

YOUSIGN - POLITIQUE DE CERTIFICATION DE L'AC "YOUSIGN SAS - SIGN2 CA"

Version 1.0.1 au 14/07/2015

Historique

Version	Date	Rédigé par	Mise à jour
1.0.0	29/04/2015	Antoine Louiset	Création du document
1.0.1	14/07/2015	Antoine Louiset	Modifications mineures

Table des matières

Historique	2
Table des matières	3
1- Introduction.....	12
1.1 Présentation générale	12
1.2 Identification du document.....	12
1.3 Entités intervenant dans l'IGC.....	13
1.3.1 Autorités de certification.....	13
1.3.2 Autorités d'enregistrement.....	13
1.3.3 Responsables de certificats de cachets	13
1.3.4 Utilisateurs de certificats.....	13
1.4 Usage des certificats.....	14
1.4.1 Domaines d'utilisation applicables.....	14
1.4.2 Bi-clés et certificats d'AC et de composantes	14
1.4.3 Domaines d'utilisation interdits	14
1.5 Gestion de la PC.....	15
1.5.1 Entité gérant la PC	15
1.5.2 Point de contact	15
1.5.3 Entité déterminant la conformité d'une DPC avec cette PC	15
1.5.4 Procédure d'approbation de la conformité de la DPC	15
1.6 Définitions et acronymes	15
1.6.1 Acronymes	15
1.6.2 Définitions	16
2- Responsabilités concernant la mise à disposition des informations devant être publiées	20
2.1 Entités chargées de la mise à disposition des informations	20
2.2 Informations devant être publiées.....	20
2.3 Délais et fréquences de publication.....	20
2.4 Contrôle d'accès aux informations publiées	21

3- Identification et authentification	22
3.1 Nommage	22
3.1.1 Types de noms.....	22
3.1.2 Nécessité d'utilisation de noms explicites	22
3.1.3 Pseudonymisation des RCC	Erreur ! Signet non défini.
3.1.4 Règles d'interprétation des différentes formes de nom.....	23
3.1.5 Unicité des noms	23
3.1.6 Identification, authentification et rôle des marques déposées.....	23
3.2 Validation initiale de l'identité	23
3.2.1 Méthode pour prouver la possession de la clef privée	23
3.2.2 Validation de l'identité d'un organisme	24
3.2.3 Validation de l'identité d'un individu	24
3.2.3.1 Enregistrement d'un RCC pour un certificat de cachet à émettre	24
3.2.4 Informations non vérifiées du RCC.....	26
3.2.5 Validation de l'autorité du demandeur.....	26
3.2.6 Certification croisée d'AC.....	26
3.3 Identification et validation d'une demande de renouvellement des clés	26
3.3.1 Identification et validation pour un renouvellement courant	26
3.3.2 Identification et validation pour un renouvellement après révocation.....	26
3.4 Identification et validation d'une demande de révocation.....	26
4- Exigences opérationnelles sur le cycle de vie des certificats	28
4.1 Demande de certificat	28
4.1.1 Origine d'une demande de certificat	28
4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat.....	28
4.2 Traitement d'une demande de certificat	28
4.2.1 Exécution des processus d'identification et de validation de la demande	28
4.2.2 Acceptation ou rejet de la demande.....	29
4.2.3 Durée d'établissement du certificat.....	29
4.3 Délivrance du certificat	29
4.3.1 Actions de l'AC concernant la délivrance du certificat.....	29
4.3.2 Notification par l'AC de la délivrance du certificat au RCC	30
4.4 Acceptation du certificat	30

4.4.1	Démarche d'acceptation du certificat	30
4.4.2	Publication du certificat	30
4.4.3	Notification par l'AC aux autres entités de la délivrance du certificat.....	30
4.5	Usages de la bi-clé et du certificat	30
4.5.1	Utilisation de la clé privée et du certificat par le RCC	30
4.5.2	Utilisation de la clé publique et du certificat par l'utilisateur du certificat.....	31
4.6	Renouvellement d'un certificat.....	31
4.6.1	Causes possibles de renouvellement d'un certificat.....	31
4.6.2	Origine d'une demande de renouvellement.....	31
4.6.3	Procédure de traitement d'une demande de renouvellement.....	31
4.6.4	Notification au RCC de l'établissement du nouveau certificat.....	31
4.6.5	Démarche d'acceptation du nouveau certificat.....	32
4.6.6	Publication du nouveau certificat	32
4.6.7	Notification par l'AC aux autres entités de la délivrance du nouveau certificat.....	32
4.7	Délivrance d'un nouveau certificat suite au changement de la bi-clé	32
4.7.1	Causes possibles de changement d'une bi-clé	32
4.7.2	Origine d'une demande d'un nouveau certificat	32
4.7.3	Procédure de traitement d'une demande d'un nouveau certificat	33
4.7.4	Notification au RCC de l'établissement du nouveau certificat.....	33
4.7.5	Démarche d'acceptation du nouveau certificat.....	33
4.7.6	Publication du nouveau certificat	33
4.7.7	Notification par l'AC aux autres entités de la délivrance du nouveau certificat.....	33
4.8	Modification du certificat.....	33
4.8.1	Causes possibles de modification d'un certificat	33
4.8.2	Origine d'une demande de modification d'un certificat	34
4.8.3	Procédure de traitement d'une demande de modification d'un certificat.....	34
4.8.4	Notification au RCC de l'établissement du certificat modifié	34
4.8.5	Démarche d'acceptation du certificat modifié.....	34
4.8.6	Publication du certificat modifié	34
4.8.7	Notification par l'AC aux autres entités de la délivrance du certificat modifié	34
4.9	Révocation et suspension des certificats	34
4.9.1	Causes possibles d'une révocation.....	34

4.9.2	Origine d'une demande de révocation.....	36
4.9.3	Procédure de traitement d'une demande de révocation	36
4.9.4	Délai accordé au RCC pour formuler la demande de révocation	37
4.9.5	Délai de traitement par l'AC d'une demande de révocation	37
4.9.6	Exigences de vérification de la révocation par les utilisateurs de certificats.....	38
4.9.7	Fréquence d'établissement des LCR.....	38
4.9.8	Délai maximum de publication d'une LCR.....	38
4.9.9	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats	38
4.9.10	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats	38
4.9.11	Autres moyens disponibles d'information sur les révocations	38
4.9.12	Exigences spécifiques en cas de compromission de la clé privée	39
4.9.13	Causes possibles d'une suspension.....	39
4.9.14	Origine d'une demande de suspension.....	39
4.9.15	Procédure de traitement d'une demande de suspension.....	39
4.9.16	Limites de la période de suspension d'un certificat.....	39
4.10	Fonction d'information sur l'état des certificats	39
4.10.1	Caractéristiques opérationnelles	39
4.10.2	Disponibilité de la fonction	40
4.10.3	Dispositifs optionnels	40
4.11	Fin de la relation entre le RCC et l'AC.....	40
4.12	Séquestration de clé et recouvrement	40
4.12.1	Politique et pratiques de recouvrement par séquestration des clés	40
4.12.2	Politique et pratiques de recouvrement par encapsulation des clés de session	41
5-	MESURES DE SÉCURITÉ NON TECHNIQUES.....	42
5.1	Mesures de sécurité physique.....	42
5.1.1	Situation géographique et construction des sites.....	42
5.1.2	Accès physique	42
5.1.3	Alimentation électrique et climatisation.....	42
5.1.4	Vulnérabilité aux dégâts des eaux.....	42
5.1.5	Prévention et protection incendie	43

