Identification du document

Nom / référence	**Politique de Certification de l'AC Racine**
Objet	Politique de Certification pour les certificats de l'Autorité de Certification Racine

Auteur / propriétaire	Rémi BLANCHER
Relecteur	Olivier CLEF
Version actuelle	1.2
Statut actuel	Publié
Destinataire de l'information	Public
Date d'application	06/06/2023
Périodicité de contrôle	1 fois par an

Historique des versions

Révision	Nbr de pages	Objet de la modification	Date
1.0	41	Version initiale du document	23/05/2023
1.1	41	Modifications suite à audit interne - Ajout des valeurs dates de validité, AKI et SKI dans gabarits de certificats de l'AC Racine et de l'AC Horodatage suite à la Cérémonie de clés - Ajout de l'extension « CRL number » pour l'ARL	10/07/2023
1.2	41	Mise à jour URL du site de publication	10/10/2023

© APP Solutions | 25 rue de la Plaine, 75020 Paris

Table des matières

© APP Solutions | 25 rue de la Plaine, 75020 Paris

© APP Solutions | 25 rue de la Plaine, 75020 Paris

© APP Solutions | 25 rue de la Plaine, 75020 Paris

© APP Solutions | 25 rue de la Plaine, 75020 Paris

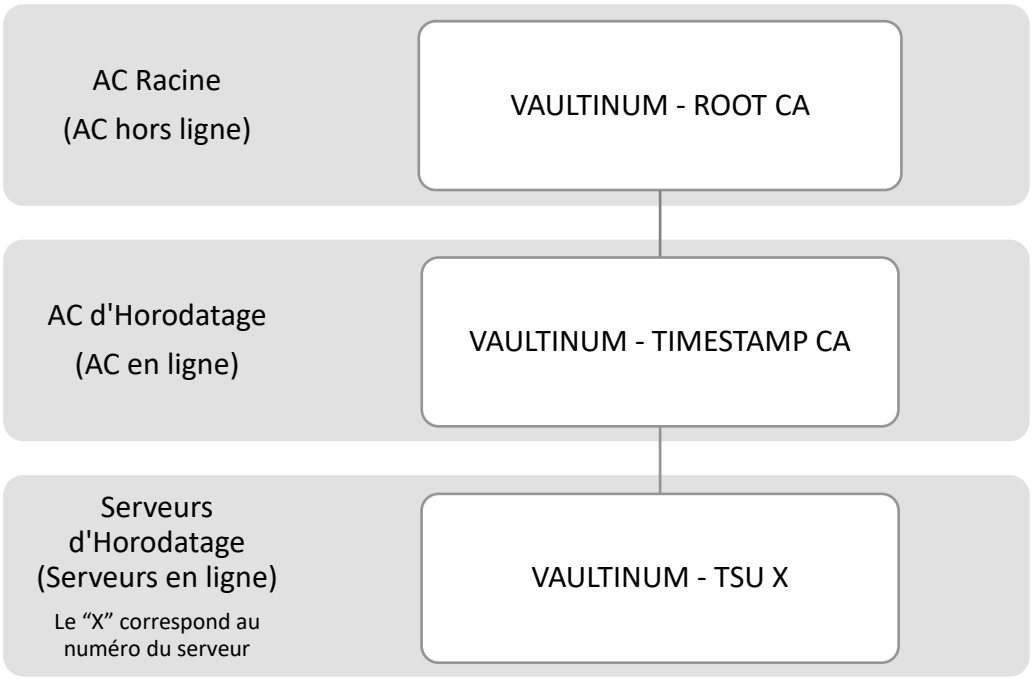
© APP Solutions | 25 rue de la Plaine, 75020 Paris

1. Introduction

1.1. Présentation générale

APP Solutions (ci-après nommée « la Société ») met en œuvre une Infrastructure de Gestion de Clés (IGC ou PKI) afin de gérer notamment les certificats utilisés dans le cadre de son service d'horodatage.

L'IGC de « la Société » s'appuie sur une hiérarchie de certification illustrée sur le schéma ci-dessous :



Le présent document constitue la politique de certification (PC) de l'autorité de certification racine (ACR) « VAULTINIM - ROOT CA » de « la Société » et contient les informations publiques de la Déclaration des Pratiques de Certification (DPC) associée.

L'ACR « VAULTINUM - ROOT CA » est une AC racine auto-signée et en mode hors-ligne.

L'ACR délivre des certificats exclusivement à des **Autorités de Certification Filles** de « la Société » dites :

- **Intermédiaires** : AC émettant des certificats pour des AC Emettrices
- **Emettrices** : AC émettant des certificats pour des utilisateurs finaux (personnes physiques et services applicatifs).

La présente politique de certification est structurée sur la base des exigences du document ETSI EN 319 411-1 relatif aux autorités de certification délivrant des certificats. Sa structure est conforme au RFC 3647.

1.2. Identification du document

La présente PC est dénommée « Politique de Certification de l'AC Racine VAULTINUM ».

Le numéro d'OID de la présente PC est : **1.3.6.1.4.1.60053.1.1.1.1.1**

1.3. Entités intervenant dans l'IGC

Le certificat de l'ACR est mis en œuvre pour :

- Signer les demandes de certificats des certificats des AC Filles (Intermédiaire ou Emettrice)
- Signer la Liste des Autorités Révoquées (LAR)

1.3.1. **Autorités de certification Racine**

© APP Solutions | 25 rue de la Plaine, 75020 Paris

L'Autorité de Certification Racine (ACR) responsable de la présente PC est « la Société » et est sous la responsabilité de son responsable légal.

L'ACR a la charge de l'application de la présente politique de certification.

Chaque certificat final possède un OID spécifique en complément de l'OID de la PC dans le champ « Politique de Certification » qui précise à quel sous-ensemble il appartient et comme cela est indiqué dans le paragraphe 1.2.

L'ACR a la charge du maintien en conditions opérationnelles et en conditions de sécurité de l'ensemble des composants constituant l'IGC. Cela comprend notamment :

- Les fonctions de génération des certificats ;
- La fonction de publication des informations ;
- La fonction de gestion des révocations ;
- La fonction d'information sur l'état des certificats.

1.3.2. **Autorité d'enregistrement (AE)**

Dans le cadre de l'AC Racine, les activités d'AE sont directement réalisées par l'AC Racine.

1.3.3. **Porteurs de certificats**

Sans objet, les certificats couverts par cette PC sont des certificats d'Autorités de Certification, il n'y a donc pas de porteurs.

Un certificat d'AC ne peut être délivré qu'à « la Société ».

1.3.4. **Utilisateurs de certificats**

Les certificats couverts par la présente PC sont utilisés dans les applications métiers mis en œuvre par « la Société ». Il s'agit donc d'application métiers ayant des besoins de valider des certificats finaux émis par une des AC filles de la chaîne d'AC portée par l'AC Racine.

1.4. Usage des certificats

1.4.1. **Domaines d'utilisation applicables**

Les certificats couverts dans la présente PC sont ceux de la hiérarchie portée par l'AC Racine.

1.4.1.1. Bi-clés et certificats d'AC Racine et de ses composantes

La bi-clé de l'ACR est utilisée uniquement pour :

- Signer les certificats d'AC Filles qu'elle émet ;
- Signer les listes des AC révoqués (LAR) qu'elle émet.

L'ACR signe son propre certificat X.509 d'AC (certificat auto-signé).

L'ACR signe les certificats des AC Filles ainsi que la liste des certificats des AC Filles révoquées.

Le certificat de l'ACR est utilisé par les utilisateurs pour vérifier l'authenticité d'un certificat d'AC Fille.

1.4.1.2. Bi-clés et certificats des AC Filles

L'ACR délivre exclusivement des certificats d'AC Filles à « la Société ».

Le bi-clé d'une AC Fille est utilisée uniquement pour :

- Signer les certificats qu'elle émet ;

© APP Solutions | 25 rue de la Plaine, 75020 Paris

- Signer les listes des AC révoquées (LAR) qu'elle émet (cas d'une AC Intermédiaire) ;
- Signer les listes des certificats révoquées (LCR) qu'elle émet (cas d'une AC Emettrice).

1.4.2. **Domaines d'utilisation interdits**

En dehors des usages identifiés dans le paragraphe précédent, tous les autres usages sont interdits.

1.5. Gestion de la PC

1.5.1. **Entité gérant la PC**

La gestion de la PC est de la responsabilité du RSSI (Responsable de la Sécurité des Systèmes d'Information) de « la Société ».

