POLITIQUE DE CERTIFICATION RACINE - YOUSIGN

Version 1.0.0 au 28/10/2013

Historique

Version	Date	Rédigé par	Mise à jour
0.0.0	01/06/2013	Yousign	Création du document
1.0.0	28/10/2013	Yousign	Validation du document

Table des matières

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 Primaire « Root CA » (ACP). 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'ACP, tant sur le plan des exigences de sécurité techniques qu'organisationnelles.

L'ACP ne peut être utilisée que pour produire des certificats d'Autorités de Certification Intermédiaires (ACI). Le présent document n'intervient pas dans le cadre des ACI. Chaque ACI devra mettre en place sa PC.

1.2 Identification du document

Le présent document correspond à la Politique de Certification (PC) des Autorités de Certification Primaires de Yousign. L'identifiant de ce document est :

- OID : 1.2.250.1.302.1.1.1.0

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 0 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. Dans le cadre de ce document, nous nous

intéressons aux ACP opérés par Yousign. En ce qui concerne les ACI opérées par Yousign, il faut se référer aux documents correspondants. Voici une liste non exhaustive :

- Politique de certification de l'Autorité YOUSIGN SAS – SIGN CA
- Politique de certification de l'Autorité YOUSIGN SAS – COSIGN CA

1.3.2 Autorités d'enregistrement

L'Autorité d'Enregistrement (AE) a pour rôle de vérifier l'identité du futur porteur de certificat. L'AE de l'ACP est opérée par un service interne à Yousign et n'acceptera que Yousign comme porteur. Les AE des ACI seront décrites dans la PC de chacune des ACI.

1.3.3 Porteurs de certificats

Dans le cadre de cette PC, le porteur de certificat ne peut être que Yousign, une de ses filiales ou un de ses mandataires, qui opèrera l'ACI désignée par le certificat certifié par une ACP. Le porteur sera identifié dans le sujet du certificat grâce au nom de l'ACI en tant que nom commun, et par l'organisation qui ne peut être que « Yousign ».

1.3.4 Utilisateurs de certificats

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

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

Les bi-clés ne peuvent être utilisées que pour les actions associées à l'autorité de certification racine par la présente PC et en particulier : signatures de certificats (ACI, autres composantes de l'infrastructure Yousign), signature de ses LCR/LAR.

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

Yousign SAS
2 rue neuve bourg l'abbé
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
2 rue neuve bourg l'abbé
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

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
RSA	Rivest Shamir Adelman
SMS	Short Message Service
URL	Uniform Resource Locator
CGU	Conditions Générales d'Utilisation
OTP	One Time Password

1.6.2 Définitions

Les termes utilisés dans la présente PC Type sont les suivants :

Agent - Personne physique agissant pour le compte d'une autorité administrative.

Autorités administratives - Ce terme générique, désigne les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

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 **Erreur ! Source du renvoi introuvable.** 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 usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

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

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

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

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

Fonction d'information sur l'état des certificats - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR).

Infrastructure de gestion de clés (IGC) - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, d'une entité d'archivage, d'une entité de publication, etc.

Modules cryptographiques - dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée utilisé pour conserver et mettre en œuvre la clé privée d'AC, les bi-clés des porteurs et réaliser des opérations cryptographiques.

One Time Password (OTP) - un OTP est un mot de passe unique valable seulement pour une transaction lors d'une signature réalisée avec le système de signature Yousign permettant d'authentifier un porteur.

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

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

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

Prestataire de services de certification électronique (PSCE) - Un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles).

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

privée, les porteurs doivent s'authentifier via deux canaux successifs (un couple login / mot de passe, puis un OTP envoyé par SMS ou par courrier électronique).

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/public/documents

2.2 Informations devant être publiées

Yousign publie les informations suivantes :

- L'ensemble des PC/DPC gérées par Yousign, dont la présente ;
- Les LCR/LAR,
- Les certificats d'AC, accompagnés de leurs empreintes
- Les CGU Yousign.