5.1.6	Conservation des supports.....	43
5.1.7	Mise hors service des supports	43
5.1.8	Sauvegardes hors site.....	43
5.2	Mesures de sécurité procédurales	44
5.2.1	Rôles de confiance.....	44
5.2.2	Nombre de personnes requises par tâche	45
5.2.3	Identification et authentification pour chaque rôle.....	45
5.2.4	Rôles exigeant une séparation des attributions.....	45
5.3	Mesures de sécurité vis-à-vis du personnel	45
5.3.1	Qualifications, compétences et habilitations requises	45
5.3.2	Procédures de vérification des antécédents.....	46
5.3.3	Exigences en matière de formation initiale.....	46
5.3.4	Exigences et fréquence en matière de formation continue.....	46
5.3.5	Fréquence et séquence de rotation entre différentes attributions.....	46
5.3.6	Sanctions en cas d'actions non autorisées.....	47
5.3.7	Exigences vis-à-vis du personnel des prestataires externes	47
5.3.8	Documentation fournie au personnel.....	47
5.4	Procédure de constitution des données d'audit.....	47
5.4.1	Type d'évènements à enregistrer.....	47
5.4.2	Fréquence de traitement des journaux d'évènements	49
5.4.3	Période de conservation des journaux d'évènements	49
5.4.4	Protection des journaux d'évènements	49
5.4.5	Procédure de sauvegarde des journaux d'évènements	49
5.4.6	Système de collecte des journaux d'évènements	49
5.4.7	Notification de l'enregistrement d'un évènement au responsable de l'évènement ...	50
5.4.8	Évaluation des vulnérabilités.....	50
5.5	Archivage des données.....	50
5.5.1	Types de données à archiver	50
5.5.2	Période de conservation des archives.....	50
5.5.3	Protection des archives	51
5.5.4	Procédure de sauvegarde des archives	51
5.5.5	Exigences d'horodatage des données	51

5.5.6	Système de collecte des archives	52
5.5.7	Procédures de récupération et de vérification des archives.....	52
5.6	Changement de clé d'AC	52
5.7	Reprise suite à la compromission et sinistre	52
5.7.1	Procédures de remontée et de traitement des incidents et des compromissions.....	52
5.7.2	Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)	53
5.7.3	Procédures de reprise en cas de compromission de la clé privée d'une composante .	53
5.7.4	Capacités de continuité d'activité suite à un sinistre	54
5.8	Fin de vie de l'IGC	54
5.8.1	Transfert d'activité ou cessation d'activité affectant une composante de l'IGC	54
5.8.2	Cessation d'activité affectant l'AC.....	55
6-	Mesures de sécurité techniques	56
6.1.1	Génération des bi-clés.....	56
6.1.2	Transmission de la clé privée à son propriétaire.....	57
6.1.3	Transmission de la clé publique à l'AC	57
6.1.4	Transmission de la clé publique de l'AC aux utilisateurs de certificats.....	57
6.1.5	Tailles des clés	57
6.1.6	Vérification de la génération des paramètres des bi-clés et de leur qualité	57
6.1.7	Objectifs d'usage de la clé	58
6.2	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques	58
6.2.1	Standards et mesures de sécurité pour les modules cryptographiques	58
6.2.2	Contrôle de la clé privée par plusieurs personnes	58
6.2.3	Séquestration de la clé privée	59
6.2.4	Copie de secours de la clé privée	59
6.2.5	Archivage de la clé privée.....	59
6.2.6	Transfert de la clé privée vers / depuis le module cryptographique	59
6.2.7	Stockage de la clé privée dans un module cryptographique	60
6.2.8	Méthode d'activation de la clé privée.....	60
6.2.9	Méthode de désactivation de la clé privée	60
6.2.10	Méthode de destruction des clés privées	60

6.2.11	Niveau de qualification du module cryptographique et des dispositifs de création de signature	60
6.3	Autres aspects de la gestion des bi-clés	61
6.3.1	Archivage des clés publiques	61
6.3.2	Durées de vie des bi-clés et des certificats	61
6.4	Données d'activation	61
6.4.1	Génération et installation des données d'activation	61
6.4.1.1	Clés de l'AC	61
6.4.1.2	Clés privées de serveurs	61
6.4.2	Protection des données d'activation	62
6.4.2.1	Clés de l'AC	62
6.4.2.2	Clés de serveurs	62
6.4.3	Autres aspects liés aux données d'activation	62
6.5	Mesures de sécurité des systèmes informatiques	62
6.5.1	Exigences de sécurité technique spécifiques aux systèmes informatiques	62
6.5.2	Niveau de qualification des systèmes informatiques	62
6.6	Mesures de sécurité liées au développement des systèmes	63
6.6.1	Mesures liées à la gestion de la sécurité	63
6.6.2	Niveau d'évaluation sécurité du cycle de vie des systèmes	63
6.6.3	Niveau d'évaluation sécurité du cycle de vie des systèmes	63
6.7	Mesures de sécurité réseau	63
6.8	Horodatage / Système de datation	63
7-	Profil des certificats et des LCR	64
7.1	Profils de certificats	64
7.1.1	Certificats de l'ACP	64
7.1.2	Certificats de l'AC « YOUSIGN SAS - SIGN2 CA »	64
7.1.3	Certificats de cachet	65
7.2	Liste de Certificats Révoqués	66
8-	Audit de conformité et autres évaluations	67
8.1	Fréquences et / ou circonstances des évaluations	67
8.2	Identités / qualifications des évaluateurs	67
8.3	Relations entre évaluateurs et entités évaluées	67

