CONSEIL SUPÉRIEUR DU NOTARIAT

PC Gestion des certificats émis par l'AC Notaires de France – Format RFC 3647

Politique de Certification pour les Certificats d'Autorité de Certification émis par l'autorité de certification NOTAIRES DE FRANCE

PC NOTAIRES DE FRANCE

Statut du document : Standard
Version : 01.3
Date de la dernière mise à jour :16/05/2019

PUBLIÉ

Entrée en vigueur le 02/03/2017

Historique du document

16/05/2019

Version : 01.3, Standard

Changement REAL.NOT en ADSN

21/02/2017

Version : 01.2, Standard

Prise en compte des remarques de l'audit à blanc CSN

13/12/2016

Version : 01.1, Standard

Prise en compte des remarques de l'audit à blanc CSN

21/06/2016

Version : 01.0, Standard

Création du document

Table des matières

1. Introduction

1.1. Présentation générale

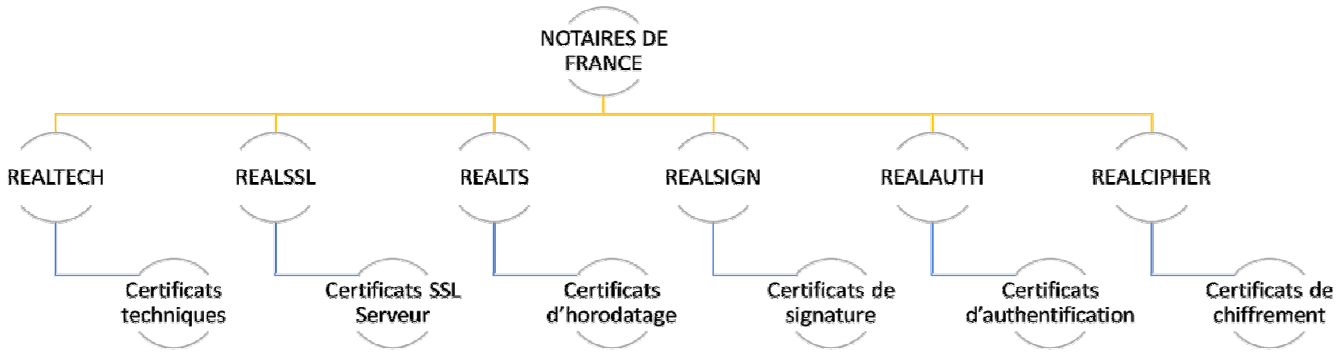
Le Conseil Supérieur du Notariat s'est positionné comme prestataire de service de certification électronique à destination des Notaires de France, en offrant des services supports à la signature de manière à permettre aux Notaires d'élaborer des actes authentiques dématérialisés et plus généralement de sécuriser l'ensemble de leurs échanges.
Pour ce faire, une hiérarchie de certification a été mise en place, qui est présentée dans le paragraphe 2.3. La présente politique de certification définit les exigences relatives à l'AC NOTAIRES DE FRANCE. Il s'agit de l'autorité de certification racine permettant de signer les certificats d'autorités de certification intermédiaires.
Sa structure est conforme au RFC 3647, [A1].

1.2. Identification du document

Le numéro d'OID du présent document est 1.2.250.1.78.2.1.1.1

1.3. Entités intervenant dans l'IGC

Le certificat de l'AC NOTAIRES DE FRANCE est un certificat auto-signé, base de la confiance de la hiérarchie de certification du Notariat mise en œuvre. L'AC NOTAIRES DE FRANCE signe les différentes AC Filles mises en œuvre par le Notariat.
La hiérarchie d'Autorités de Certification mise en œuvre est la suivante :



Le prestataire de service de certification électronique (PSCE) est le Conseil Supérieur du Notariat (CSN). Le CSN est également l'autorité de certification (AC) à laquelle les utilisateurs des services de certification accordent leur confiance pour la création et l'émission des certificats.
Le CSN a recourt à ADSN en tant qu'Opérateur de Service de Certification (OSC), pour opérer les fonctions de gestion des certificats.

1.3.1. Autorités de certification

L'Autorité de certification est le CSN. Elle est en charge de l'application de la présente politique de certification. L'autorité de certification est en charge de la réalisation des fonctions d'enregistrement.
Elle peut déléguer la réalisation de ces étapes à l'Opérateur de Service de Certification. Les opérations de validation d'une demande de certificat racine sont réalisées lors d'une cérémonie des clés validées par le CSN.

