca.crl http://crl2.yousign.fr/crl/yousignsasroot2ca.crl http://crl3.yousign.fr/crl/yousignsasroot2ca.crl
Basic Constraints	O	O	CA:true Longueur de chemin : aucune

Authority Information Access	O	N	Certificat autorité : http://crl.yousign.fr/yousignsasroot2ca.crt http://crl2.yousign.fr/yousignsasroot2ca.crt http://crl3.yousign.fr/yousignsasroot2ca.crt
-------------------------------------	---	---	--

8.1.3 - Certificats éphémère de signature

Champs de base	Valeur
Version	2
Numéro de série	Défini par l'outil
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS – QUALIFIED SIGNATURE CA, OU=0002 794513986, O=YOUSIGN SAS, OI=NTRFR-794513986, C=FR
Validity	15 minutes
Subject	Se reporter au chapitre 3.1.1
Longueur des clés	2048 bits

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	Hash SHA-1 de la clé publique de l'ACI QUALIFIED SIGNATURE CA
Subject Key Identifier	O	N	Hash SHA-1 de la clé publique du certificat
Key Usage	O	O	Non Repudiation
Extended Key Usage	O	N	MS Document Signing Adobe PDF Signing
Certificate Policies	O	N	1.2.250.1.302.1.11.1.0 URL de publication : http://yousign.fr/fr/public/document

CRL Distribution Points	O	N	http://crl.yousign.fr/crl/yousignsasqualifsignca.crl http://crl2.yousign.fr/crl/yousignsasqualifsignca.crl http://crl3.yousign.fr/crl/yousignsasqualifsignca.crl
Basic Constraints	O	O	CA:false
Authority Information Access	O	N	Certificat autorité : http://crl.yousign.fr/yousignsasqualifsignca.crt http://crl2.yousign.fr/yousignsasqualifsignca.crt http://crl3.yousign.fr/yousignsasqualifsignca.crt Répondeur OCSP : http://ocsp.yousign.fr
qcStatements	O	N	esi4- qcStatement-1 = id-etsi-qcsQcCompliance esi4- qcStatement-6 = id-etsi-qct-esign

8.1.4 - Certificats du service OCSP

Champs de base	Valeur
Version	2
Numéro de série	Défini par l'outil
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS – QUALIFIED SIGNATURE CA, OU=0002 794513986, O=YOUSIGN SAS, OI=NTRFR-794513986, C=FR
Validity	5 ans
Subject	CN=OCSP Service N Yousign QUALIFIED SIGNATURE CA, SERIAL NUMBER= <date de lancement de génération du certificat>, OU=0002 794513986, O=YOUSIGN SAS, OI=NTRFR-794513986, C=FR N est un numéro fixé par Yousign
Longueur des clés	2048 bits

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	Hash SHA-1 de la clé publique de l'ACI QUALIFIED SIGNATURE CA
Subject Key Identifier	O	N	Hash SHA-1 de la clé publique du certificat
Key Usage	O	O	Digital Signature
Extended Key Usage	O	N	id-kp-OCSPSigning
Certificate Policies	O	N	1.2.250.1.302.1.12.1.0 URL de publication : http://yousign.fr/fr/public/document
id-ocsp-nocheck	O	N	NULL

Basic Constraints	O	O	CA:false
CRL Distribution Points	O	N	http://crl.yousign.fr/crl/yousignsasqualifsignca.crl http://crl2.yousign.fr/crl/yousignsasqualifsignca.crl http://crl3.yousign.fr/crl/yousignsasqualifsignca.crl
Authority Information Access	O	N	Certificat autorité : http://crl.yousign.fr/yousignsasqualifsignca.crt http://crl2.yousign.fr/yousignsasqualifsignca.crt http://crl3.yousign.fr/yousignsasqualifsignca.crt

8.2 - Liste de Certificats Révoqués

Champs de base	Valeur
Version	1
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS – QUALIFIED SIGNATURE CA, OU=0002 794513986, O=YOUSIGN SAS, OI=NTRFR-794513986, C=FR
Validité	7 jours
Revoked Certificates	Serial Number Revocation Date <i>La CRL contient les certificats expirés sans limitation de durée</i>

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	Hash SHA-1 de la clé publique de l'ACI QUALIFIED SIGNATURE CA
CRL Number	O	N	Numéro de séquence défini par l'outil
ExpiredCertsOnCRL	O	N	Date à partir de laquelle tous les certificats révoqués sont conservés dans la CRL. Il s'agit de la date de début de validité du certificat de l'AC émettrice.