8.4	Sujets couverts par les évaluations	67
8.5	Actions prises suite aux conclusions des évaluations	68
9-	Autres problématiques métiers et légales	69
9.1	Tarifs	69
9.1.1	Tarifs pour la fourniture ou le renouvellement de certificats.....	69
9.1.2	Tarifs pour accéder aux certificats	69
9.1.3	Tarifs pour accéder aux LCR	69
9.1.4	Politique de remboursement	69
9.2	Responsabilité financière	69
9.2.1	Couverture par les assurances	69
9.2.2	Autres ressources	69
9.2.3	Couverture et garantie concernant les entités utilisatrices	70
9.3	Confidentialité des données professionnelles	70
9.3.1	Périmètre des informations confidentielles.....	70
9.3.2	Informations hors du périmètre des informations confidentielles.....	70
9.3.3	Responsabilités en termes de protection des informations confidentielles.....	70
9.4	Protection des données personnelles	70
9.4.1	Politique de protection des données personnelles.....	70
9.4.2	Informations à caractère personnel.....	71
9.4.3	Informations à caractère non personnel.....	71
9.4.4	Responsabilité en termes de protection des données à caractères personnelles.....	71
9.4.5	Notification et consentement d'utilisation des données personnelles	71
9.4.6	Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives.....	71
9.4.7	Autres circonstances de divulgation d'informations personnelles	71
9.4.8	Autres circonstances de divulgation d'informations personnelles	72
9.5	Droits sur la propriété intellectuelle et industrielle	72
9.6	Interprétations contractuelles et garanties	72
9.6.1	Autorités de Certification	73
9.6.2	Service d'enregistrement	73
9.6.3	RCC de certificats.....	73
9.6.4	Utilisateurs de certificats.....	74

9.6.5	Autres participants	74
9.7	Limite de garantie.....	74
9.8	Limite de responsabilité	74
9.9	Indemnités.....	75
9.10	Durée et fin anticipée de validité de la PC	75
9.10.1	Durée de validité	75
9.10.2	Fin anticipée de validité.....	75
9.10.3	Effets de la fin de validité et clauses restant applicables.....	75
9.11	Amendements à la PC	75
9.11.1	Procédures d'amendements	75
9.11.2	Mécanisme et période d'information sur les amendements.....	75
9.11.3	Circonstances selon lesquelles l'OID doit être changé.....	76
9.12	Dispositions concernant la résolution de conflits	76
9.13	Juridictions compétentes	76
9.14	Conformité aux législations et réglementations	76
9.15	Dispositions diverses	76
9.15.1	Accord global.....	76
9.15.2	Transfert d'activités.....	76
9.15.3	Conséquences d'une clause non valide.....	77
9.15.4	Application et renonciation.....	77
9.15.5	Force majeure.....	77
9.15.6	Autres dispositions	77
10-	Annexe 1 : Exigences de sécurité du module cryptographique de l'AC	78
10.1	Exigences sur les objectifs de sécurité	78
10.2	Exigences sur la certification	78
11-	Annexe 2 : Exigences de sécurité du dispositif du système de signature	79
11.1	Exigences sur les objectifs de sécurité	79
11.2	Exigences sur la certification	79

1-Introduction

1.1 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 décrit la Politique de Certification (PC) de l'Autorité de Certification « YOUSIGN SAS - SIGN2 CA ». Ce document regroupe l'ensemble des règles, exigences et engagements de Yousign dans le cadre de la mise en place, du fonctionnement et du cycle de vie de l'AC « YOUSIGN SAS - SIGN2 CA », tant sur le plan des exigences de sécurité techniques qu'organisationnelles.

L'AC « YOUSIGN SAS - SIGN2 CA » ne peut être utilisée que pour produire des certificats à usage de signature et pour la signature des Listes des Certificats Révoqués (LCR) correspondantes.

Le certificat de l'AC « YOUSIGN SAS - SIGN2 CA » est intégré à une chaîne de certification qui dépend de l'AC « YOUSIGN SAS - ROOT2 CA ».

1.2 Identification du document

Le présent document correspond à la Politique de Certification (PC) de l'Autorité de Certification « YOUSIGN SAS - SIGN2 CA ». L'identifiant de ce document est :

- OID : 1.2.250.1.302.1.7.1.0

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

Les références à des documents annexes sont répertoriées dans le document « Procédure de classification de l'information ».

1.3 Entités intervenant dans l'IGC

1.3.1 Autorités de certification

La notion d'Autorité de Certification (AC) telle qu'utilisée dans la présente PC est définie au chapitre 1.6 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.

1.3.2 Autorités d'enregistrement

L'Autorité d'Enregistrement (AE) a pour rôle de vérifier l'identité du futur RCC¹ de certificat. L'AE de l'AC « YOUSIGN SAS - SIGN2 CA » est opérée par un service interne à Yousign.

1.3.3 Responsables de certificats de cachets

Dans le cadre de la présente PC, un RCC est une personne physique qui est responsable de l'utilisation du certificat de cachet du serveur informatique identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat. Le RCC a un lien contractuel / hiérarchique / réglementaire avec cette entité.

Le RCC respecte les conditions qui lui incombent définies dans la PC de l'AC « YOUSIGN SAS - SIGN2 CA ». Il est à noter que le certificat étant attaché au serveur informatique et non au RCC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RCC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.

1.3.4 Utilisateurs de certificats

Un utilisateur désigne une entité ou partie d'une entité (y incluant les personnes physiques et morales) pouvant être amené à utiliser des certificats afin d'en vérifier la validité ainsi que son lien avec les données signées.

¹ Responsable de certificats de cachets

Les utilisateurs peuvent utiliser les informations contenues dans le certificat afin de vérifier sa validité (révocation, date de validité, ...).

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

La présente PC traite des bi-clés et des certificats gérés par les RCC, afin les entités puissent signer électroniquement des données (documents ou messages) dans le cadre d'échanges dématérialisés avec les catégories d'utilisateurs de certificats identifiées au chapitre 1.3.4 ci-dessus. Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

1.4.2 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 - SIGN2 CA » (signature des certificats des RCC, des LCR / LAR) ainsi que des clés, bi-clés et certificats des composantes de l'IGC (sécurisation des échanges entre composantes, authentification des opérateurs, etc.).

L'AC « YOUSIGN SAS - SIGN2 CA » génère et signe différents types d'objets : certificats, LCR / LAR. Pour signer ces objets, l'AC « YOUSIGN SAS - SIGN2 CA » dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur dans la hiérarchie des AC que YouSign met en œuvre.

Les bi-clés et certificats de l'AC « YOUSIGN SAS - SIGN2 CA » ne sont utilisées que pour la signature de certificats, de LCR / LAR et ne doivent être utilisés qu'à cette fin. Ils ne doivent notamment être utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

1.4.3 Domaines d'utilisation interdits

Tout domaine d'application n'étant pas prévu dans le chapitre précédent 1.4.1, est interdit. De plus, les usages du certificat doivent être en conformité avec la législation et la réglementation.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

La société Yousign SAS est responsable de la PC. Ses coordonnées sont :

Yousign SAS
8 allée Henri Pigis
14000 Caen

1.5.2 Point de contact

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

Gestion de l'AC Yousign
Yousign SAS
8 allée Henri Pigis
14000 CAEN
contact@yousign.fr

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

Yousign met en œuvre un Comité de Direction Technique Yousign. Celui-ci procède à la validation de la conformité de la DPC par rapport à la PC.