La gouvernance est assurée à travers son Comité de Pilotage (COPIL).

Le comité se réunit mensuellement et assure le suivi des activités des services de confiance de « la Société ».

1.5.2. **Point de contact**

Toute demande relative au service est à adresser au point de contact fourni à l'adresse suivante :

APP SOLUTIONS
Autorité de Certification
25, rue de la Plaine
75020 PARIS

APP SOLUTIONS peut également être contacté au travers du formulaire de contact disponible sur son site internet : https://vaultinum.com.

1.5.3. **Entité déterminant la conformité d'une DPC avec ce document**

Le COPIL est en charge de prononcer la conformité de la Déclaration des Pratiques de Certification (et des procédures associées) à la Politique de Certification.

1.5.4. **Procédures d'approbation de la conformité de la DPC**

L'approbation de la conformité à la DPC est formalisée à travers d'un compte rendu du COPIL.

Cette approbation intervient préalablement à la production d'un certificat final par les services concernés par la présente PC.

1.6. Définitions et acronymes

1.6.1. **Acronymes**

AC	Autorité de Certification
AE	Autorité d'Enregistrement
COPIL	COmité de PILotage du Système d'Information et des Services de Confiance
DN	Distinguished Name
DPC	Déclaration de Pratiques de Certification
ETSI	Institut européen des normes de télécommunication (European Telecommunications Standards Institute)

© APP Solutions | 25 rue de la Plaine, 75020 Paris

HSM	Hardware Security Module / Module cryptographique
IGC	Infrastructure de Gestion de Clés
LAR	Liste des Autorités Révoquées
LCR	Liste des Certificats Révoqués
OID	Identifiant d'objet (Object IDentifier)
PC	Politique de Certification

1.6.2. **Définitions**

Authentification : Processus permettant de vérifier l'identité déclarée d'une personne ou de tout autre entité, ou de garantir l'origine de données reçues.

Autorité de certification (AC) : Autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer des certificats.

Bi-clé : Un bi clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques.

Certificat : Clé publique d'un utilisateur, concaténée à d'autres informations rendues infalsifiables par signature avec la clé privée de l'autorité de certification qui l'a délivré.

Certificat d'AC : Certificat d'une autorité de certification.

Certificat de signature : Certificat final disposant des usages permettant de faire de la signature électronique. Le certificat est émis au nom d'une personne physique.

Déclaration des pratiques de certification : Déclaration des pratiques mises en œuvre par une autorité de certification pour émettre et gérer des certificats.

Données d'activation : Données privées permettant d'initialiser ses éléments secrets.

Indentification d'objet (OID) : Série d'entiers globalement unique permettant d'identifier un objet.

Infrastructure de Gestion de Clés (IGC) : Ensemble de composantes fournissant des services de gestion de clés et de certificats au profit d'une communauté d'utilisateurs.

Liste d'Autorités Révoqués (LAR) : Liste contenant les identifiants des certificats d'Autorités de Certification révoqués ou invalides.

Politique de certification (PC) : Ensemble de règles relatives à l'applicabilité d'un certificat à une communauté et / ou à une classe d'applications ayant des besoins de sécurité communs.

Rôle de confiance : Rôle dévolu à un acteur, personne physique nommément identifié, intervenant dans la mise en œuvre ou l'exploitation de l'AC afin d'assurer, ou maintenir en opération, une ou plusieurs fonctions.

Utilisateur : Utilisateur ou système faisant confiance à un certificat.

X.509 : Format standard de certificat électronique.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

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

2.1. Service de publication

L'ACR est chargée de la mise à disposition de la politique de certification et des conditions générales d'utilisation.

Ces informations sont accessibles via Internet, sur le site : https://vaultinum.com/fr/publication-autorite-horodatage.

L'accès à ce service est assuré 24h/24 et 7j/7 avec un taux de disponibilité de 99%.

2.2. Informations publiées

Les informations publiées sont les suivantes :

- La présente Politique de Certification
- Les certificats de l'AC Racine en cours de validité
- La liste des Autorités Révoquées (LAR) pour les certificats d'AC Filles
- Les informations permettant aux utilisateurs de s'assurer de l'origine et de l'état des certificats de l'AC Racine (certificats auto signés)

Le document PC est publié :

- Au format PDF/A
- En français.

2.3. Délais et fréquences de publication

La politiques de certification est mise à jour et publiée en cas de modification.

Les certificats d'AC sont diffusés ou mis en ligne préalablement à toute diffusion de certificats ou de LAR.

La LAR est mise à jour annuellement ou après une révocation.

2.4. Contrôle d'accès aux informations publiées

Les demandes de publication sont tracées dans des outils internes de suivi de ticket.

La publication de documents liés aux activités de l'ACR et des nouvelles LAR se fait manuellement par un administrateur système disposant des habilitations systèmes.

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

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.

Dans chaque certificat X 509, le fournisseur (Issuer) et le porteur (Subject) sont identifiés par un Distinguished Name (DN).

L'identification des AC se fait en utilisant le DN dont la composition est décrite ci-dessous :

Attribut du DN	Valeur
Country (C)	Pays de résidence de l'entité responsable de l'AC
OrganizationName (O)	Nom officiel complet de l'entité responsable de l'AC
OrganizationIdentifier (OI)	Numéro d'immatriculation officiel de l'entité responsable de l'AC conformément à [EN_319_412-1] clause 5.1.4.
CommonName (CN)	Nom significatif de l'AC

3.1.2. **Nécessité d'utilisation de noms explicites**

Les noms choisis sont explicites.

3.1.2.1. Identité de l'AC Racine

L'identification de l'ACR dans le certificat de l'ACR est la suivante :

Champ de base	Valeur
Issuer DN	C = FR O = APP SOLUTIONS OI = NTRFR-519136170 CN = VAULTINUM - ROOT CA
Subject DN	C = FR O = APP SOLUTIONS OI = NTRFR-519136170 CN = VAULTINUM - ROOT CA

3.1.2.2. Identité de l'AC d'Horodatage

L'AC d'Horodatage est une AC Fille.

L'identification de l'AC d'Horodatage dans le certificat de l'AC d'Horodatage est la suivante :

Champ de base	Valeur
Issuer DN	C = FR O = APP SOLUTIONS OI = NTRFR-519136170 CN = VAULTINUM - ROOT CA
Subject DN	C = FR O = APP SOLUTIONS OI = NTRFR-519136170 CN = VAULTINUM - TIMESTAMP CA

3.1.3. **Anonymisation ou pseudonymisation**

Sans objet.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

3.1.4. **Règles d'interprétation des différentes formes de noms**

Les informations portées dans un certificat d'AC sont validées préalablement à sa génération par le COPIL.

Le COPIL est garant de la légitimité à utiliser des noms d'AC sous le périmètre de « la Société ».

Tous les caractères sont au format UTF8String ou PrintableString.

3.1.5. **Unicité des noms**

Le champ DN identifie une AC de façon unique au sein du domaine de l'IGC de « la Société ».

3.1.6. **Identification, authentification et rôle des marques déposées**

Pour les marques, dénominations sociales ou autres signes distinctifs, l'ACR n'effectue aucune recherche d'antériorité ou autre vérification ; il appartient au demandeur ou au titulaire de vérifier que la dénomination demandée ne porte pas atteinte à des droits de propriété de tiers.

3.2. Validation initiale de l'identité

3.2.1. **Méthode pour prouver la possession de la clé privée**

Les clés privées ne sont pas extractibles et sont générées au sein d'un HSM dans le cadre d'une cérémonie des clés.

Un huissier est présent en tant que témoin pour la cérémonie de clé de création de l'AC Racine.

3.2.2. **Validation de l'identité d'un organisme**

Un certificat d'AC ne peut être délivré qu'à « la Société ».

L'AC est demandé par le COPIL. Cette demande est formalisée à travers d'un compte rendu du COPIL.

Le document de nommage de l'AC (nom de l'AC, caractéristiques techniques) et le script de cérémonie de clés sont validés par le COPIL préalablement au lancement de la cérémonie de clés.

3.2.3. **Informations non vérifiées**

Sans objet.

3.2.4. **Validation de l'autorité du demandeur**

Cf paragraphe 3.2.2.

L'ensemble des actions réalisées durant la cérémonie des clés est conservé et archivé dans le procès-verbal de cérémonie.

3.2.5. **Certification croisée d'AC**

L'ACR n'a aucun accord de reconnaissance avec une AC extérieure au domaine de sécurité auquel elle appartient.