1.3.2. Opérateur de Service de Certification

L'opérateur de service de certification est ADSN. Il est en charge des :

- Fonctions d'enregistrement ;

- Fonctions de génération des certificats ;
- Fonction de remise des éléments secrets aux porteurs de secrets ;
- Fonction de publication ;
- Fonction de gestion des révocations ;
- Fonction d'information sur l'état des certificats ;
- Fonction de mise en œuvre opérationnelle des clés privées d'AC racine sur ses centres de production.

1.3.3. Autorité d'enregistrement

Les fonctions d'enregistrement sont assurées directement par l'AC dans le cadre de l'organisation d'une cérémonie des clés.

1.3.4. Mandataires de certification

Sans objet.

1.3.5. Porteurs de certificats

Le porteur des AC Filles est le Conseil Supérieur du Notariat (CSN).

1.3.6. Utilisateurs de certificats

Toute application faisant confiance à la chaîne de certification émise par l'AC NOTAIRES DE FRANCE est un utilisateur du certificat de cette AC racine.

1.4. Usage des certificats

1.4.1. Domaines d'utilisation applicables

La présente politique de certification traite de la bi-clé et du certificat de l'AC NOTAIRES DE FRANCE utilisées exclusivement pour :

- Signer des demandes de certificats pour les AC Filles ;
- Signer les ARL correspondantes ;

1.4.2. Domaines d'utilisation interdits

Les certificats de l'AC NOTAIRES DE FRANCE ne peuvent pas être utilisés en dehors des usages définis dans le paragraphe 1.4.1.

1.5. Gestion de la PC

1.5.1. Entité gérant la PC

La gestion de la PC est de la responsabilité du CSN.

1.5.2. Point de contact

Membre du bureau du CSN, chargé des technologies de l'information et de la communication
60 Boulevard de la Tour Maubourg
75007 Paris
01 44 90 30 00

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

Le CSN est en charge des opérations internes de contrôle de conformité de la DPC à la PC.

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

L'approbation de la conformité de la DPC à la Politique de certification est prononcée par le CSN, au vu des audits internes effectués.

1.6. Définitions et acronymes

1.6.1. Acronymes

AC	**A**utorité de **C**ertification
CSN	**C**onseil **S**upérieur du **N**otariat
DPC	**D**éclaration de **P**ratiques de **C**ertification
ETSI	Institut européen des normes de télécommunication (**E**uropean **T**elecommunications **S**tandards **I**nstitute)
IGC	**I**nfrastructure de **G**estion de **C**lés
LCR	**L**iste des **C**ertificats **R**évoqués
OID	Identifiant d'objet (**O**bject **ID**entifier)
OSC	**O**pérateur de **S**ervice de **C**ertification
PC	**P**olitique de **C**ertification
PSCE	**P**restataire de **S**ervice de **C**ertification **E**lectronique

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
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 ka clé privée de l'autorité de certification qui l'a délivré.

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

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 associées à un porteur permettant d'initialiser ses éléments secrets.

Infrastructure de Gestion de Clés

Ensemble de composantes fournissant des services de gestion de clés et de certificats au profit d'une communauté d'utilisateurs.

Liste de Certificats Révoqués
Liste contenant les identifiants des certificats révoqués ou invalides.

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

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

2.1. Entités chargées de la mise à disposition des informations

L'AC est chargée de la mise à disposition de la politique de certification.

Ces informations sont accessibles via Internet, sur le site https://www.preuve-electronique.org.

L'accès à ce service est assuré 24h/24 et 7j/7.

La mise à disposition des informations sur l'état des certificats est du ressort de l'OSC. Ces informations sont accessibles sur l'Intranet au travers de l'annuaire de publication des LCR par LDAP, et sur Internet sur le site https://www.preuve-electronique.org.

2.2. Informations devant être publiées

Les informations publiées sont les suivantes :

- La présente politique de certification ;
- Le document présentant les profils des certificats et CRL ;
- La liste des autorités révoquées (LAR) ;
- Le certificat de l'AC NOTAIRES DE FRANCE en cours de validité ;
- Les informations permettant aux utilisateurs de s'assurer de l'origine et de l'état des certificats de l'AC NOTAIRES DE FRANCE (certificats auto signés) en faisant une demande auprès du point de contact identifié au paragraphe 1.5.2.