1.5.4 Procédure d'approbation de la conformité de la DPC

Le Comité de Direction Technique Yousign réalise ou fait réaliser l'ensemble des actions nécessaires (audits, etc.) à la validation et à l'approbation de la DPC.

1.6 Définitions et acronymes

1.6.1 Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AC Autorité de Certification

ACI	Autorité de Certification Intermédiaire
ACP	Autorité de Certification Primaire
AE	Autorité d'Enregistrement
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
HSM	Hardware Security Module (module cryptographique)
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
OID	Object Identifier
PC	Politique de Certification
PSCE	Prestataire de Services de Certification Électronique
RCC	Responsable du Certificat de Cachet
RSA	Rivest Shamir Adelman
SMS	Short Message Service
URL	Uniform Resource Locator
CGU	Conditions Générales d'Utilisation

1.6.2 Définitions

Les termes utilisés dans la présente PC sont les suivants :

Autorité d'enregistrement - Cf. chapitre 1.3.2

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.

Clé privée : clé de la bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité.

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

Comité de Direction Technique – le comité de direction technique est un comité interne à 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 RCC 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 RCC de la fonction de génération des éléments secrets du RCC.

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

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

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

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 RCC et réaliser des opérations cryptographiques.

Personne autorisée - Il s'agit d'une personne autre que le RCC 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 RCC (demande de révocation, de renouvellement, ...). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du RCC.

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 RCC et les utilisateurs de certificats.

RCC – Cf chapitre **Erreur ! Source du renvoi introuvable.**

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 RCC et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles).

Responsable du certificat de cachet – Cf chapitre **Erreur ! Source du renvoi introuvable.**

Système de signature Yousign – Le système de signature Yousign est une application fournie par Yousign permettant à un RCC d'utiliser la clé privée correspondant à la clé publique qui

est dans le certificat qui l'identifie en vue de réaliser des signatures électroniques de données et d'autoriser la signature de ces données par d'autres utilisateurs. C'est le seul système autorisé à accéder aux clés privées des RCC. Pour pouvoir utiliser leur clé privée, les RCC doivent utiliser des données d'activation.

Utilisateur de certificat - Cf. chapitre 1.3.4.

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

2.1 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.fr/fr/public/document>

2.2 Informations devant être publiées

Yousign publie les informations suivantes :

- L'ensemble des PC gérées par Yousign, dont la présente ;
- Les LCR/LAR,
- Les certificats de la hiérarchie d'AC jusqu'à l'AC racine, accompagnés de leurs empreintes pour assurer aux utilisateurs des certificats l'intégrité des certificats de la chaîne d'AC,
- Les CGU Yousign.

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

2.3 Délais et fréquences de publication

Les délais et fréquences de publication sont les suivants :

- La fréquence de publication des PC/DPC Yousign sont décrites dans chaque PC/DPC. La PC est publiée avant toute émission d'un certificat final contenant l'OID correspondant,
- Les LCR/LAR sont publiées quotidiennement.
- 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.

2.4 Contrôle d'accès aux informations publiées

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

L'accès en modification aux données publiées est restreint aux équipes internes Yousign en charge de publier les documents sur l'espace de publication.

3-Identification et authentification

3.1 Nommage

3.1.1 Types de noms

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

Les certificats des RCC sont conformes à la norme [X.509]. Les certificats des RCC seront identifiés par un « Distinguished Name » (DN) conforme aux spécifications de la norme [X.501].

Nom du champ	Description	Obligatoire
CN	<i>Common Name</i> : nom libre désignant le certificat. Le nom doit contenir le nom officiel de l'entité.	Oui
O	<i>Organization</i> : Nom de la société.	Oui
OU	<i>Organisation Unit</i> : champ contenant la référence de l'entité du RCC structurée conformément à la norme ISO 6523. Le format sera <ICD>. Par exemple, pour la France, la valeur sera fixée comme ceci : 0002 NUMERO_SIREN	Oui
OU	<i>Organisation Unit</i> : champ permettant de renseigner une information facultative. Ne doit pas commencer par 4 chiffres.	Non
C	<i>Country</i> : pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée.	Oui

3.1.2 Nécessité d'utilisation de noms explicites

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

3.1.3 Pseudonymisation des services de création de cachet

Sans objet.

3.1.4 Règles d'interprétation des différentes formes de nom

Les éléments contenus dans les chapitres 3.1.1 et 3.1.2 fournissent les explications permettant d'interpréter correctement les différentes formes de nom.

3.1.5 Unicité des noms

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

3.1.6 Identification, authentification et rôle des marques déposées

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

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

3.2 Validation initiale de l'identité

L'enregistrement d'un service de création de cachet d'une entité auquel un certificat doit être délivré se fait via l'enregistrement du RCC correspondant auprès de l'AE.

L'enregistrement d'un RCC, et l'entité correspondante, se fait directement auprès de l'AE.

L'AE valide l'identité "personne morale" de l'entité de rattachement du RCC.

3.2.1 Méthode pour prouver la possession de la clef privée

La clef privée est entièrement gérée, stockée et protégée par l'IGC Yousign. Néanmoins, nous mettons en œuvre des moyens techniques et organisationnels afin d'assurer que la clef privée ne sera utilisée que par le RCC.

La clef privée est associée de manière logique à l'entité et le RCC de celle-ci est le seul à posséder les données d'activation.

En effet, pour pouvoir utiliser sa clef privée, le RCC devra s'authentifier.

Notre architecture technique ne permet l'utilisation d'une clef privée qu'à condition que les données d'authentification soient saisies par le RCC. De plus, une signature réalisée via l'AC « YOUSIGN SAS - SIGN2 CA » n'est valable que si l'IGC Yousign peut attester le cycle complet d'une demande de signature via un ensemble de journaux, et de traces qui sont documentés.

Le RCC devra s'authentifier par un couple login/mot de passe. Cette authentification se fait sur un canal HTTPS au travers d'une plateforme web, d'une application mobile ou encore via l'utilisation des web services Yousign.

3.2.2 Validation de l'identité d'un organisme

Cf chapitre 3.2.3.

3.2.3 Validation de l'identité d'un individu

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

L'enregistrement du futur RCC (personne physique) représentant une entité nécessite, l'identification de cette entité et l'identification de la personne physique. S'agissant d'un certificat de cachet, le RCC doit de plus être habilité en tant que RCC pour le service de création de cachet considéré.

Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre :

- une demande de certificat, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le nom du service de création de cachet concerné par cette demande,
- un mandat, daté de moins de 3 mois, désignant le futur RCC comme étant habilité à être RCC pour le service de création de cachet pour lequel le certificat de cachet doit être délivré. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCC,
- [ENTREPRISE] toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers, ...), 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,

- [ENTREPRISE] tout document attestant de la qualité du signataire de la demande de certificat,
- [ADMINISTRATION] une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,
- un document officiel d'identité en cours de validité du futur RCC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- les conditions générales d'utilisation signées.

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

Dans le cas de changement d'un RCC en cours de validité d'un certificat de cachet, le nouveau RCC doit être enregistré en tant que tel par l'AC en remplacement de l'ancien RCC.

L'enregistrement du nouveau RCC (personne physique) représentant une entité nécessite l'identification de la personne physique et la vérification de son habilitation en tant que représentant de l'entité à laquelle le service de création de cachet est rattaché et en tant que RCC pour ce service.

Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre :

- un mandat, daté de moins de 3 mois, désignant le futur RCC comme étant habilité à être le nouveau RCC pour le service de création de cachet auquel le certificat a été délivré, en remplacement du RCC précédent. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCC,
- [ENTREPRISE] tout document attestant de la qualité du signataire du mandat,
- [ADMINISTRATION] une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,
- un document officiel d'identité en cours de validité du futur RCC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- les conditions générales d'utilisation signées.

3.2.4 Informations non vérifiées du RCC

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

3.2.5 Validation de l'autorité du demandeur

Le rattachement de la personne physique à la personne morale est suffisant pour permettre au RCC de demander un certificat pour le compte de son entité de rattachement.

3.2.6 Certification croisée d'AC

Sans objet.

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

3.3.1 Identification et validation pour un renouvellement courant

L'identification et la validation de l'identité du RCC pour un renouvellement correspond à une nouvelle demande de certificat. Nous suivrons le processus spécifié dans le chapitre 3.2.

3.3.2 Identification et validation pour un renouvellement après révocation

L'identification et la validation de l'identité du RCC pour un renouvellement après révocation correspond à une nouvelle demande de certificat. Nous suivrons le processus spécifié dans le chapitre 3.2.

3.4 Identification et validation d'une demande de révocation

La demande de révocation d'un certificat pourra se faire par téléphone, par courrier ou par courriel. Voici la procédure à suivre :

- Révocation via téléphone : l'utilisateur pourra contacter Yousign par téléphone afin de demander la révocation de son certificat. Pour ce faire, Yousign s'assure de son identité. Une série de 2 questions aléatoires concernant son identité sera posée au

RCC. Ces questions seront fondées sur les informations en possession de Yousign. La validation sera effective, suite à une confirmation obtenue via un autre canal que l'appel téléphonique. Par exemple, nous pouvons lui envoyer un lien de confirmation sur son adresse courrier électronique.

- Révocation par courriel : l'utilisateur pourra contacter Yousign par mail afin de demander la révocation de son certificat. Pour ce faire, Yousign s'assure de son identité. Une série de 2 questions aléatoires concernant son identité sera posée au porteur. Ces questions seront fondées sur les informations en possession de Yousign. La validation sera effective, suite à une confirmation obtenue via un autre canal que le mail. Par exemple, nous pouvons :
 - lui envoyer un code sur son numéro de téléphone
 - effectuer un appel téléphonique pour avoir une confirmation
- Révocation par courrier : une demande pourra être faite par courrier, via une lettre recommandée avec accusé de réception. La demande écrite doit être signée par le RCC, ou par un responsable de l'entité de rattachement du RCC.

4-Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

La demande de certificat provient du RCC nommé par le responsable légal de l'entité.

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

Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. chapitre 3.2 ci-dessus) :

- le nom du service de création de cachet à utiliser dans le certificat ;
- les données personnelles d'identification du RCC ;
- les données d'identification de l'entité ;

Le dossier de demande est établi soit directement par le futur RCC à partir des éléments fournis par son entité, soit par son entité et validé par le futur RCC. Le dossier est transmis directement à l'AE par voie électronique. L'AE s'assure de disposer d'une information permettant de contacter le futur RCC du certificat.

4.2 Traitement d'une demande de certificat

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

Les identités "personne physique" et "personne morale" sont vérifiées conformément aux exigences du chapitre 3.2.

L'AE, doit effectuer les opérations suivantes :

- valider l'identité du futur RCC ;
- vérifier la cohérence des justificatifs présentés ;

- s'assurer que le futur RCC a pris connaissance des modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation).

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat et de la bi-clé vers la fonction adéquate de l'IGC.

L'AE conserve ensuite une trace des justificatifs d'identité présentés. Les différents justificatifs électroniques seront signés et horodatés via un système d'archivage à vocation probatoire.

4.2.2 Acceptation ou rejet de la demande

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

4.2.3 Durée d'établissement du certificat

L'AC doit s'efforcer de traiter la demande de certificat dans un délai raisonnable. Néanmoins, il n'y a aucune restriction concernant la durée maximale ou minimale de traitement.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments du RCC : la bi-clé, ainsi que le certificat associé. À partir de ce moment, le dispositif de signature Yousign sera activé.

Le processus de génération du certificat est lié de manière sécurisée au processus de génération de la bi-clé. La clef 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 à respecter sont précisées aux chapitres 5- et 6- ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre 5.2).

4.3.2 Notification par l'AC de la délivrance du certificat au RCC

Une fois la bi-clé et le certificat générés, et le service de cachet Yousign du RCC activé, le RCC en sera informé via courrier électronique. Le service de cachet Yousign permet d'utiliser la clef privée du RCC afin de signer des documents. Seul cet outil peut utiliser le certificat émis par l'AC « YOUSIGN SAS - SIGN2 CA ».

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

L'acceptation d'un certificat émis par l'AC est tacite dès la signature effectuée via le système de signature Yousign.

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

L'AC conserve une trace de l'acceptation (action de la signature) du certificat par le RCC. Cette acceptation sera horodatée.

4.4.2 Publication du certificat

L'AC ne publie pas les certificats des RCC émis.

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

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

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le RCC

La clef privée et le certificat du RCC sont stockés dans un module cryptographique au sein de l'IGC Yousign. Ces éléments ne peuvent être utilisés que dans le cadre de l'utilisation du service de cachet Yousign par le RCC. Toute autre utilisation est strictement interdite. De plus, seul le RCC peut utiliser sa clef privée et son certificat dans le cadre d'une signature.

Cette restriction d'utilisation de la clé privée et du certificat associé par le seul RCC est assurée par un système d'authentification. Une authentification via des codes d'accès ainsi qu'une clé unique associée au cachet. L'utilisation de la clé privée et du certificat est conditionnée à la validation de cette authentification par l'application de signature Yousign.