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

Un nouveau certificat ne peut pas être fourni sans renouvellement de la bi-clé correspondante.

Le renouvellement se traduit alors par une nouvelle demande de certificat et bénéficie des mêmes procédures que pour une demande initiale.

3.4. Identification et validation d'une demande de révocation

La demande de révocation de clé pour une AC Fille signée par l'ACR émane de représentant légal ou d'une personne autorisée, et est validée formellement avant prise en compte par le COPIL.

Le certificat de l'ACR étant un certificat auto-signé, il ne peut pas être révoqué.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

En cas de compromission de la clé privée correspondante au certificat de l'ACR, l'ACR publiera une information sur le site identifié au paragraphe 2. Cela permet à tout porteur ou à toute application utilisatrice d'être informé de cette compromission.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Génération d'une bi-clé et d'un certificat de l'ACR

La génération de la bi-clé et du certificat est décidée par le COPIL.

La génération de la bi-clé de l'ACR est réalisée dans le cadre d'une cérémonie des clés. Le but de cette cérémonie est de générer la clé de signature de l'ACR ainsi qu'un certificat racine auto-signé.

La génération de la clé de signature de l'ACR est réalisée au sein d'un module cryptographique.

La cérémonie implique la présence d'au moins les personnes tenant les rôles de confiance suivants, outre le maître de cérémonie :

- Un représentant de l'ACR, garant du déroulement conforme au scénario de la cérémonie établie,
- Un administrateur système de l'IGC et des modules cryptographiques, garants du fait que les systèmes (matériels, logiciels et modules cryptographiques) sont correctement configurés et opérationnels conformément au document de cérémonie des clés,
- Le Responsable sécurité pour la cérémonie, garant du bon déroulement de la cérémonie sur le plan de la sécurité,
- Les détenteurs de secret et de supports sensibles ;
- Un huissier présent à titre de témoin impartial.

L'ACR s'engage à établir le scénario complet de la cérémonie. Ce document n'est pas public.

L'ACR s'engage à émettre des procès-verbaux pour chaque étape importante de la cérémonie, marquant notamment la conformité de la cérémonie déroulée, et l'engagement des détenteurs de secret à respecter les règles de conservation des secrets remis. Ces documents ne sont pas publics.

La publication du certificat de l'Autorité Racine par l'AC (cf. paragraphe 2) marque l'acceptation de ce certificat par celle-ci.

4.2. Renouvellement d'une bi-clé et d'un certificat de l'ACR

Les exigences concernant cette cérémonie sont similaires à la cérémonie décrite ci-dessus.

4.3. Demande de certificat d'AC Fille

4.3.1. **Origine d'une demande de certificat**

Une demande de certificat d'AC Fille émane du représentant légal ou d'une personne autorisée par l'organisation.

4.3.2. **Processus et responsabilités pour l'établissement d'une demande de certificats**

L'ACR est chargé d'établir un document de cérémonie des clés décrivant les conditions de génération et d'émission du certificat d'AC Fille.

4.4. Traitement d'une demande de certificat d'AC Fille

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

La demande est validée par le COPIL préalablement à son traitement.

Le document de cérémonie de clés est validé par le COPIL préalablement au traitement de la demande de certificat.

4.4.2. **Acceptation ou rejet de la demande**

© APP Solutions | 25 rue de la Plaine, 75020 Paris

Toutes les demandes de certificat sont acceptées ou rejetées par l'ACR. L'acceptation ou le rejet sont prononcés par le COPIL au travers d'un compte rendu de comité.

4.4.3. Délai de traitement de la demande de certification

La présente PC ne formule pas d'exigence vis-à-vis du délai maximum de traitement de la demande de certification.

4.5. Délivrance du certificat d'AC Fille

Lorsque la demande est validée par le COPIL, une cérémonie des clés est organisée et planifiée pour générer le bi-clés et le certificat de l'AC Fille.

4.5.1. Actions de l'ACR concernant la délivrance du certificat d'AC Fille

La génération du bi-clé et d'un certificat d'AC Fille se fait dans le cadre d'une cérémonie des clés. La clé privée de l'ACR devant être mise en œuvre dans ce cadre, le quorum des porteurs de secrets est nécessaire.

Pour toute demande de certificat d'AC Fille, l'ACR effectue les opérations suivantes :

- Signature du certificat de l'AC Fille par la clé privée de l'ACR ;
- Vérification du contenu du certificat généré et de la conformité des informations du certificat avec le document de cérémonie de clés ;

La génération de certificat d'AC Fille est consignée dans un procès-verbal lors de la cérémonie des clés.

4.5.2. Notification par l'ACR de la délivrance du certificat au responsable de l'AC Fille

Le certificat de l'AC Fille est remis à son représentant (représentant légal ou personne autorisée) au cours de la cérémonie des clés. La signature du procès-verbal (PV) de cérémonie atteste de la remise du certificat.

4.6. Acceptation du certificat d'AC Fille

4.6.1. Démarche d'acceptation du certificat

La signature du PV de cérémonie des clés vaut acceptation du certificat.

4.6.2. Publication du certificat

Le certificat de l'ACR et les certificats signés d'AC Fille sont publiés sur le point de publication indiqué au paragraphe 2.

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

Sans objet.

4.7. Usage de la bi-clé et du certificat de l'AC Fille

4.7.1. Utilisation de la clé privée et du certificat

L'utilisation de la clé privée et du certificat associé est décrite au chapitre 1.4.1.2

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

Les utilisateurs de certificats ne doivent les utiliser que dans les domaines d'utilisation spécifiés au chapitre 1.4.1.2.

L'usage autorisé du certificat est indiqué dans le certificat dans les extensions concernant les usages des clés.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

L'utilisation de la clé publique et du certificat est limitée au contrôle des certificats gérés par les AC Filles, et à la validation des LCR.

4.8. Renouvellement d'un certificat

La notion de renouvellement de certificat, au sens RFC 3647, correspondant à la seule modification des dates de validité, n'est pas retenue.

Seule la délivrance d'un nouveau certificat à la suite de changement de la bi-clé est autorisée.

4.8.1. Causes possibles de renouvellement d'un certificat

Sans objet.

4.8.2. Origine d'une demande de renouvellement

Sans objet.

4.8.3. Procédure de traitement d'une demande de renouvellement

Sans objet.

4.8.4. Notification de l'établissement du nouveau certificat

Sans objet.

4.8.5. Démarche d'acceptation du nouveau certificat

Sans objet.

4.8.6. Publication du nouveau certificat

Sans objet.

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

Sans objet.

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

4.9.1. Cause possible de changement de bi-clé

La bi-clé est changée à la suite d'une révocation ou bien en cas de fin de vie du certificat précédemment délivré.

Les bi-clés des AC Filles ainsi que les certificats correspondants sont renouvelés au **minimum tous les 10 ans.**

Par ailleurs, une bi-clés et un certificat peuvent être renouvelés :

- Par anticipation (ex : pour minimiser les possibilités d'attaques cryptographiques),
- Ou suite à la révocation du certificat d'une AC Fille (cf. chapitre 4.9)

4.9.2. Origine d'une demande de nouveau certificat

Dans tous les cas, la procédure de demande de nouveau certificat est identique à la procédure de demande initiale.

4.9.3. Procédure de traitement d'une demande de nouveau certificat

Identique à la demande initiale.

4.9.4. Notification de l'établissement du nouveau certificat

© APP Solutions | 25 rue de la Plaine, 75020 Paris

Identique à la demande initiale.

4.9.5. Démarche d'acceptation du nouveau certificat

Identique à la demande initiale.

4.9.6. Publication du nouveau certificat

Identique à la demande initiale.

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

Identique à la demande initiale.

4.10. Modification du certificat

Les modifications de certificats ne sont pas autorisées.

4.10.1. Cause possible de modification d'un certificat

Sans objet.

4.10.2. Origine d'une demande de modification de certificat

Sans objet.

4.10.3. Procédure de traitement d'une demande de modification de certificat

Sans objet.

4.10.4. Notification de l'établissement du certificat modifié

Sans objet.

4.10.5. Démarche d'acceptation du certificat modifié

Sans objet.

4.10.6. Publication du certificat modifié

Sans objet.

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

Sans objet.

4.11. Révocation et Suspension des certificats

4.11.1. Causes possibles d'une révocation

Les causes de révocation sont les suivantes :

- Obsolescence des informations figurant dans le certificat ;
- Compromission, suspicion de compromission, perte ou vol de clé privée ;
- Compromissions ou dépréciation d'algorithme ;
- Cessation de l'activité de l'AC Fille ;
- Décision à la suite d'un échec de contrôle de conformité ;
- Compromission ou révocation de l'ACR.