Les documents PC sont publiés au format PDF/A.

2.3. Délais et fréquences de publication

Les politiques de certification sont remises à jour et publiées tous les deux ans.
Les certificats d'AC sont diffusés ou mis en ligne préalablement à toute diffusion de certificats ou de LAR, dans un délai de 24 heures suivant sa génération.

Les LAR sont établies tous les six (6) mois et après chaque révocation de certificat d'AC.
Elles sont publiées dans un délai de :

- 1 heure sur l'Intranet REAL à partir du point d'accès ldap://annuaire.real.notaires.fr et ldaps://annuaire.real.notaires.fr;
- 2 heures sur l'Internet à partir du point d'accès https://www.preuve-electronique.org.

2.4. Contrôle d'accès aux informations publiées

Les PC et LAR sont accessibles en lecture de manière internationale à toute personne souhaitant en prendre connaissance sur le site https://www.preuve-electronique.org.
Les ajouts, suppressions et modifications des informations publiées se font au travers d'un processus automatisé qui fait l'objet d'une demande formelle par les personnes autorisées de l'AC ou de l'OSC. Ces demandes sont tracées.

3. Identification et authentification

3.1. Nommage

3.1.1. Types de noms

Les noms utilisés dans un certificat sont décrits selon la norme ISO/IEC 9594 (distinguished names), [A3], chaque titulaire ayant un nom distinct (DN).

3.1.2. Nécessité d'utilisation de noms explicites

Les noms pour distinguer les titulaires sont explicites. Le nom distinctif est sous la forme d'une chaîne de type UTF8string de type nom X 501.

3.1.3. Anonymisation ou pseudonymisation des porteurs

Sans objet

3.1.4. Règles d'interprétation des différentes formes de noms

Les règles d'interprétation sont définies dans le document [A4].
Le nom de l'AC NOTAIRES DE FRANCE est défini par le comité de pilotage de l'AC et sous la validation du CSN.

3.1.5. Unicité des noms

Un code distinctif ajouté assure le caractère unique du DN en cas d'homonymie. Ce code correspond à l'année de fin de validité du certificat d'AC.
En cas de certificat d'AC devant être généré avec une même date de fin de validité, un index supplémentaire unique est ajouté (2033-1, 2033-2 par exemple).

3.1.6. Identification, authentification et rôle des marques déposées

Pour les marques, dénominations sociales ou autres signes distinctifs, le CSN 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

La validation de l'identité de la personne à l'origine de la demande de certificat d'AC est effectuée en face à face, lors de la cérémonie des clés.

3.2.1. Méthode pour prouver la possession de la clé privée

La génération des bi clés est effectuée en central par un HSM.
Les clés privées ne sont pas extractibles, et ne signent que des demandes où les clés privées sont générées dans une cérémonie des clés en présence d'un huissier, sous la responsabilité de l'AC.

3.2.2. Validation de l'identité d'un responsable d'AC Filles

La validation de l'identité d'un responsable d'une AC Fille signée par l'AC NOTAIRES DE FRANCE est effectuée lors de la cérémonie des clés et décrite dans le document de cérémonie des clés.

3.2.3. Informations non vérifiées du porteur

Sans objet

3.2.4. Validation de l'autorité du demandeur

En ce qui concerne le demandeur opérant pour une AC Fille signée par l'AC NOTAIRES DE FRANCE, il ne peut s'agir que de la personne autorisée à effectuer cette demande. Cela est validé lors de la cérémonie des clés.

A cette occasion, le maître de cérémonie demande aux personnes présentes de fournir les pièces suivantes :

- Pièce justificative de l'identité (carte d'identité, passeport ou permis de conduire) ;
- Le formulaire de demande de création de l'AC Fille concerné, signé, et détaillant les caractéristiques nécessaire à la génération de ce nouveau certificat d'AC (nom de l'AC, caractéristiques techniques) [R4], contenant :
    - Le nom de l'AC ;
    - Le nom de l'organisation de l'AC et son numéro SIREN ;
    - Le type d'usage de la clé : signature de certificat seulement ou signature de certificat et de Liste de d'Autorités Révoquées (LAR).