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.
- Les LCR/LAR sont publiées quotidiennement.
- Les certificats d'AC sont publiés suite à leur émission.
- 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.

Toute modification des informations publiées est soumise au respect des CGU publiées par Yousign.

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 d'ACI ainsi que les certificats d'ACP sont conformes à la norme [X.509]. Les ACI et les ACP seront identifiés par un « Distinguished Name » (DN) conforme aux spécifications de la norme [X.501].

Nom du champ	Description	Obligatoire
CN	*Common Name* : nom commun de l'AC. Il commencera par la raison sociale de la société gérante de l'AC et terminera par le numéro de version du certificat. (on incrémente suite à un changement de certificat). Pour le premier certificat, aucun numéro de version n'est nécessaire.	Oui
OU	*Organisation Unit* : champ contenant la référence de la société gérante de l'AC structurée conformément à la norme ISO 6523. Le format sera <ICD>. La valeur sera fixée comme ceci : 0002 79451398600016	OUI
O	*Organisation* : nom de l'organisation. La valeur sera fixée à « YOUSIGN SAS ».	Oui
C	*Country* : code du pays de l'autorité compétente auprès de laquelle l'entité émettant le certificat est officiellement enregistrée. La valeur sera fixée à « FR ».	Oui
L	*Locality* : Ville dans laquelle est implantée la société gérante de l'AC. La valeur sera fixée à « CAEN ».	Oui
ST	*State* : département dans lequel la société gérante de l'AC est implanté. La valeur sera fixée à « CALVADOS »	Oui

3.1.2 Nécessité d'utilisation de noms explicites

Le nom (CN) d'une ACI doit être explicite, c'est-à-dire qu'il doit être formé de mots du langage naturel, français ou anglais. Le nom doit pouvoir permettre de connaître quelle est la société gérante de l'ACI et à quoi sert cette AC.

Le nom devra obligatoirement commencer par la raison sociale de la société gérante de l'ACI à savoir « YOUSIGN SAS ».

C'est l'AE qui valide si le nom est explicite ou non. En cas de litige, c'est le Conseil de Direction Technique qui statuera si le nom est bien explicite.

3.1.3 Pseudonymisation des porteurs

Il sera possible d'identifier via le nom une société gérante d'une ACI. En effet, le DN comportera les informations d'identification de la société telles que le numéro d'identification de la société ainsi que la raison sociale. De plus le CN commencera par la raison sociale de la société gérante de l'ACI.

Yousign n'autorisera donc pas la pseudonymisation des porteurs.

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

L'AE doit vérifier que le nom de l'ACI est bien unique, et qu'il n'existe pas une autre ACI délivrée par l'ACP ayant le même nom.

Pour le renouvellement des certificats d'ACI, le CN se terminera par le numéro de version (et non d'identification) du certificat. Il sera incrémenté à chaque renouvellement.

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 de propriété intellectuelle.

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

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clef privée

Le porteur qui génère la bi-clé de l'ACI, doit alors fournir à l'ACP, une preuve de possession de sa clé privée correspondant à la clé publique contenue dans la demande de certificat.

Cette preuve peut être matérialisée en signant avec la clef privée de l'ACI la demande de certificat au format PKCS#10

3.2.2 Validation de l'identité d'un organisme

Seuls Yousign et ses filiales peuvent être porteurs d'une ACI délivré par une ACP soumis à la présente PC. De ce fait, la demande sera émise en interne par le Conseil de Direction Technique.

3.2.3 Validation de l'identité d'un individu

Le responsable du Conseil Technique de Direction de Yousign sera le représentant de l'ACI. De ce fait, nous ne demanderons aucun justificatif documentaire, puisque la demande sera réalisée en interne. Néanmoins, nous demanderons que le responsable du Conseil Technique de Direction de Yousign signe une demande écrite (électronique ou manuscrite) de l'émission d'un certificat d'ACI.