4.11.2. Origine d'une demande de révocation

Les personnes pouvant demander une révocation sont les suivantes :

© APP Solutions | 25 rue de la Plaine, 75020 Paris

- Le responsable légal de l'AC ;
- Le COPIL.

4.11.3. Procédure de traitement d'une demande de révocation

La demande de révocation est validée par le COPIL et elle est formalisée à travers un compte rendu COPIL.

La révocation d'un certificat d'AC Fille se fait dans le cadre d'une cérémonie des clés. La clé privée de l'ACR devant être mise en œuvre dans ce cadre, le quorum des porteurs de secrets est nécessaire.

A l'issue de la révocation du certificat d'AC Fille, une nouvelles LAR est produite et est mise en ligne.

4.11.4. Délai accordé pour formuler la demande de révocation

La demande de révocation doit être formulée au plus tôt dès la connaissance d'une cause effective de révocation.

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

L'ACR s'engage à traiter la demande de révocation d'un certificat d'AC Fille dans les meilleurs délais après réception de la demande avec un délai maximal de 72 heures.

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

Les applications de « la Société » souhaitant utiliser les certificats couverts par la présente PC doivent s'assurer que :

- Le certificat d'AC Fille est bien émis par l'ACR de « la Société »
- Le certificat d'AC Fille n'est pas révoqué en récupérant le statut de la LAR
- Le certificat d'AC Fille n'est pas expiré

4.11.7. Fréquence d'établissement des LAR

Les LAR sont générées au minimum tous les ans avec une période de validité de maximum 365 jours.

Les LAR sont générés en cérémonie de clés et ces LAR sont signées par l'ACR.

4.11.8. Délai maximum de publication d'une LAR

Une LAR est publiée dans les meilleurs délais après sa génération.

En cas de révocation d'un certificat d'AC Fille, la nouvelle LAR valide est publiée immédiatement.

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

Les systèmes de révocation et de vérification ont un taux de disponibilité d'au moins 99%, et sont disponibles 24 heures sur 24.

En cas de défaillance du système, l'ACR s'engage à rétablir le système sous 24h.

Ces services bénéficient d'une redondance et d'un plan de reprise d'activité qui permet d'assurer leur disponibilité.

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

Voir le paragraphe 4.9.6 du présent document.

4.11.11. Autres moyens disponibles d'information sur les révocations

Sans objet.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

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

Dans le cadre de la révocation d'un certificat d'AC Fille pour cause de compromission, le COPIL fera publier sur le site de publication une information claire de la compromission de la clé privée.

L'ACR indiquera sur son site les impacts et les précautions à prendre en la matière.

4.11.13. Causes possibles d'une suspension

La suspension de certificat n'est pas autorisée.

4.11.14. Origine d'une demande de suspension

Sans objet.

4.11.15. Procédure de traitement d'une demande de suspension

Sans objet.

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

Sans objet.

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

4.12.1. Caractéristiques opérationnelles

Les LAR sont au format LCR v2, publiées sur le site internet identifié au chapitre 2.

Ces adresses figurent également dans le champ « Point de Distribution des LCR » de chaque certificat.

4.12.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24, 7 jours sur 7 avec un taux de disponibilité de 99%.

4.12.3. Dispositifs optionnels

Sans objet.

4.13. Fin d'abonnement

En cas de fin d'activité de l'ACR, l'ensemble des certificats émis par la chaîne d'AC correspondante sont révoqués.

4.14. Séquestre de clé et recouvrement

Il n'est pas procédé à un séquestre de clé.

4.14.1. Politique et pratiques de recouvrement par séquestre de clés

Sans objet.

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

Sans objet.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

5. Mesures de sécurité non techniques

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

Les composants techniques de l'IGC sont redondés sur plusieurs sites.

Les sites d'hébergement sont situés en France et leur exposition géographique couvre par des mesures particulières les risques de type tremblement de terre, explosion, risque volcanique ou crue.

5.1.2. Accès physique

L'accès physique aux fonctions de génération des certificats, génération des éléments secrets et de gestion des révocations, est strictement limité aux seules personnes nominativement autorisées.

L'accès physique aux composantes de l'IGC supportant ces fonctions est limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique, permettant la séparation des rôles entre les différents intervenants.

La traçabilité des accès est assurée.

En dehors des heures ouvrables, des mesures de détection d'intrusion physique sont mises en œuvre.

Des mesures de sécurité physique sont également mises en place pour limiter les accès aux supports sensibles (supports de clés, dossier d'enregistrement, documents d'applications).

5.1.3. Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre de manière qu'une interruption de service d'alimentation électrique, ou une défaillance de climatisation ne portent pas atteinte aux engagements pris par l'ACR en matière de disponibilité (gestion des révocations et informations relatives à l'état des certificats en particulier).

5.1.4. Exposition aux dégâts des eaux

La définition du périmètre de sécurité prend en considération les risques inhérents aux dégâts des eaux. Des moyens de protection sont mis en œuvre pour parer les risques résiduels (rupture de canalisation par exemple).

5.1.5. Prévention et protection incendie

Les moyens de prévention et de lutte contre l'incendie permettent de respecter les engagements pris par l'ACR en matière de disponibilité (gestion des révocations et informations relatives à l'état des certificats en particulier), et de pérennité de l'archivage.

5.1.6. Conservation des supports

Les moyens de conservation des supports permettent de respecter les engagements pris par l'ACR en matière de restitution et de pérennité de l'archivage.

5.1.7. Mise hors service des supports

Les supports recensés comme sensibles en termes de confidentialité font l'objet de mesures de destruction, ou peuvent être réutilisés dans un contexte opérationnel identique à un même niveau de sensibilité.

5.1.8. Sauvegarde hors site

Afin de permettre une reprise après incident conforme aux engagements pris par l'ACR, des sauvegardes sont mis en place hors site des informations et fonctions critiques. La confidentialité des informations, et l'intégrité des applications sauvegardées sont garantie de manière homogène sur le site opérationnel et sur le site de sauvegarde.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

Cela concerne en particulier les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.2. Mesures de sécurité procédurales

5.2.1. **Rôles de confiance**

L'AC distingue les rôles de confiance suivants (équivalents aux Trusted Roles de la norme ETSI [EN 319401]) :

- **Responsable de sécurité / Officier de Sécurité** : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats. Ce rôle correspond au rôle Security Officer défini dans la norme [EN 319401].
- **Administrateur des plateformes** : 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. Ce rôle correspond au System Administrator défini dans la norme [EN 319401].
- **Exploitant** : Un opérateur système (ou exploitant) 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. Ce rôle correspond au System Operator défini dans la norme [EN 319401].
- **Contrôleur / Auditeur de système** : Personne désignée par une autorité compétente et 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. Ce rôle correspond au System Auditor défini dans la norme [EN 319401].

En plus de ces rôles de confiance, l'ACR a défini le rôle de **Porteur de part de secret**. Le Porteur de part de secret a la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité de la part qui lui a été confiée.

5.2.2. **Nombre de personnes requises par tâche**

Les différentes entités du service de confiance s'organisent pour assurer la disponibilité de leurs personnels en fonction des tâches qui leurs sont dédiées.

La reconstruction du secret de l'ACR nécessite le regroupement de **2 porteurs de secrets parmi 4** chacun possédant une partie du secret.

5.2.3. **Identification et authentification pour chaque rôle**

Des mesures d'identification et d'authentification sont mises en place afin de supporter la mise en œuvre de la politique de contrôle d'accès et la traçabilité des opérations ; la politique de contrôle d'accès limite l'accès aux seules personnes habilitées à réaliser les opérations d'administration et de génération de clés sur l'infrastructure de confiance.

Les rôles attribués sont notifiés par écrit aux personnes concernées dans la description de poste et sont contre-signées par le responsable hiérarchique. Les formulaires d'obtention d'un rôle de confiance permettent d'assurer le suivi de ce rôle, notamment les modifications de postes dans le temps ou le retrait d'un rôle de confiance.

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.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- Le responsable de sécurité ne peut pas être administrateur système ou exploitant ;
- Le contrôleur ne peut pas être administrateur système ou exploitant.

Les attributions associées à chaque rôle sont conformes à la politique de sécurité de la composante.

Les porteurs de secret ne doivent jamais détenir deux parts différentes d'un même secret.