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

Cf. chapitre précédent 4.5.1.

4.6 Renouvellement d'un certificat

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

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

4.6.1 Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au RCC de l'établissement du nouveau certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

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

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

4.7.1 Causes possibles de changement d'une bi-clé

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

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du serveur (cf. chapitre IV.9, notamment le chapitre IV.9.1 pour les différentes causes possibles de révocation).

4.7.2 Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat de cachet peut-être automatique ou bien à l'initiative du RCC.

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

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 3.3 ci-dessus.

Pour les actions de l'AC, cf. chapitre 4.3.1.

4.7.4 Notification au RCC de l'établissement du nouveau certificat

Cf. chapitre 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1

4.7.6 Publication du nouveau certificat

Cf. chapitre 4.4.2

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

Cf. chapitre 4.4.3

4.8 Modification du certificat

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

Les actions réalisées par l'AC sont décrites dans les chapitres relatifs à la révocation (chap. 4.9) et à la demande (chap. 4.7).

4.8.1 Causes possibles de modification d'un certificat

Sans objet.

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

Sans objet.

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

Sans objet.

4.8.4 Notification au RCC de l'établissement du certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6 Publication du certificat modifié

Sans objet.

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

Sans objet.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats de cachet

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat de cachet :

- les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du nom de l'entité), ceci avant l'expiration normale du certificat ;
- le RCC n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le RCC et/ou, le cas échéant, l'entité n'ont pas respecté leurs 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 RCC ;
- la clé privée du serveur est suspectée de compromission, est compromise ou, est perdue (éventuellement les données d'activation associées) ;
- les données d'authentification du RCC ont été compromises ;
- le RCC ou une entité autorisée (représentant légal de l'entité par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du RCC et/ou de son support) ;
- l'arrêt définitif du serveur ou la cessation d'activité de l'entité du RCC de rattachement du serveur.
- Le certificat de l'AC « YOUSIGN SAS - SIGN2 CA » est révoqué, entraînant de fait la révocation de tous les certificats RCC qui ont été émis par cette 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.

4.9.1.2 Certificats d'une composante de l'AC

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

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

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats de cachet

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

- le RCC du certificat de cachet ;
- un représentant légal de l'entité ;
- l'AC émettrice du certificat ou l'une de ses composantes (AE).

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

4.9.2.2 Certificats d'une composante de l'IGC

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

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

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat de cachet

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre 3.4.

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

- le nom du demandeur de la révocation ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série, identifiant du RCC) ;
- 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 RCC du certificat n'est pas le demandeur, il sera également informé de la révocation effective de son certificat.

L'entité, doit être informée de la révocation de tout certificat des RCC qui lui sont rattachés. L'opération est enregistrée dans les journaux d'évènements.

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

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

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

4.9.4 Délai accordé au RCC pour formuler la demande de révocation

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

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

4.9.5.1 Révocation d'un certificat de cachet

Par nature, une demande de révocation doit être traitée en urgence.

La fonction de gestion des révocations est disponible 24h/24h 7j/7j.

Toute demande de révocation d'un certificat RCC sera traitée 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.

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

La révocation d'un certificat d'une composante de l'IGC doit être effectuée dès la détection d'un 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.

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

L'utilisateur d'un certificat de cachet est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Il pourra utiliser la dernière LCR publiée.

4.9.7 Fréquence d'établissement des LCR

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

4.9.8 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.

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

Sans objet.

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

Sans objet.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

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

Pour les certificats d'AC, outre les exigences du chapitre 4.9.3.2 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/blog. 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.

4.9.13 Causes possibles d'une suspension

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

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

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 2.1, et à l'adresse contenue dans les certificats émis.

4.10.2 Disponibilité de la fonction

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

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

4.10.3 Dispositifs optionnels

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

4.11 Fin de la relation entre le RCC et l'AC

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

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

4.12 Séquestration de clé et recouvrement

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

4.12.1 Politique et pratiques de recouvrement par séquestration des clés

Sans objet.

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

Sans objet.

5-MESURES DE SÉCURITÉ NON TECHNIQUES

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

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

5.1.2 Accès physique

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

5.1.3 Alimentation électrique et climatisation

Des systèmes de protection de l'alimentation électrique et de la climatisation sont mis en œuvre afin d'assurer la continuité des services délivrés.

Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et/ou constructeurs.

5.1.4 Vulnérabilité aux dégâts des eaux

L'hébergement est réalisé dans une zone non inondable.

5.1.5 Prévention et protection incendie

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

5.1.6 Conservation des supports

Des sauvegardes des supports sont réalisées quotidiennement. Les sites dans lesquels sont conservées les sauvegardes sont protégés contre les risques d'incendie et d'inondation. De plus, les accès physiques et logiques sont protégés et soumis à une gestion des droits et à une authentification forte.

S'il y a utilisation de documents papiers, ou de supports amovibles 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 responsable du Conseil de Direction Technique.

Des procédures de gestion protègent les supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

5.1.7 Mise hors service des supports

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

5.1.8 Sauvegardes hors site

Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, disposent d'une sauvegarde hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.). Les fonctions de sauvegarde et de restauration seront effectuées par des administrateurs autorisés conformément aux mesures de sécurité procédurales.

Les sauvegardes hors sites sont réalisées dans un environnement sécurisé en accès physique et logique, et sécurisé contre les risques d'incendie et d'inondation.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

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

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

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

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

5.2.2 Nombre de personnes requises par tâche

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, il est demandé de répartir les fonctions sensibles sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC (cf. chapitre 6-).

5.2.3 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 d'application gère les autorisations. Il devra gérer la liste des autorisations en fonction des rôles. De plus, il devra assigner à chaque personne le bon rôle. Enfin, c'est également lui qui délivrera les données d'authentification au personnel. Il délivrera un certificat d'authentification.

Chaque attribution d'un rôle à un membre du personnel de l'IGC doit être notifiée par écrit. Ce rôle doit être clairement mentionné et décrit dans sa fiche de poste.

5.2.4 Rôles exigeant une séparation des attributions

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

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Tout le personnel amené à travailler au sein de composantes de l'IGC est soumis à une clause de confidentialité vis-à-vis de 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.

5.3.2 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.

5.3.3 Exigences en matière de formation initiale

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

5.3.4 Exigences et fréquence en matière de formation continue

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

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Les sanctions et procédures disciplinaires associées sont définies dans le règlement intérieur et la charte informatique fournie à l'ensemble des employés de Yousign. Celles-ci sont plus ou moins importantes en fonction de l'impact que peut avoir une action non autorisée.

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

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

5.3.8 Documentation fournie au personnel

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

5.4 Procédure de constitution des données d'audit

5.4.1 Type d'évènements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre de l'IGC, celle-ci journalise les 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 ;
- 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 RCC,...), qui sont journalisées dans un document électronique et/ou papier signé et horodaté.