3.2.4 Informations non vérifiées du porteur

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

3.2.5 Validation de l'autorité du demandeur

Aucune vérification n'est faite. Seul le responsable du Comité de Direction Technique de Yousign est habilité à réaliser une demande de certificat d'ACI.

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

Le renouvellement de la bi-clé d'un porteur entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la bi-clé correspondante.

3.3.1 Identification et validation pour un renouvellement courant

Un renouvellement est réalisé suite à la demande du responsable du Comité de Direction Technique. Un document de demande de renouvellement doit alors être signé par celui-ci (électronique ou manuscrit).

3.3.2 Identification et validation pour un renouvellement après révocation

Un renouvellement est réalisé suite à la demande du responsable du Comité de Direction Technique. Un document de demande de renouvellement doit alors être signé par celui-ci (électronique ou manuscrit).

3.4 Identification et validation d'une demande de révocation

La demande de révocation est réalisée par le responsable du Conseil de Direction Technique. Celui-ci doit signée la demande de révocation (électronique ou manuscrite) afin que Yousign procède à la révocation de l'ACI. La demande inclura obligatoirement la raison de la révocation.

4-Exigences opérationnelles sur le cycle de vis des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Une demande de certificat d'ACI ne peut qu'émaner du responsable du Conseil de Direction Technique de Yousign.

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

Le responsable du Conseil de Direction Technique de Yousign, remplit le document de demande d'ACI. Suite à cela, l'AE vérifie que la demande respecte les exigences contenues dans la présente PC. Si tout est en ordre, l'ACI doit générer sa bi-clé. Le responsable du Conseil Technique de Yousign, fournira la clef publique ainsi que la preuve que la clef privée associé à la clef publique lui appartient.

4.2 Traitement d'une demande de certificat

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

Les ACP exerce la fonction d'AE afin d'émettre les certificats d'ACI. Pour ce faire, les ACP doivent recevoir une demande signée par le responsable du Conseil de Direction Technique de Yousign. Si la demande respecte les exigences de la présente PC, le certificat pourra alors être émis.

La demande signée est conservée par l'AE soit sous forme papier, soit sous forme électronique (signée électroniquement et horodatée).

4.2.2 Acceptation ou rejet de la demande

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

4.2.3 Durée d'établissement du certificat

L'ACP 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 conformément au chapitre 4.2, l'ACP déclenche les processus de génération et de préparation du certificat. Celui-ci sera alors transmis au responsable du Conseil de Direction Technique qui pourra alors la récupérer en utilisant un code de récupération.

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

Le responsable du Conseil de Direction Technique sera notifié par courrier électronique de la délivrance du certificat. Afin de le récupérer il devra utiliser un code de récupération qui lui sera fourni en main propre par l'ACP. Ceci permet de s'assurer que le certificat a bien été récupéré par le responsable du Conseil de Direction Technique.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Le responsable devra signer (manuscritement ou électroniquement) une attestation d'acceptation du certificat une fois qu'il l'aura récupéré et accepté. Ce document sera conservé par l'ACP.

4.4.2 Publication du certificat

L'ACP n'est pas autorisé à publier les certificats d'ACI émis.

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

Lors de la délivrance du certificat l'ACP sera notifiée.

4.5 Usages de la bi-clé et du certificat

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

L'utilisation de la clé privée d'une ACI et du certificat associé est strictement limitée aux usages définis dans le chapitre 1.4. Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

De plus, les ACI s'engagent à protéger leurs bi-clés. En cas de compromission, les ACI s'engagent à en faire part à l'ACP et à demander la révocation du certificat.

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

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

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 porteur).

Dans le cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. L'ACI s'engage à renouveler sa bi-clé lors d'une demande de renouvellement au travers de la demande de renouvellement signée par le responsable du Conseil de Direction Technique de Yousign.