5.3. Mesures de sécurité vis à vis du personnel

5.3.1. Qualifications, compétences, et habilitations requises

Tout intervenant amené à occuper un rôle de confiance est soumis à une clause de confidentialité et de non-conflit d'intérêts. En outre les intervenants disposant d'un rôle de confiance attestent sur l'honneur n'avoir commis aucun délit en matière de cybercriminalité.

L'ACR s'assure que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles. Notamment les personnels suivent des formations au moins annuellement sur les menaces informatiques et les pratiques de sécurité du système d'information.

Le personnel d'encadrement possède l'expertise appropriée, et est familier des procédures de sécurité.

Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités (description de poste) et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2. Procédures de vérification des antécédents

Des procédures de vérification des antécédents sont mises en place pour les personnes appelées à occuper un rôle sensible. Notamment il est demandé au futur porteur d'un rôle de confiance lors d'une prise d'un rôle de confiance de fournir l'extrait n°3 du casier judiciaire. Pour chaque porteur d'un rôle de confiance, une revue de l'extrait n°3 du casier judiciaire est effectuée au moins une fois tous les 3 ans.

5.3.3. Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement. Cela concerne essentiellement le personnel opérant sur les composantes de l'IGC.

5.3.4. Exigences en matière de formation continue et fréquences des formations

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants.

Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.

5.3.5. Fréquence et séquence de rotations entre différentes attributions

Sans objet.

5.3.6. Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans la définition de poste ou la Charte Informatique pour les rôles sensibles tenus par le personnel de l'ACR.

5.3.7. Exigences vis à vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées.

5.3.8. Documentation fournie au personnel

© APP Solutions | 25 rue de la Plaine, 75020 Paris

Les règles de sécurité sont communiquées au personnel lors de la prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans le service de confiance disposent des procédures correspondantes.

5.4. Procédures de constitution des données d'audit

5.4.1. **Type d'événement à enregistrer**

Les éléments suivants font l'objet de traces d'enregistrement :

- Tous les événements relatifs à la sécurité, en particulier :
  - Les changements de politique de sécurité des systèmes ;
  - Les démarrages et arrêts des systèmes ;
  - Les pannes matérielles et logicielles ;
  - Les tentatives d'accès au système IGC.
- Tous les événements relatifs à la gestion des certificats d'AC, en particulier :
  - Validation / rejet d'une demande de certificat ;
  - Evénements liés aux clés et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction, ...) ;
  - 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 LAR.

Ces journaux permettent d'assurer la traçabilité et l'imputabilité des actions effectuées (horodatage, affectation à l'intervenant).

5.4.2. **Fréquence de traitement des journaux d'événements**

L'analyse du contenu des journaux d'événements est effectuée de manière ponctuelle par l'ACR dans le cadre d'audit ou de contrôle.

5.4.3. **Période de conservation des journaux d'événements**

Les journaux techniques sont conservés directement dans l'environnement utilisé pour réaliser les cérémonies des clés, cet environnement étant éteint en dehors d'une cérémonie des clés.

5.4.4. **Protection des journaux d'événements**

Les journaux d'événements sont accessibles uniquement au personnel autorisé de l'AC.

5.4.5. **Procédure de sauvegarde des journaux d'événements**

Les éléments de journalisation sont sauvegardés à l'issue d'une cérémonie des clés.

5.4.6. **Système de collecte des journaux d'événements**

Sans objet.

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

Sans objet

© APP Solutions | 25 rue de la Plaine, 75020 Paris

5.4.8. Evaluation des vulnérabilités

L'environnement n'est pas connecté sur le réseau durant sa mise en route en cérémonie des clés et est conservé éteint en dehors des cérémonies.

Les journaux d'évènements sont contrôlés au moins 1 fois par jour, afin d'identifier des anomalies.

5.5. Archivage des données

5.5.1. Types de données à archiver

Les données à archiver sont les suivantes :

- Logiciels exécutables et fichiers de configuration
- PC et DPC
- Certificats, LAR publiés
- Fiches de postes des rôles de confiance signées
- Dossiers de demande de certificats d'AC Fille
- Journaux d'événements

5.5.2. Période de conservation des archives

Le tableau suivant présente les périodes de conservation des archives pour chaque type de donnée

Type de données	Période de conservation
Logiciels	Version n-1
Configurations des logiciels	Version n-1
Dossiers de demande de certificats	7 ans après expiration du certificat de l'AC Fille
Certificats des AC	7 ans après expiration du certificat de l'ACR
LAR	7 ans après expiration du certificat de l'ACR
Journaux d'évènements	7 ans après expiration du certificat de l'ACR
Documentation	7 ans après expiration du certificat de l'ACR

5.5.3. Protection des archives

Quel que soit leur support, les archives sont protégées en intégrité, et ne sont accessibles qu'aux personnes autorisées. Ces archives sont lisibles et exploitables sur l'ensemble de leur cycle de vie.

L'AC met en œuvre les moyens nécessaires pour garantir la conservation des archives sur une période conforme aux exigences légales en matière de fourniture d'éléments de preuves.

5.5.4. Procédure de sauvegarde des archives

Les archives sont sauvegardées de manière sécurisée. Les moyens mis en œuvre pour réaliser la sauvegarde garantissent que les éléments ne peuvent pas être supprimés ou détruits facilement.

5.5.5. Exigences d'horodatage des données

L'horodatage des données des événements journalisés est synchrone en dehors des opérations hors ligne. Pour cela, les composants utilisés durant les cérémonies des clés est mis à jour manuellement, avant démarrage des opérations techniques.

5.5.6. Système de collecte des archives

Sans objet.

5.5.7. Procédure de récupération et de vérification des archives

© APP Solutions | 25 rue de la Plaine, 75020 Paris

La récupération et la vérification des archives peuvent être effectuées dans un délai conforme à l'utilisation des certificats délivrés. Un délai de 7 jours ouvrés est nécessaire pour récupérer les archives et les mettre à disposition du demandeur.

5.6. Changement de clés d'AC

La durée de vie des clés d'AC Racine **est de 20 ans**. La durée de vie des certificats d'AC Fille est de **10 ans**. L'ensemble de la chaîne d'AC devra être renouvelé :

- A la fin de vie de l'AC Racine ;
- Au renouvellement d'un certificat d'AC Fille si la durée de validité du certificat l'ACR est inférieur à 10 ans.

5.7. Reprise suite à compromission et sinistre

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

Des procédures et des moyens de remontée et de traitement des incidents (sensibilisation, formation des personnels, et analyse des différents journaux d'événements) sont mis en œuvre.

Un incident majeur – perte, suspicion de compromission, compromission ou vol de clé privée de gestion des certificats par exemple – est immédiatement signalé à l'ACR. La publication de révocation du certificat, si elle s'avère nécessaire, est effectuée dans la plus grande urgence par tout moyen nécessaire.

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

Un plan de continuité est mis en place permettant de répondre aux exigences de disponibilité des différentes composantes de l'IGC.

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

La compromission d'une clé d'AC entraîne immédiatement la révocation du certificat correspondant. Les cas de compromission des éléments secrets des autres composantes sont traités dans le plan de continuité d'activité. La révocation en cascade de tous les certificats émis par cette AC est également mise en œuvre.

Les éléments ci-après traitent de la compromission d'un algorithme ou d'un paramètre associé, tels que l'algorithme de condensat utilisé dans les certificats ou la longueur de la clé des certificats.

L'ACR se tient continuellement informée des cas de compromission des éléments susmentionnés, par le biais d'organismes comme l'ANSSI.

En cas d'information d'une compromission impactant les certificats des AC, l'ACR déclenchent une cellule de crise afin de déterminer les actions à mener pour rétablir le service au plus tôt.

Par mesure de précaution, l'ACR :

- Procède à l'arrêt immédiat des services de dématérialisation exploitant les certificats de l'ACR ;
- Fait diffuser immédiatement l'information à toutes les parties prenantes par mail.

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

Chaque entité opérant une composante de l'IGC met 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, y compris dans le cas d'incidents majeurs (compromission de clés privées, faiblesse des algorithmes utilisés, …). Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant des engagements de l'ACR dans

© APP Solutions | 25 rue de la Plaine, 75020 Paris

les présentes PC notamment en ce qui concerne les fonctions liées à la publication et à la révocation des certificats.

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les engagements des présentes PC.

En cas de détection d'un incident de sécurité sur l'infrastructure de confiance, l'ACR doit en être informée, et s'engage à informer le COPIL qui se charge ensuite, pour les incidents liés à la sécurité ou pour toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel, de prévenir l'ANSSI à travers l'adresse suivante : cert-fr.cossi@ssi.gouv.fr.