Le lancement de la cérémonie des clés est lié à la vérification préalable par le maître de cérémonie du formulaire de demande de création de l'AC Fille.
L'ensemble des actions réalisées durant la cérémonie des clés est conservé et archivé dans le procès-verbal de cérémonie.

3.2.5. Contrôle de l'autorité du demandeur et approbation de la demande

Le contrôle est effectué lors de la cérémonie des clés et est basé sur la vérification formelle de l'identité du demandeur.
L'ensemble des contrôles sont notifiés dans le procès-verbal signé à l'issue de la cérémonie des clés.

3.2.6. Critères d'interopérabilité

Sans objet

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.

3.3.1. Identification et validation pour un renouvellement courant

Identique à une demande initiale.

3.3.2. Identification et validation pour un renouvellement après révocation

Identique à 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'AC NOTAIRES DE FRANCE ne peut émaner que d'une personne autorisée, et est validée formellement avant prise en compte.
Le certificat de l'AC NOTAIRES DE France étant un certificat auto-signé, il ne peut pas être révoqué. En cas de compromission de la clé privée correspondante au certificat de l'AC NOTAIRES DE FRANCE, l'AC publiera une information sur le site www.preuve-electronique.org permettant à tout porteur ou à toute application utilisatrice d'être informé de cette compromission.

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

Une demande de certificat émane de la personne autorisée par l'organisation, présente lors de la cérémonie.

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

L'établissement d'une demande de certificat s'effectue selon une procédure de cérémonie de clés. Les opérations techniques se font dans une salle protégée et prévue à cet effet.

4.2. Traitement d'une demande de certificat

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

Les clés de l'AC NOTAIRES DE FRANCE ne sont mises en œuvre que dans le cadre d'une cérémonie de clés soit pour :

- La signature d'une demande de certificat pour un certificat d'AC Fille
- La signature d'une nouvelle ARL

En dehors de ces phases, les clés de l'AC NOTAIRES DE FRANCE restent hors ligne et stockées dans un coffre-fort.
La génération des clés d'AC se fait lors de la phase de cérémonie des clés en présence d'un représentant de l'AC, des administrateurs techniques de la PKI et des porteurs de secrets. Cette génération se fait dans un environnement dédié à l'AC NOTAIRES DE FRANCE. A l'issue de la cérémonie des clés, cet environnement est sauvegardé et éteint pour être stocké dans un coffre-fort.
Cette cérémonie des clés est constatée par un huissier et des témoins sur la base d'un script de cérémonie des clés établi au préalable.

4.2.2. Acceptation ou rejet de la demande

Toutes les demandes de certificat sont acceptées ou rejetées avant la signature de cette demande par l'AC NOTAIRES DE FRANCE.

4.2.3. Durée d'établissement du certificat

Les certificats des AC Filles signés par l'AC NOTAIRES DE FRANCE sont générés et installés lors de la cérémonie.

4.3. Délivrance du certificat

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

La génération des bi-clés est consignée lors de la cérémonie des clés. Cette génération se fait dans l'environnement dédié à l'AC NOTAIRES DE FRANCE. Cela consiste à faire signer par la bi-clé de l'AC NOTAIRES DE FRANCE la demande de certificat de l'AC Fille. Cette demande de certificat est transmise à l'AC NOTAIRES DE FRANCE via un support physique dédié à cette opération.

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

Le demandeur de certificat est présent lors de la cérémonie des clés.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'acceptation du certificat signé par l'AC NOTAIRES DE FRANCE est consignée sur le procès-verbal de la cérémonie des clés. Le procès-verbal est contresigné par l'huissier présent et remis au responsable de l'AC NOTAIRES DE FRANCE.

4.4.2. Publication du certificat

Le certificat de l'AC NOTAIRES DE FRANCE et des certificats signés par cette AC sont publiés sur l'intranet REAL au travers de l'annuaire LDAP de publication des certificats annuaire.real.notaires.fr, et sur l'Internet sur le site https://www.preuve-electronique.org.

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

Sans objet

4.5. Usage de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat

La clé privée est utilisée pour :

- Signer des certificats d'AC Filles;
- Signer la liste des autorités révoquées ;

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

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 LAR.