4.6.1 Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au porteur de l'établissement du nouveau certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

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

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

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi, les bi-clés, et les certificats correspondants des ACI, seront renouvelés au minimum tous les 10 ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du porteur (cf. chapitre 4.9, notamment le chapitre 4.9.1 pour les différentes causes possibles de révocation).

Nota - Dans la suite du présent chapitre, le terme utilisé est "fourniture d'un nouveau certificat". Ce terme recouvre également, dans le cas où elle est générée par l'AC, la fourniture de la nouvelle bi-clé du porteur.

4.7.2 Origine d'une demande d'un nouveau certificat

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

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 porteur 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'ACP.

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 porteur 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

Il peut exister plusieurs causes de révocation de certificat d'une ACI. Les voici :

- Les informations d'une ACI figurant dans son certificat ne sont plus correctes ;
- L'ACI n'a pas respecté les modalités applicables d'utilisation du certificat ;
- L'ACI n'a pas respecté ses obligations découlant de la PC de l'AC ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement de l'ACI ;

- La clé privée de l'ACI est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- L'ACI demande explicitement la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur et/ou de son support) ;
- Cessation d'activité de l'ACI ;
- Cessation d'activité de l'ACP ;

Lorsqu'une des circonstances ci-dessus se réalise et que l'ACP 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.

4.9.2 Origine d'une demande de révocation

Une demande de révocation de certificat d'ACI ne peut émaner que d'un responsable légal, ou mandaté de Yousign, ou par les autorités judiciaires via une décision de justice.

4.9.3 Procédure de traitement d'une demande de révocation

Une demande de révocation de certificat d'ACI réceptionnée par l'ACP doit au moins contenir les informations suivantes :

- Le numéro de série du certificat à révoquer ;
- Le nom de l'ACI (DN complet) ;
- Le nom du demandeur de la révocation ;
- Eventuellement, la cause de révocation.

La demande est authentifiée et contrôlée par l'ACP, et lance la fonction de gestion des révocations révoquant le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.

Le responsable du Conseil de Direction Technique de Yousign sera alors notifié du bon déroulement de la révocation du certificat d'ACI.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

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

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

Le délai maximum de traitement d'une demande de révocation d'un certificat d'ACI est de 24h.

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

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

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 d'ACI, et d'ACP, outre les exigences du chapitre 4.9.3 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'ACI ou de connaissance de la compromission de la clé privée de l'ACP ayant émis son certificat, l'ACI ou l'ACP s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat.

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 publiés à l'adresse spécifié 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 porteur et l'AC

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

4.12 Séquestre de clé et recouvrement

Les clefs privées d'ACI ne sont pas séquestrées par l'ACP.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

5-MESURES DE SÉCURITÉ NON TECHNIQUES

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

Les sites d'hébergement des services de certification 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.
- **Contrôleur** : Personne désignée dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

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

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 tâches

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

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont 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 contrôleur) 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 sur le territoire français.

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

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

- réception d'une demande de certificat (initiale et renouvellement) ;
- validation / rejet d'une demande de certificat ;
- évènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- génération des certificats des porteurs ;
- 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.

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.

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 archivés 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 des journaux d'événements en vue d'une détection en échec d'événement ou d'opération est réalisée par du personnel disposant d'un rôle de confiance. Cette analyse est réalisée quotidiennement (jours ouvrés).
- Une analyse complète des journaux d'événements, en vue de détecter toute anomalie, est réalisée par du personnel disposant d'un rôle de confiance. Cette analyse est réalisée une fois par semaine.
- Une analyse complète, avec un rapprochement de l'ensemble des journaux est réalisée, de manière à détecter toute anomalie et toute divergence entre événements dépendants, par du personnel disposant d'un rôle de confiance. Cette analyse est réalisée une fois par mois.

L'ensemble de ces actions doit être noté dans un cahier de suivi électronique. Ce cahier comportera les renseignements suivants : date, identité de la personne réalisant l'opération, nature de l'action réalisée, compte rendu de l'action réalisée. Ce cahier devra être horodaté et signé électroniquement.