8.3 - Répondeur OCSP

8.3.1 - Requêtes OCSP

Les requêtes OCSP acceptées sont celles qui respectent le format décrit par la RFC 6960.

Le service OCSP ignore la signature si elle est présente.

Les requêtes attendues sont de la forme :

Champ	Commentaires	Valeur attendue
version	Version de la requête	0 (version 1)

requestorName	Nom de l'émetteur de la requête	Valeur absente ou ignorée
requestList <ul style="list-style-type: none"> • reqCert • singleRequestExtensions 	Liste des certificats à vérifier	Un ou plusieurs identifiants de certificats sont acceptés. La valeur des extensions est ignorée
requestExtensions	Extensions	Seule l'extension Nonce est prise en compte, les autres sont ignorées

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

8.3.2 - Réponses OCSP

Les réponses OCSP respectent le format décrit par la RFC 6960. Elles sont signées par le service sauf si une erreur s'est produite (requête rejetée ou échec de traitement). Les certificats révoqués, même ceux expirés, sont signalés révoqués.

Les réponses sont de la forme BasicOCSPResponse :

Champ	Commentaires	Valeur
version	Version de la requête	0 (version 1)
responderID	Nom du répondeur	Hash de la clé publique du répondeur
producedAt	Heure de production de la réponse	Heure de production à la seconde près
responses <ul style="list-style-type: none"> • certID • certStatus • revocationDate • thisUpdate 	Statut des certificats identifiés dans la requête	Le statut du certificat est le statut actuel du certificat (thisUpdate est la date courante). La date de révocation est fournie le cas échéant, mais pas la raison de révocation
responseExtensions	Extensions	L'extension Nonce fournie par un émetteur est renvoyée dans la réponse

9 - Audit de conformité et autres évaluations

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification eIDAS (selon un processus décrit dans [ANSSI_PSCO]) et, d'autre part, ceux que doit réaliser l'AC afin de s'assurer que l'ensemble de son IGC est bien conforme aux engagements qu'elle prend et aux pratiques qu'elle déclare dans le présent document.

La suite du présent chapitre ne concerne que les audits et évaluations de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

9.1 - Fréquences et ou circonstances des évaluations

Un contrôle de conformité est réalisé avant la mise en service du système et suite à toute modification significative d'une composante de l'IGC. De plus, un audit est réalisé au minimum chaque année.

9.2 - Identités qualifications des évaluateurs

Les audits sont réalisés soit en interne par du personnel de Yousign, soit sous la forme d'une prestation auprès d'acteurs spécialisés. Dans tous les cas, Yousign s'engage à mandater des personnes disposant des compétences en sécurité requises pour auditer et vérifier la conformité du système.

9.3 - Relations entre évaluateurs et entités évaluées

Les contrôleurs sont soit des membres internes de Yousign, soit des auditeurs en contrat de prestation.

9.4 - 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 (procédures opérationnelles, ressources mises en œuvre, etc.) définies dans le présent document.

Pour ce faire, les auditeurs présenteront pour approbation au Comité de Direction Technique la liste des composantes et procédures qui seront auditées.

9.5 - 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 du présent document.

10 - Autres problématiques métiers et légales

10.1 - Tarifs

10.1.1 - Tarifs pour la fourniture ou le renouvellement de certificats

Sans objet.

10.1.2 - Tarifs pour accéder aux certificats

Sans objet.

10.1.3 - Tarifs pour accéder aux LCR et au répondeur OCSP

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

10.1.4 - Politique de remboursement

Sans objet.

10.2 - Responsabilité financière

10.2.1 - Couverture par les assurances

L'AC applique des niveaux de couverture d'assurance raisonnables et a souscrit à cet effet une assurance responsabilité civile au titre de la réalisation de son activité professionnelle.