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

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

Chaque enregistrement d'un 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.

5.4.2 Fréquence de traitement des journaux d'évènements

Cf. chapitre 5.4.8 ci-dessous.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins 1 mois. Ils sont archivés au plus tard sous un délai d'un mois.

5.4.4 Protection des journaux d'évènements

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

5.4.5 Procédure de sauvegarde des journaux d'évènements

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

5.4.6 Système de collecte des journaux d'évènements

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

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

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

5.4.8 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.

5.5 Archivage des données

5.5.1 Types de données à archiver

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

Les données à archiver sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les certificats, LAR et LCR tels qu'émis ou publiés ;
- les engagements signés par le responsable du Conseil de Direction Technique ;
- les journaux d'événements des différentes entités de l'IGC ;
- les dossiers d'enregistrements ;
- la trace d'acceptation du certificat par le RCC.

5.5.2 Période de conservation des archives

Dossiers de demande de certificat

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

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

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.

Ce dossier, doit permettre de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

Certificats, LAR et LCR émis par l'AC

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

Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 seront archivés pendant 5 ans après leur génération. L'archivage se fera dans un milieu sécurisé, permettant de garantir l'intégrité des données au cours du temps.

5.5.3 Protection des archives

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

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

5.5.4 Procédure de sauvegarde des archives

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

5.5.5 Exigences d'horodatage des données

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

5.5.6 Système de collecte des archives

Les systèmes de collecte des archives de Yousign sont internes.

5.5.7 Procédures de récupération et de vérification des archives

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

5.6 Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.

Au regard de la date de fin de validité de ce certificat, son renouvellement sera demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée sera utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 Reprise suite à la compromission et sinistre

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

L'IGC 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 Conseil 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 RCC devient insuffisant pour son utilisation prévue restante, alors le responsable du Conseil 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.

5.7.2 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 sera testé au minimum une fois tous les 2 ans.

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

La compromission d'une clé d'infrastructure ou de contrôle d'une composante est traitée dans le plan de continuité de la composante (cf. chapitre 5.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant sera immédiatement révoqué : cf. chapitre 4.9.

En outre, l'AC respecte les engagements suivants :

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

5.7.4 Capacités de continuité d'activité suite à un sinistre

L'IGC 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 5.7.2).

5.8 Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

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

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

- Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats de cachet et des informations relatives aux certificats).
- Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LAR et LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC. À défaut, les applications de l'Administration refuseront les certificats émis par des AC dont les LCR en cours de validité ne seraient plus accessibles, même si le certificat de cachet est encore valide.
- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des RCC ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire.

5.8.2 Cessation d'activité affectant l'AC

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

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

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

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

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

- s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- révoquer son certificat ;
- révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- informer (par exemple par récépissé) tous les RCC des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

6-Mesures de sécurité techniques

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (cf. chapitre 5-). Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 10- ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre 5.2.1), 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 clefs est réalisée par deux personnes internes à Yousign occupant des rôles de confiance. De plus, un témoin valider la bonne mise en œuvre de la cérémonie.

6.1.1.2 Clés serveurs

La génération des clés des serveurs doit être effectuée dans un environnement sécurisé (cf. chapitre 5-).

Les bi-clés des serveurs doivent être générées directement dans le dispositif de création de signature conforme aux exigences du chapitre 11- ci-dessous. Ce dispositif est un module cryptographique conforme aux exigences du chapitre 10- et est détenu par Yousign.

6.1.2 Transmission de la clé privée à son propriétaire

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

6.1.3 Transmission de la clé publique à l'AC

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

6.1.4 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 voir chapitre 2.1.

6.1.5 Tailles des clés

Les clefs d'AC auront ces caractéristiques :

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

Les clefs des RCC devront avoir ces caractéristiques :

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

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

L'équipement de génération de bi-clés utilisé pour la génération des paramètres des bi-clés de l'AC « YOUSIGN SAS - SIGN2 CA » et de serveurs est un module cryptographique.

Les bi-clés ne peuvent être générées que sur un module conforme à cette exigence, ou d'un niveau cryptographique et sécuritaire supérieur.

6.1.7 Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR (cf. chapitre 1.4.1).

L'utilisation d'une clé privée de serveur et du certificat associé est strictement au service de cachet de données (cf. chapitre 1.4.1).

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

Les modules cryptographiques, utilisés par l'AC et les serveurs, pour la génération et la mise en œuvre de leurs clés de signature, sont des modules cryptographiques répondant aux exigences du chapitre 10- ci-dessous. Yousign utilise des HSM certifiés 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 leurs mise en place, lors de la cérémonie des clés, lors de leurs utilisation, et ce jusqu'à leur fin de vie.

6.2.2 Contrôle de la clé privée par plusieurs personnes

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

Le contrôle de la clé privée du RCC est sous contrôle exclusif. Yousign ne dispose pas des éléments permettant d'accéder et d'utiliser la clé privée d'un serveur durant le processus de signature. Le processus technique garantit que seule la clé privée générée pour le serveur durant le processus de signature est utilisée.

6.2.3 Séquestration de la clé privée

Les clefs privées d'AC et des RCC ne sont pas séquestrées.

6.2.4 Copie de secours de la clé privée

Les clés privées d'AC font l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences du chapitre 10- 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.

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

Le contrôle des opérations de chiffrement / déchiffrement doit être conforme aux exigences du chapitre 6.2.2.

6.2.5 Archivage de la clé privée

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

6.2.6 Transfert de la clé privée vers / depuis le module cryptographique

La génération des clés privées d'AC et de serveurs se fait dans le module cryptographique.

Le transfert vers / depuis le module cryptographique ne se fait que pour la génération des copies de sauvegardes. Ceci se fait sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.7 Stockage de la clé privée dans un module cryptographique

Le stockage des clés privées d'AC et de serveurs est réalisé dans un module cryptographique répondant aux exigences du chapitre 10- et du chapitre 11- ci-dessous pour le niveau de sécurité considéré.

Cependant, dans le cas des copies de secours, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences du chapitre 6.2.4.

Yousign met les moyens en place afin de garantir que les clés privées d'AC ne sont pas compromises pendant leur stockage ou leur transport.

6.2.8 Méthode d'activation de la clé privée

L'activation des clés privées d'AC se fera dans un module cryptographique et sera contrôlée via des données d'activation (cf. chapitre 6.4). Pour l'AC, les porteurs de secrets devront être présents afin de réaliser l'activation.

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

6.2.9 Méthode de désactivation de la clé privée

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

Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans le chapitre 10- pour le niveau de sécurité considéré.

6.2.10 Méthode de destruction des clés privées

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

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de création de signature

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

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

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

6.3.2 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 de cachet qu'elle émet. Les clefs de signatures de l'AC auront une durée de vie de maximum 10 ans.