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 et LCR tels qu'émis ou publiés ;
- les engagements signés par le responsable du Conseil de Direction Technique ;
- les journaux d'évènements des différentes entités de l'IGC.

5.5.2 Période de conservation des archives

- Les dossiers de demande de certificats
  Les dossiers de demande de certificat d'ACI signés par le responsable du Conseil de Direction Technique seront archivés pendant 10 ans.
- Les certificats et LCR émis par l'AC
  Ces éléments sont conservés au minimum pendant 5 ans après leurs expirations.
- Les journaux d'événements
  Ces éléments seront archivés pendant une durée de 10 ans après leurs générations. Ils seront archivés dans un environnement garantissant leur pérennité et leur intégrité. Un horodatage permettant d'assurer la date de mise en archivage sera réalisée.

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.

Notre prestataire, CDC Arkhinéo, assure la réalisation de la procédure d'archivage des archives.

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 porteurs 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 Type, des engagements de l'AC dans sa propre PC notamment en ce qui concerne les fonctions liées à la publication et / ou liées à 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 des porteurs et des informations relatives aux certificats).
- Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des 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 du porteur est encore valide.

Des précisions quant aux engagements suivants doivent ainsi être annoncées par l'AC dans sa PC :

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

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 LCR conformément aux engagements pris dans sa PC.

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

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

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

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

6-Mesures de sécurité techniques

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'ACP

La génération des clés de signature d'AC sera effectuée dans un environnement sécurisé (cf. chapitre 5-). Les clés de signature d'AC seront générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 11- ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature d'AC sera 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 dérouleront 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'accompagnera 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 seront remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Ils seront stockés 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 sera réalisée par deux personnes internes à Yousign occupant des rôles de confiance. De plus, un témoin validera la bonne mise en œuvre de la cérémonie.

6.1.1.2 Clés des porteurs (ACI) générées par le porteur

Les bi clefs d'ACI devront être générées suivant les mêmes exigences que le chapitre 6.1.1.1.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet.

6.1.3 Transmission de la clé publique à l'AC

La clé publique est transmise en interne par le responsable du Conseil de Direction Technique à l'ACP, de manière physique. La clé publique devra être contenue sur un support de type clé USB de stockage ou carte à puce.

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

La clé publique des ACP est enveloppée dans un certificat racine autosigné. Sa diffusion s'accompagne de l'empreinte numérique du certificat ainsi que d'une déclaration précisant 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'ACP auront ces caractéristiques :

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

Les clefs d'ACI devront avoir ces caractéristiques :

- Algorithme utilisé : RSA.
- Taille minimale des clefs : 4096 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 des ACP et des ACI, 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'ACP et d'ACI et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR (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'ACP et les ACI, 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 protégés contre les pannes électriques, les inondations ainsi que les incendies.

Yousign s'assure de la sécurité des HSM lors de leur mise en place, lors de la cérémonie des clés, lors de leur utilisation, et ce jusqu'à leur fin de vie.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature des ACP 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 ACP, qui se voient remettre ces secrets sur carte à puce lors de la cérémonie des clés. Nous utilisons une méthode N-M.

6.2.3 Séquestre de la clé privée

Les clefs privées d'ACP et d'ACI 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'ACP ne soient à aucun moment en clair en dehors du module cryptographique.

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'ACP et des porteurs (ACI) ne sont jamais archivées.

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

La génération des clés privées d'ACP et d'ACI 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'ACP est réalisé dans un module cryptographique répondant aux exigences du chapitre 10- 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'ACP 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'ACP et d'ACI se fera dans un module cryptographique et sera contrôlée via des données d'activation (cf. chapitre 6.4). Pour l'ACP, les porteurs de secrets devront être présents afin de réaliser l'activation.