10.2.2 - Autres ressources

Sans objet.

10.2.3 - Couverture et garantie concernant les entités utilisatrices

Sans objet.

10.3 - Confidentialité des données professionnelles

10.3.1 - Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- Les procédures internes de l'AC,
- les clés privées de l'AC, des composantes et des porteurs de certificats,
- les données d'activation associées aux clés privées d'AC et des porteurs,
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les dossiers d'enregistrement des porteurs,
- les causes de révocations, sauf accord explicite du porteur.

10.3.2 - Informations hors du périmètre des informations confidentielles

Sans objet.

10.3.3 - Responsabilités en termes de protection des informations confidentielles

Yousign applique des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre [Confidentialité des données professionnelles](#). Yousign s'engage à respecter la législation et la réglementation en vigueur sur le territoire français.

10.4 - Protection des données personnelles

10.4.1 - Politique de protection des données personnelles

Yousign 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).

10.4.2 - Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur) ;
- le dossier d'enregistrement du porteur et ses pièces annexes ;
- les données d'activation de la clé privée.

10.4.3 - Informations à caractère non personnel

Sans objet.

10.4.4 - Responsabilité en termes de protection des données à caractères personnelles

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

10.4.5 - Notification et consentement d'utilisation des données personnelles

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

10.4.6 - Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

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

10.4.7 - Autres circonstances de divulgation d'informations personnelles

Sans objet.

10.5 - Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par Yousign 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 Yousign pour assurer son IGC.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, ...) est sanctionnée par le Code de

la propriété intellectuelle.

Le porteur détient tous les droits de propriété intellectuelle sur les informations personnelles contenues dans les certificats porteurs émis par l'AC et dont il est propriétaire.

10.6 - Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent,
- respecter et appliquer les pratiques spécifiées dans de document et leur incombant,
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre [Audit de conformité et autres évaluations](#)3),
- respecter les accords ou contrats qui les lient entre elles ou aux porteurs,
- documenter leurs procédures internes de fonctionnement,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

10.6.1 - Autorités de Certification

L'AC opérée par Yousign est responsable de :

- la validation et de la publication de la PC,
- la conformité des certificats émis vis-à-vis de la présente PC,
- du respect de tous les principes de sécurité par les différentes composantes de l'IGC, et des contrôles afférents.

Sauf à démontrer qu'elle n'a commis aucune faute intentionnelle ou de négligence, Yousign est responsable des préjudices causés aux utilisateurs si :

- les informations contenues dans le certificat ne correspondent pas aux informations d'enregistrement,
- Yousign n'a pas fait procéder à l'enregistrement de la révocation d'un certificat, et n'a pas publié cette information conformément à ses engagements.

10.6.2 - Service d'enregistrement

Se reporter au chapitre 9.6.1.

10.6.3 - Porteurs de certificats

Le porteur a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- protéger ses données d'authentification ;
- accepter les conditions d'utilisation du service de signature Yousign ;
- informer l'AC de toute modification concernant les informations contenues dans son certificat ;
- vérifier que les données présentes dans le certificat du document signé qui lui est remis sont correctes ;
- demander le renouvellement de son certificat avec un délai raisonnable avant son expiration ;
- faire, sans délai, une demande de révocation de son certificat auprès de Yousign en cas de compromission ou de suspicion de compromission de ses données d'authentification.

10.6.4 - Utilisateurs de certificats

Les utilisateurs des certificats doivent :

- vérifier et respecter l'usage pour lequel un certificat a été émis ;
- pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'ACR, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

10.6.5 - Autres participants

Sans objet.

10.7 - Limite de garantie

Sans objet.

10.8 - Limite de responsabilité

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

De plus, dans la mesure des limitations de la loi française, Yousign ne saurait être tenu responsable :

- d'aucune perte financière ;
- d'aucune perte de données ;
- d'aucun dommage indirect lié à l'utilisation d'un certificat ;
- d'aucun autre dommage.

En toute hypothèse, la responsabilité de Yousign sera limitée, tous faits générateurs confondus et pour tous préjudices confondus, au montant payé à Yousign pour l'accès au service de signature et ce, dans le respect et les limites de la loi applicable.