Les bi-clés et les certificats de cachet doivent avoir une durée de vie au maximum de 3 ans. Les clefs de signatures de l'AC auront une durée de vie maximum 10 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

6.4.1.1 Clés de l'AC

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

6.4.1.2 Clés privées de serveurs

Les données d'activation sont générées :

- L'URL à usage unique lui permettant d'accéder au processus de signature
- Des codes d'accès
- Une clé unique associée au cachet.

6.4.2 Protection des données d'activation

6.4.2.1 Clés de l'AC

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

6.4.2.2 Clés de serveurs

Le RCC est le seul à connaître ses codes d'accès et de la clé unique associée au cachet.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 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 ;
- Protection du réseau.

6.5.2 Niveau de qualification des systèmes informatiques

Sans objet.

6.6 Mesures de sécurité liées au développement des systèmes

6.6.1 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.

6.6.2 Niveau d'évaluation sécurité du cycle de vie des systèmes

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

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

6.7 Mesures de sécurité réseau

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

6.8 Horodatage / Système de datation

L'AC « YOUSIGN SAS - SIGN2 CA » réalise un horodatage sur l'ensemble des éléments archivés.

7-Profil des certificats et des LCR

7.1 Profils de certificats

7.1.1 Certificats de l'ACP

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 clefs de l'AC	4096 bits

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	
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

7.1.2 Certificats de l'AC « YOUSIGN SAS - SIGN2 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 - SIGN2 CA,OU=794513986,O=YOUSIGN SAS,

Longueur des clefs de l'AC	L=CAEN,ST=CALVADOS,C=FR 4096 bits
----------------------------	--------------------------------------

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	
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

7.1.3 Certificats de cachet

Champs de base	Valeur
Version	2
Numéro de série	Défini par l'outil
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS - SIGN2 CA,OU=79451398600016,O=YOUSIGN SAS,L=Caen,ST=Calvados,C=FR
Validity	3 ans
Subject	Se reporter au chapitre 3.1.1
Longueur des clefs	2048 bits

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	
Key Usage	O	O	Non Repudiation
Extended Key Usage	O	N	MS Document Signing Adobe PDF Signing
Certificate Policies	O	N	1.2.250.1.302.1.7.1.0
CRL Distribution Points	O	N	http://crl.yousign.fr/crl/yousignsassign2ca.crl http://crl2.yousign.fr/crl/yousignsassign2ca.crl http://crl3.yousign.fr/crl/yousignsassign2ca.crl
Basic Constraints	O	O	CA:false

7.2 Liste de Certificats Révoqués

Champs de base	Valeur
Version	1
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS - SIGN2 CA,OU=79451398600016,O=YOUSIGN SAS,L=Caen,ST=Calvados,C=FR
Validité	7 jours
Next update	This update + 1 jour
Revoked Certificates	Serial Number Revocation Date

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	
CRL Number	O	N	Défini par l'outil

8-Audit de conformité et autres évaluations

8.1 Fréquences et / ou circonstances des évaluations

Un contrôle de conformité est réalisé lors de la mise en service du système et suite à toute modification significative. De plus, un audit sera réalisé au moins tous les ans. Les audits sont réalisés en interne par du personnel de Yousign ou bien sous la forme d'une prestation auprès d'acteurs spécialistes de la sécurité des systèmes d'information et ayant des compétences reconnues dans le domaine de la signature électronique.

Dans le cadre d'obtention de certifications des services de l'IGC, l'audit de certification est réalisé par une société externe dument accréditée.

8.2 Identités / qualifications des évaluateurs

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

8.3 Relations entre évaluateurs et entités évaluées

Les contrôleurs sont des membres internes de Yousign.

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

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

8.5 Actions prises suite aux conclusions des évaluations

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

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.
- En cas de résultat "à confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

9-Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Sans objet.

9.1.2 Tarifs pour accéder aux certificats

Sans objet.

9.1.3 Tarifs pour accéder aux LCR

L'accès aux LCR est gratuit.

9.1.4 Politique de remboursement

Sans objet.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

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.

9.2.2 Autres ressources

Sans objet.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

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

9.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3 Responsabilités en termes de protection des informations confidentielles

Yousign applique des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 9.3.1. Yousign s'engage à respecter la législation et la réglementation en vigueur sur le territoire français.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

Yousign s'engage à respecter la législation et de la réglementation en vigueur sur le territoire français, en particulier de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

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

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données à caractères personnelles

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

9.4.5 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 RCC à l'AC ne sont pas divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du RCC, décision judiciaire ou autre autorisation légale.

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

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

9.4.7 Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.4.8 Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par 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.

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

9.6 Interprétations contractuelles et garanties

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 la partie de la DPC leur incomitant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre 8-),
- respecter les accords ou contrats qui les lient entre elles ou aux RCC,
- 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.

9.6.1 Autorités de Certification

L'AC opérée par Yousign est responsable de :

- la validation et de la publication de la PC,
- la validation de la DPC, et de leur conformité à 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.

9.6.2 Service d'enregistrement

Se reporter au chapitre 9.6.1.

9.6.3 RCC de certificats

Le RCC 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 ;
- respecter les conditions d'utilisation du service de cachet Yousign ;
- informer l'AC de toute modification concernant les informations contenues dans son certificat ;
- 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.

9.6.4 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 de cachet jusqu'à l'ACP, 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.

9.6.5 Autres participants

Sans objet.

9.7 Limite de garantie

Sans objet.

9.8 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 RCC.

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 cachet et ce, dans le respect et les limites de la loi applicable.

9.9 Indemnités

Sans objet.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

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

9.10.2 Fin anticipée de validité

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

9.10.3 Effets de la fin de validité et clauses restant applicables

Sans objet.

9.11 Amendements à la PC

9.11.1 Procédures d'amendements

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

9.11.2 Mécanisme et période d'information sur les amendements

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

9.11.3 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 RCC, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

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

9.12 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.

9.13 Juridictions compétentes

Se rapporter au chapitre 9.12.

9.14 Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 10- ci-dessous.

9.15 Dispositions diverses

9.15.1 Accord global

Sans objet.

9.15.2 Transfert d'activités

Sans objet.

9.15.3 Conséquences d'une clause non valide

Sans objet.

9.15.4 Application et renonciation

Sans objet.

9.15.5 Force majeure

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

9.15.6 Autres dispositions

Sans objet.

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

10.1 Exigences sur les objectifs de sécurité

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

- garantir que la génération des bi-clés des RCC 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 RCC ;
- 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.

10.2 Exigences sur la certification

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

11-Annexe 2 : Exigences de sécurité du dispositif du système de signature

11.1 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 RCC 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 RCC 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.

11.2 Exigences sur la certification

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