Les composants de l'IGC sont redondés sur plusieurs sites en mode actif/passif. Un sinistre majeur déclenche la bascule des services vers la seconde salle.

En cas de destruction du site d'hébergement, l'ACR établit dans le cadre d'une cellule de crise les conditions de continuité de son service de confiance. En fonction des éléments, l'ACR pourra considérer :

- Déclencher la fin de vie de ses services de confiance et assurer le transfert des activités de publication vers un tiers ;
- Reconstruire ses services sur un autre site, cela pouvant passer par la reconstruction de la chaîne d'AC ou bien par la mise en œuvre d'une nouvelle chaîne d'AC.

5.8. Fin de vie de l'IGC

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

L'ACR mettra en œuvre les mesures requises pour assurer au minimum la continuité de l'archivage des informations et la continuité des services de révocation. Le COPIL s'assurera que les coûts permettant de respecter ces exigences minimales sont couverts.

Dans la mesure où les changements envisagés peuvent entraîner des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, l'ACR les avisera aussitôt que nécessaire et, dans la mesure du possible, sous le délai de 6 mois. De même, l'ACR informera les autorités publiques concernées.

En cas d'arrêt de service, les exigences suivantes seront prises en compte :

1) La clé privée d'émission des certificats ne sera transmise en aucun cas ;
2) Toutes mesures nécessaires seront prises pour détruire cette clé privée ou la rendre inopérante ;
3) Tous les certificats émis encore en cours de validité seront révoqués et les parties prenantes seront prévenues ;
4) Les certificats d'AC Filles seront révoqués ;
5) L'ACR communiquera à l'ANSSI au point de contact identifié sur http://ssi.gouv.fr, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'ACR communiquera à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. L'ACR mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement ;
6) L'ACR tiendra informée l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

6. Mesures de sécurité techniques

6.1. Génération et installation de bi clés

6.1.1. Génération de bi clé

6.1.1.1. Clés de l'AC Racine

Les clés de l'ACR sont générées lors de la cérémonie des clés, en présence d'un représentant de l'ACR, des porteurs de secrets, du maître de cérémonie et d'un huissier.

Cette cérémonie de clé se fait dans un environnement totalement hors-ligne. La clé privée de l'ACR est générée au sein d'un HSM.

6.1.1.2. Clés des AC Filles

Les clés d'une AC Fille sont générées lors de la cérémonie des clés, en présence d'un représentant de l'AC, du maître de cérémonie des porteurs de secrets.

Les clés privées d'une AC Fille sont générées sur un HSM dans une partition différente des clés de l'ACR.

6.1.2. Transmission de la clé privée à son propriétaire

Sans objet.

6.1.3. Transmission de clé publique à l'AC

La demande de certificat est transmise à l'ACR durant la cérémonie des clés sur un support USB dédié à cet usage.

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

La clé publique de l'ACR est diffusées auprès des utilisateurs sous forme de certificats.

Par ailleurs, l'empreinte numérique du certificat figure sur le site de publication (cf. chapitre 2).

6.1.5. Tailles des clés

RSA 4096 bits pour la taille des clés AC.

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

Voir paragraphe 7.

6.1.7. Objectifs d'usages de la clé

L'utilisation de la clé privée pour l'ACR et du certificat associé est limitée à la signature de certificats d'AC Filles et de LAR.

La clé privée de l'AC Racine n'est utilisée que dans un environnement sécurisé, hors-ligne et actif que pendant la cérémonie des clés.

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 de l'ACR et des AC Filles doivent répondre aux mêmes exigences.

Le stockage de la clé privée est réalisé par le module cryptographique dans les conditions de sécurité définies par le profil de protection support à l'évaluation EAL 4+ et est qualifié par l'ANSSI au niveau renforcé du RGS.

Le module cryptographique ne fait pas l'objet de manipulation non autorisée lors de son transport.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

Le module cryptographique ne fait pas l'objet de manipulation non autorisée lors de son stockage.

Le module cryptographique fonctionne dans les conditions prévues dans la décision de qualification de l'ANSSI.

6.2.2. **Contrôle des clés privées par plusieurs personnes**

Il y a un contrôle de la clé privée par **au moins deux personnes**.

6.2.3. **Séquestre de la clé privée**

Les clés privées ne font pas l'objet de séquestre.

6.2.4. **Copie de secours de la clé privée**

Les clés privées font l'objet de copie de secours dans un environnement du même niveau de sécurité que le site nominal.

6.2.5. **Archivage de la clé privée**

Les clés privées ne font pas l'objet d'archivage.

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

Il n'y a pas de transfert de clé privée en dehors de celui réalisé vers le HSM de secours : ce transfert nécessite la présence d'au moins deux personnes, et est effectué de manière que ne subsiste aucune information sensible sur le serveur.

6.2.7. **Stockage de la clé privée dans le module cryptographique**

Le stockage de la clé privée est réalisé par le module cryptographique dans les conditions de sécurité définies par le profil de protection support à l'évaluation EAL 4+.

6.2.8. **Méthode d'activation de la clé privée**

L'activation de la clé privée ne peut être effectuée que par la personne autorisée, et nécessite la présence de deux personnes au moins.

6.2.9. **Méthode de désactivation de la clé privée**

La clé privée est désactivée à partir du module cryptographique.

6.2.10. **Méthode de destruction des clés privées**

La destruction de la clé privée est effectuée à partir du module cryptographique.

6.2.11. **Niveau d'évaluation sécurité du module cryptographique**

Les modules cryptographiques ont fait l'objet d'une qualification renforcée par l'ANSSI.

6.3. Autres aspects de la gestion des bi clés

6.3.1. **Archivage des clés publiques**

Les clés publiques sont archivées dans le cadre de la politique d'archivage des certificats.

6.3.2. **Durée de vie des bi-clés et des certificats**

Les clés de signature et les certificats de l'ACR ont une durée de vie de **20 ans.**

Les clés de signature et les certificats de l'AC Fille ont une durée de vie de **10 ans.**

6.4. Données d'activation

6.4.1. **Génération et installation des données d'activation**

© APP Solutions | 25 rue de la Plaine, 75020 Paris

L'initialisation et l'utilisation des données d'activation des clés d'AC se font dans le cadre d'une cérémonie des clés qui fait l'objet d'une attestation formelle à travers procès-verbal de cérémonie des clés. Ce procès-verbal est conservé par l'AC.

6.4.2. Protection des données d'activation

Les données d'activation sont remises directement au porteur de secrets qui en assure l'intégrité et la confidentialité.

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

6.5.1.1. Identification et authentification

Les systèmes informatiques de l'IGC identifient et authentifient de façon unique les utilisateurs. Toute interaction entre le système et un utilisateur n'est possible qu'après une identification et une authentification réussie. Pour chaque interaction, le système peut établir l'identité de la source de l'événement.

Les informations d'authentification sont stockées de façon telle qu'elles soient seulement accessibles par des utilisateurs autorisés.

L'accès aux interfaces de gestion des certificats nécessitent une authentification forte basée sur au moins deux facteurs.

6.5.1.2. Contrôle d'accès

Les profils et droits d'accès aux équipements de l'IGC sont définis et documentés, ainsi que les procédures d'enregistrement et de désenregistrement des utilisateurs.

Dans tous les cas une personne non habilitée ne peut accéder aux composants de l'IGC sans l'accompagnement d'une personne habilitée.

Les systèmes informatiques de l'IGC peuvent distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. Il est possible de :

- Refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet ;
- Limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas cet objet ;
- Accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel.

Quelqu'un qui n'est pas un utilisateur autorisé ne peut pas accorder ou retirer des droits d'accès à un objet. De même, seuls des utilisateurs autorisés peuvent introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.

Les supports utilisés par les intervenants autorisés de l'IGC sont manipulés conformément aux exigences du plan de classification.

6.5.1.3. Administration et exploitation

L'utilisation de programmes utilitaires est restreinte et contrôlée.

Les procédures opérationnelles d'administration et exploitation de l'IGC sont documentées, suivies et régulièrement mises à jour.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

Les conditions de mise en service (paramétrage initial de sécurité des serveurs) sont documentées. Les configurations mises en œuvre permettent de renforcer le niveau de sécurité des systèmes en appliquant des mesures de durcissement.

Les conditions de fin de vie (destruction et mise au rebus) des équipements sont documentés afin de garantir la non-divulgation des informations sensibles qu'ils peuvent détenir.