6.2.9 Méthode de désactivation de la clé privée

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

Une clé privée d'ACP pourra également être désactivée après une certaine période d'inactivité. 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'ACP, 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 ACP ainsi que des ACI 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 ACI doivent avoir une durée de vie au maximum de 10 ans.

La fin de validité d'un certificat d'ACP doit être postérieure à la fin de vie des certificats d'ACI qu'elle émet. Les clefs de signatures de l'ACP auront une durée de vie de maximum 10 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

6.4.2 Protection des données d'activation

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

6.4.3 0 0vfAutres 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 ACP soumises à la présente PC, sont des ACP hors ligne. C'est-à-dire qu'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

Les ACP réalisent 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 - ROOT CA,OU=0002 79451398600016,O=YOUSIGN SAS,L=Caen,ST=Calvados,C=FR
Validity	10 ans
Subject	CN=YOUSIGN SAS - ROOT CA,OU=0002 79451398600016,O=YOUSIGN SAS,L=Caen,ST=Calvados,C=FR
Longueur des clefs de l'ACP	4096 bits

Champs d'extension	Obligatoire (O/N)	Critique (O/N)	Valeur
Authority Key Identifier	O	N	
Key Usage	O	O	DigitalSignature Key_CertSign Crl_Sign
Certificate	O	N	1.2.250.1.302.1.1.1.0

Policies			
CRL Distribution Points	O	N	https://yousign.fr/files/documents/yousignsasrootca.crl
Basic Constraints	O	O	CA:true

7.1.2 Certificats Porteurs

Champs de base	**Valeur**
Version	2
Numéro de série	Défini par l'outil
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS - ROOT CA,OU=00027945139860001 6,O=YOUSIGN SAS,L=Caen,ST=Calvados,C=FR
Validity	10 ans
Subject	Se reporter au chapitre 3.1.1
Longueur des clefs des ACI	4096 bits

Champs d'extension	**Obligatoire (O/N)**	**Critique (O/N)**	**Valeur**
Authority Key Identifier	O	N	
Key Usage	O	O	DigitalSignature Key_CertSign Crl_Sign
Certificate	O	N	1.2.250.1.302.1.1.1.0

Policies			
CRL Distribution Points	O	N	https://yousign.fr/files/documents/yousignsasrootca.crl
Basic Constraints	O	O	CA:true

7.2 Liste de Certificats Révoqués

Champs de base	Valeur
Version	1
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS - ROOT CA,OU=00027945139860001 6,O=YOUSIGN SAS,L=Caen,ST=Calvados,C=FR
Validité	1 jour
Next update	This update + 1 jour
Revoked Certificates	Serial Number Revocation Date CRL entry entensions : X509v3 CRL Reason Code

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.

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

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.

Pour ce faire Yousign a mandaté un correspondant Informatique et libertés.

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur) ;
- le dossier d'enregistrement du porteur.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données 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 porteurs à l'AC ne sont pas divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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.

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

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 incombant (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 porteurs,
- documenter leurs procédures internes de fonctionnement,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

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'GC, 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 Porteurs de certificats

Le porteur a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- protéger ses données d'authentification ;
- respecter les conditions d'utilisation du service de signature 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 de la sphère publique utilisant les certificats doivent :

- vérifier et respecter l'usage pour lequel un certificat a été émis ;
- pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'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 données d'authentifications, 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 l'Abonné.

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

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

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

9.9 Indemnités

Sans objet.

9.10Durée 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 porteurs 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 porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

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

9.12 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.

9.13Juridictions compétentes

Se rapporter au chapitre 9.12.

9.14Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre **Erreur ! Source du renvoi introuvable.** ci-dessous.

9.15Dispositions 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 2 : Exigences de sécurité du module cryptographique de l'AC

10.1Exigences sur les objectifs de sécurité

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

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

10.2Exigences sur la certification

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

11- Annexe 3 : Exigences de sécurité du dispositif du système de signature Yousign

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

11.2 Exigences sur la certification

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