10.9 - Indemnités

Sans objet.

10.10 - Durée et fin anticipée de validité de la PC

10.10.1 - Durée de validité

Cette PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de celle-ci. Une nouvelle version de la PC devient applicable à une date indiquée dans le document de description publié par Yousign.

10.10.2 - Fin anticipée de validité

L'application de la PC peut être interrompue en cas de fin de vie de l'AC (voir [Horodatage _ Système de datation2](#)).

10.10.3 - Effets de la fin de validité et clauses restant applicables

Sans objet.

10.11 - Amendements à la PC

10.11.1 - Procédures d'amendements

10.11.1.1 - Décision

La mise à jour de cette PC se fait sous le contrôle du Comité de Direction Technique. Les événements pouvant demander une évolution du document peuvent être les suivants :

- Evolution majeure du processus d'enregistrement des porteurs ou de gestion des certificats ;
- Intégration de nouvelles conditions réglementaires applicable au service ;
- Modification majeure de l'architecture technique ;
- Fin ou perte d'une certification ou d'une qualification de l'Autorité de Certification.

Le Comité de Direction Technique contrôle que tout projet de modification de la PC reste conforme aux exigences réglementaires, en particulier celles liées au règlement eIDAS. En cas de changement important, Yousign pourra faire appel à une expertise technique ou juridique externe, si elle le juge nécessaire.

10.11.1.2 - Réalisation

La procédure d'amendement de la PC comprend les actions suivantes :

- Organisation d'un Comité de Direction Technique Yousign ;
- Analyse du périmètre et des impacts des modifications ;
- Contact de l'organisme ayant prononcé la certification de l'AC, et si nécessaire de l'ANSSI, afin de s'assurer de la recevabilité des modifications apportées et des modalités de continuité des certifications et qualifications obtenues ;
- Identification des personnes impliquées pour apporter les modifications ;
- Implémentation (technique, organisationnelle, juridique) des modifications décidées ;
- Modification des documents associés ;
- Mise à jour de l'OID si nécessaire (voir au [Amendements à la PC](#)) ;
- Déclenchement d'un audit interne, et si nécessaire externe, sur les parties concernées par les évolutions ;
- Publication des informations associées (selon les modalités du [Responsabilités concernant la mise à disposition des informations devant être publiées2](#)) ;
- Mise en service des modifications réalisées ;
- Archivage des anciennes versions des documents (Politique, Conditions Générales d'Utilisation...).

10.11.2 - Mécanisme et période d'information sur les amendements

Lors de tout changement important impactant la PC, Yousign informera les porteurs au travers d'un communiqué distribué par voie électronique au travers de son site internet. Si besoin, une communication par courrier électronique ou postal pourra être réalisée.

10.11.3 - Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID,

afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences. En particulier, l'OID de la PC de l'AC doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC) intervient dans les exigences de la présente PC applicable à la famille de certificats considérée.

10.12 - 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 au tribunal de commerce de Caen.

10.13 - Juridictions compétentes

Se rapporter au chapitre [Dispositions concernant la résolution de conflits](#)³.

10.14 - Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre [Annexe 1 _ Exigences de sécurité du module cryptographique de l'AC1](#) ci-dessous.

10.15 - Dispositions diverses

10.15.1 - Accord global

Sans objet.

10.15.2 - Transfert d'activités

Sans objet.

10.15.3 - Conséquences d'une clause non valide

Sans objet.

10.15.4 - Application et renonciation

Sans objet.

10.15.5 - Force majeure

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

10.15.6 - Autres dispositions

Sans objet.

11 - Annexe 1 Exigences de sécurité du module cryptographique de l'AC

11.1 - 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 des porteurs, répond aux exigences de sécurité suivantes :

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

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.

11.2 - Exigences sur la certification

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

12 - Annexe 2 Exigences de sécurité du dispositif du système de signature

12.1 - Exigences sur les objectifs de sécurité

Le dispositif de création de signature Yousign répond aux exigences de sécurité suivantes :

- garantir que la génération des bi-clés des porteurs est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une signature qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer la fonction de signature pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;

- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

12.2 - Exigences sur la certification

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