L'ensemble des matériels sensibles de l'IGC fait l'objet de procédure de maintenance afin de garantir la disponibilité des fonctions et des informations. Les procédures sont documentées.

Les personnels concernés par ces procédures sont désignés formellement.

Des mesures de contrôles des actions de maintenance sont mises en application.

6.5.1.4. Intégrité des composantes

Des mesures de maîtrise de détection et de prévention sont mises en œuvre sur l'ensemble des composants de l'IGC afin de fournir une protection contre les logiciels malveillants.

Les composantes réseau de l'IGC sont maintenues dans un environnement physiquement sécurisé ; des vérifications périodiques de conformité de leur configuration sont effectuées.

Des tests réguliers de pénétration et de détection de vulnérabilités sont réalisés sur l'ensemble des composantes techniques de l'IGC.

6.5.1.5. Sécurité des flux

Des mesures de sécurité sont mises en œuvre de manière à garantir l'authentification d'origine, l'intégrité et la confidentialité le cas échéant des données échangées entre composantes intervenant de l'IGC.

6.5.1.6. Journalisation et audit

Un suivi d'activité est possible au travers des journaux d'événements. Tous les événements liés à la sécurité des systèmes sont journalisés.

Les systèmes sont synchronisés sur l'heure UTC à la seconde près.

6.5.1.7. Supervision et contrôle

Une surveillance permanente est mise en place et des systèmes d'alarme installés pour détecter, enregistrer et réagir rapidement face à toute tentative non autorisée et ou irrégulière d'accès aux ressources (physique et / ou logique).

6.5.1.8. Sensibilisation

Des procédures appropriées de sensibilisation des utilisateurs de l'IGC sont mises en œuvre.

Lorsqu'une faille de sécurité est observée sur une des composantes de l'IGC, les personnes concernées sont mises au courant de l'impact de cette faille, et un plan d'action est défini pour couvrir cette faille sous un délai raisonnable.

6.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Sans objet.

6.6. Mesures de sécurité liées au développement des systèmes

Les infrastructures de développement et d'essai sont séparées des infrastructures opérationnelles de l'IGC.

Les critères de recette et validation de nouveaux systèmes d'information, de mises à niveau et nouvelles versions sont établis et des essais adéquats du système sont effectués avant sa recette et sa mise en production.

Un plan de capacité est établi pour garantir le bon traitement des certificats émis par l'ACR.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

6.6.1. **Mesures liées à la gestion de la sécurité**

Toute modification significative d'une des composantes de l'IGC est suivi par le COPIL.

Les évolutions des composantes font l'objet d'une remise à jour des procédures opérationnelles.

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

Sans objet.

6.7. Mesures de sécurité réseau

Les équipements de filtrage en amont des composantes de l'IGC interdisent tous les flux par défaut. Une matrice des flux est établie et une revue est organisée sur demande du COPIL.

Des scans périodiques de détection de vulnérabilités sur les équipements de l'IGC accessibles depuis Internet sont conduits.

Des passerelles de sécurité sont mises en place afin de protéger les composantes de l'IGC des accès non autorisés depuis l'Intranet et Internet.

La redondance des accès sur les services de l'IGC exposés sur Internet est assurée.

6.8. Horodatage / système de datation

Les composants de l'IGC sont synchronisés sur le temps UTC.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

7. Profils des certificats AC et des LCR

7.1. Certificat de l'AC RACINE VAULTINUM

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Numéro unique de taille 20 octets 09:a9:4a:0b:48:13:b3:26:1e:48:c9:50:78:79:11:72:ae:56:32:4f		
Issuer DN	C = FR O = APP SOLUTIONS OI = NTRFR-519136170 CN= VAULTINUM – ROOT CA		
NotBefore	Jun 6 09:38:38 2023 GMT (date de la cérémonie des clés)		
NotAfter	Jun 6 09:38:38 2043 GMT (date de la cérémonie des clés + 20 ans)		
Subject DN	Attribute type	Attribute value	Directory String
	C	FR	PrintableString
	O	APP SOLUTIONS	UTF8String
	OI	NTRFR-519136170	UTF8String
	CN	VAULTINUM - ROOT CA	UTF8String
Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)		
Key size	4096		
Signature (algorithm & OID)	Sha512WithRSAEncryption (1.2.840.113549.1.1.13)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		31:CF:A8:4B:39:37:D4:99:8D:7B:1B:52:60:25:FA:CB:7C:87:BB:EF
Subject Key Identifier	**FALSE**	
Methods of generating key ID		31:CF:A8:4B:39:37:D4:99:8D:7B:1B:52:60:25:FA:CB:7C:87:BB:EF
Key Usage	**TRUE**	
keyCertSign		Set

© APP Solutions | 25 rue de la Plaine, 75020 Paris

Extensions	Criticality (True/False)	Value
cRLSign		Set
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		None

7.2. Profils des certificats d'AC Filles

7.2.1. Certificat de l'AC HORODATAGE

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Numéro unique de taille 20 octets 36:a6:a4:6d:dd:0d:4d:1c:b0:77:ef:e2:0e:7c:33:81:87:a0:d3:5f		
Issuer DN	C = FR O = APP SOLUTIONS OI = NTRFR-519136170 CN = VAULTINUM - ROOT CA		
NotBefore	Oct 5 13:51:10 2023 GMT (date de la cérémonie des clés)		
NotAfter	Oct 5 13:51:10 2033 GMT (date de la cérémonie des clés + 10 ans)		
Subject DN	**Attribute type**	**Attribute value**	**Directory String1**
	C	FR	PrintableString
	O	APP SOLUTIONS	UTF8String
	OI	NTRFR-519136170	UTF8String
	CN	VAULTINUM - TIMESTAMP CA	UTF8String
Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)		
Key size	4096		
Signature (algorithm & OID)	Sha512WithRSAEncryption (1.2.840.113549.1.1.13)		

© APP Solutions | 25 rue de la Plaine, 75020 Paris

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		31:CF:A8:4B:39:37:D4:99:8D:7B:1B:52:60:25:FA:CB:7C:87:BB:EF
Subject Key Identifier	**FALSE**	
Methods of generating key ID		DA:3A:2C:7B:87:8C:4A:3C:B5:3F:95:92:1B:BC:E8:FE:EA:AA:0C:F4
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
Certificate Policies	**FALSE**	
policyIdentifiers		anyPolicy (2.5.29.32.0)
Authority Information Access	**FALSE**	
caIssuer		http://ts-pub.vaultinum/cer/root-ca.cer
CRL Distribution Points	**FALSE**	
distributionPoint		http://ts-pub.vaultinum/crl/root-ca.crl

7.3. Profils des LAR

Field	Value
Version	1 (Version=2)
Issuer DN	C = FR O = APP SOLUTIONS OI = NTRFR-519136170 CN= VAULTINUM – ROOT CA
ThisUpdate	YYMMDDHHMMSS (date d'émission de l'ARL)
NextUpdate	YYMMDDHHMMSS (date d'émission de l'ARL + 365 jours)
Signature (algorithm & OID)	Sha512WithRSAEncryption (1.2.840.113549.1.1.13)
Revoked Certificate	userCertificate : Serial Number du certificat d'AC révoqué revocationDate : date de révocation du certificat au format UTCTime crlEntryExtensions : aucune extension d'entrée n'est utilisée

© APP Solutions | 25 rue de la Plaine, 75020 Paris

CRL Extension	Include	Critical (True/False)	Value
CRL number	Yes	False	Integer incremented, start = 1
Authority Key Identifier	Yes	False	Issuer key hash

8. Audit de conformité et autres évaluations

8.1. Fréquences et / ou circonstances des évaluations

Un contrôle de conformité à la PC lors de la mise en œuvre opérationnelle du système, et lors de toute modification significative est effectué à travers un audit interne biannuel.

Cet audit interne est mené par des équipes internes de la « Société » ou bien à travers des prestations externes.

8.2. Identités : qualification des évaluateurs

L'auditeur est rigoureux pour s'assurer que les politiques, déclarations et services sont correctement mis en œuvre et détecter les cas de non-conformités qui pourraient compromettre la sécurité du service offert.

8.3. Relations entre évaluateurs et entités évaluées

L'auditeur est désigné par l'AC. Il est indépendant de l'entité opérant la composante de l'IGC contrôlée.

8.4. Périmètre des évaluations

L'auditeur procède de manière biannuelle à des contrôles de conformité de la mise en œuvre :

- Des politiques de certification
- Des déclarations de pratique de certification
- Des services mis en œuvre

Il a notamment pour objectif de s'assurer que les pratiques mises en œuvre permettent de répondre aux exigences attendues par les niveaux de qualification obtenus par l'AC. Il s'assure également que les processus de gestion du cycle de vie des certificats sont conformes aux procédures rédigées.

8.5. Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'auditeur rend à l'AC un avis qui peut être « réussite, échec, ou à confirmer ».

En cas d'échec, l'équipe d'audit remet des recommandations à l'AC ; le choix des mesures à appliquer appartient à l'AC.

En cas de résultat « à confirmer », l'équipe d'audit identifie les non-conformités, et les hiérarchisent ; il appartient au COPIL de proposer un calendrier de résolution des non-conformités ; un contrôle de vérification permettra de lever les non-conformités identifiées.

En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC.

8.6. Communication des résultats

Dans le cas d'une qualification de l'AC, les résultats d'audits sont tenus à la disposition de l'organisme en charge de la qualification.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

9. Autres problématiques métiers et légales

9.1. Tarifs

Sans objet.

9.2. Responsabilité financière

9.2.1. **Couverture par les assurances**

L'AC prend les dispositions nécessaires pour couvrir, éventuellement financièrement, ses responsabilités liées à ses opérations et/ou activités.

9.2.2. **Autres ressources**

« La société » reconnaît disposer d'une garantie financière suffisante spécialement affectée à la couverture des risques financiers sur les activités de l'AC.

9.2.3. **Couverture et garantie concernant les entités utilisatrices**

Pas d'exigence spécifique.

9.3. Confidentialité des données professionnelles

9.3.1. **Périmètre des informations confidentielles**

L'AC met en place un inventaire de tous les biens informationnels et procèdent à une classification de manière à définir des exigences de protection en accord avec les besoins.

En particulier, les informations suivantes sont traitées comme confidentielles :

- Les clés privées d'AC ;
- Les scripts de cérémonies ;
- Les codes d'activation des parts de secrets ;
- Les journaux d'événements ;
- La DPC et les procédures internes de l'AC ;
- Les dossiers de demande de certificats d'AC ;
- Les causes de révocation des certificats.

9.3.2. **Informations hors du périmètre des informations confidentielles**

Sans objet.

9.3.3. **Responsabilités en termes de protection des informations confidentielles**

L'AC s'engage à traiter (et à faire traiter par les différentes parties prenantes) les informations confidentielles recueillies dans le respect des lois et règlements en vigueur.

9.4. Protection des données personnelles

L'ACR d'Horodatage ne traite pas de donnés à caractère personnel.

9.5. Droits sur la propriété intellectuelle et industrielle

La fourniture de service par l'AC ne saurait être interprétée comme entraînant la cession d'un quelconque droit de propriété intellectuelle.

9.6. Interprétations contractuelles et garanties

© APP Solutions | 25 rue de la Plaine, 75020 Paris

9.6.1. **Autorités de certification**

Au titre des présentes PC, et pour le domaine qu'elles couvrent (voir paragraphe 1.4), l'AC garantit le respect des engagements décrits dans le présent document.

Sauf à démontrer qu'elle n'a commis aucune faute intentionnelle ou de négligence, l'AC est responsable de tout préjudice causé à toute personne physique ou morale qui s'est fiée raisonnablement aux certificats délivrés dans chacun des cas suivants :

- Les informations contenues dans le certificat ne correspondent pas aux informations fournies lors de l'enregistrement ;
- La délivrance du certificat n'a pas donné lieu à vérification de possession de la clé privée correspondante ;
- L'AC n'a pas fait procéder à l'enregistrement de la révocation d'un certificat, et publié cette information conformément à ses engagements.

Enfin, l'AC engage sa responsabilité en cas de faute ou de négligence dans les précautions à prendre en termes de confidentialité des données personnelles qui lui sont confiées.

9.6.2. **Autorité d'enregistrement**

Voir paragraphe 1.3.2.

9.6.3. **Utilisateurs de certificats**

Les utilisateurs des certificats doivent :

- Vérifier l'usage pour lequel le certificat a été émis ;
- Contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- Vérifier la signature des certificats de la chaîne d'AC et contrôler la validité des certificats.

9.6.4. **Autres participants**

Sans objet.

9.7. Limite de garanties

L'AC ne pourra pas être tenue pour responsable de tout dommage résultant de réclamation par des tiers, de perte de clientèle, d'arrêt de travail ou de tout autre dommage, notamment indirects ou perte commerciale.

9.8. Limite de responsabilité

L'AC n'est pas responsable du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation.

L'AC ne pourra pas être tenue pour responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées, des LAR ainsi que de tout autre équipement ou logiciel mis à disposition.

9.9. Indemnités

Sans objet.

9.10. Durée et fin anticipée de validité de la PC

9.10.1. **Durée de validité**

Le présent document est applicable jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

9.10.2. Fin anticipée de validité

Sauf événement exceptionnel lié à la sécurité, les évolutions du présent document n'imposent pas la révocation des certificats déjà émis.

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

La fin de validité des présentes PC rend caduques les engagements de l'AC qui y sont portés, à l'exception des clauses traitant de la fin de vie des services de l'AC, de l'archivage et du transfert d'activité.

9.11. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition des services de l'AC, l'AC s'engage à :

- Au plus tard 6 mois avant le début de l'opération, faire valider par le COPIL ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'IGC et de ses différentes composantes.
- Au plus tard 1 mois après la fin de l'opération, en informer, le cas échéant, l'organisme de qualification.

9.12. Amendements à la PC

9.12.1. Procédures d'amendements

Tout amendement de la PC devra être soumis au COPIL.

9.12.2. Mécanisme et période d'information sur les amendements

Toute nouvelle version est disponible en format électronique sur le site Internet identifié au chapitre 2 et dans un délai maximum de 24 heures suite à son approbation par le COPIL. Elle prend effet dès sa publication.

9.12.3. Circonstances selon lesquelles l'OID doit être changé

Toute évolution majeure de la PC ayant un impact majeur sur les certificats déjà émis sera signifiée par une évolution de l'OID.

9.12.4. Informations aux utilisateurs

Toute nouvelle version de la présente Politique de Certification fera l'objet d'une information sur le site Internet identifié au chapitre 2 à destination des porteurs et des applications utilisatrices.

Cette information sera préalable à toute émission d'un certificat final conforme aux nouvelles exigences de la nouvelle Politique de Certification.

9.13. Dispositions concernant la résolution de conflits

Conformément aux textes législatifs et à la réglementation en vigueur, les certificats émis en vertu de la présente Politique de Certification sont des certificats dont les conditions d'utilisation sont définies par la présente Politique ce Certification et par les conditions générales d'utilisation qui définissent les relations entre les différentes parties prenantes.

9.14. Juridictions compétentes

La présente Politique de Certification est soumise au droit français.

Tout litige relatif à la validité, l'interprétation, l'exécution de la présente Politique de Certification sera soumis aux tribunaux compétents de la cour d'appel de Paris.

9.15. Conformité aux législations et réglementations

© APP Solutions | 25 rue de la Plaine, 75020 Paris

En sus de la règlementation RGPD, l'AC vise une conformité aux normes ETSI 319401 et ETSI 319411-1.

9.16. Dispositions diverses

9.16.1. Accord global

Pas d'exigence spécifique.

9.16.2. Transfert d'activités

Sans objet.

9.16.3. Conséquences d'une clause non valide

Pas d'exigence spécifique.

9.16.4. Application et renonciation

Pas d'exigence spécifique.

9.16.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

9.17. Autres dispositions

Les politiques et procédures de l'AC sont non-discriminatoires.

9.18. Conditions générales d'utilisation

Sans objet.

© APP Solutions | 25 rue de la Plaine, 75020 Paris

10. Documents de référence

[RFC 3647]	RFC 3647. Internet X509 PKI certificate policy and certificate practice statement framework
[eIDAS]	Règlement Européen eIDAS 910/2014
[ISO 9594]	ISO/IEC 9594. Distinguished name
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
[EN 319401]	EN 319401 « General Policy Requirements for Trust Service Providers »
[EN 319411-1]	EN 319411-1 « General requirements »
[EN 319412-1]	EN 319412-1 « Overview and common data structures »
[EN 319412-3]	EN 319412-3 « Certificate profile for certificates issued to legal persons »

© APP Solutions | 25 rue de la Plaine, 75020 Paris

Philippe THOMAS

Certified by yousign