4.6. Renouvellement d'un certificat

La notion de renouvellement de certificat, au sens RFC 3647 [A1], correspondant à la seule modification des dates de validité, n'est pas retenue. Seule la délivrance d'un nouveau certificat suite à changement de la bi-clé est autorisée.

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

4.7.1. Cause possible de changement de bi-clé

Les bi-clés des certificats émis par l'AC NOTAIRES DE FRANCE ont une durée de vie de 8 ans. La délivrance d'un nouveau certificat avant la fin de vie ne peut être que la conséquence d'une révocation, ou de la demande de renouvellement au bout de 4 ans pour garantir la continuité de service.

4.7.2. 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.

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

Identique à la demande initiale.

4.7.4. Notification au porteur de l'établissement du nouveau certificat

Identique à la demande initiale.

4.7.5. Démarche d'acceptation du nouveau certificat

Identique à la demande initiale.

4.7.6. Publication du nouveau certificat

Identique à la demande initiale.

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

Identique à la demande initiale.

4.8. Modification du certificat

Les modifications de certificats ne sont pas autorisées.

4.8.1. Cause possible de modification d'un certificat

Sans objet

4.8.2. Origine d'une demande de modification de certificat

Sans objet

4.8.3. Procédure de traitement d'une demande de modification de 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

Les causes de révocation sont les suivantes :

- Obsolescence des informations relatives au porteur 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
- Décision suite à un échec de contrôle de conformité
- Compromission de l'AC NOTAIRES DE FRANCE

4.9.2. Origine d'une demande de révocation

La personne pouvant demander une révocation de certificat est le titulaire du certificat, ou le titulaire de l'AC NOTAIRES DE FRANCE (autorité du CSN).

4.9.3. Procédure de traitement d'une demande de révocation

Le traitement d'une demande de révocation est effectuée par une personne autorisée détentrice des droits correspondants.

4.9.4. Délai accordé au porteur 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.

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

L'AC s'engage à traiter la demande de révocation d'un certificat d'AC dans les meilleurs délais après réception de la demande avec un délai maximal de 24 heures.

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

L'utilisateur d'un certificat est tenu de vérifier l'état des certificats et de la chaîne correspondante (AC NOTAIRES DE FRANCE).

4.9.7. Fréquence d'établissement des LCR

Les LAR sont établies tous les six (6) mois et après chaque révocation de certificat d'AC.

4.9.8. Délai maximum de publication d'une LCR

Les LAR sont publiées dans un délai de :

- 1 heure sur l'Intranet REAL à partir du point d'accès ldap://annuaire.real.notaires.fr et ldaps://annuaire.real.notaires.fr;
- 2 heures sur l'Internet à partir du point d'accès https:// www.preuve-electronique.org.

4.9.9. 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 de 99,5 pour cent, et sont disponibles sous 24 heures.

Le statut de révocation d'un certificat est fourni de manière automatisée au travers des LCR, y compris pour les certificats expirés.
En cas de défaillance du système, l'OSC s'engage à rétablir le système sous 24h. En cas de défaillance en période non ouvrée, la cellule de crise de l'OSC s'activera afin de garantir le rétablissement du système sous 24h.

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

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

Voir 4.9.6

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

Le CSN publiera sur le site https://www.preuve-electronique.org, une information claire de la compromission de la clé privée. L'AC indiquera sur son site les impacts et les précautions à prendre en la matière.

4.9.13. Causes possibles d'une suspension

La suspension de certificat n'est pas prévue.

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

Les LAR sont au format v2, publiées :

- dans un annuaire LDAP v3 accessible au sein de la communauté notariale : ldap ://annuaire.real.notaires.fr:389 et ldaps://annuaire.real.notaires.fr :636;
- sur le site internet https://www.preuve-electronique.org

4.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24, 7 jours sur 7.

4.10.3. Dispositifs optionnels

L'OSC dispose d'une procédure permettant de vérifier l'état de révocation des certificats expirés (date de fin de validité atteinte) à la demande des utilisateurs, envoyée par mail à l'adresse exploitation.carte.real@notaires.fr.
Les modalités de demandes sont décrites sur le site https://www.preuve-electronique.org.

4.11. Fin d'abonnement

Sans objet

4.12. Séquestre de clé et recouvrement

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

4.12.1. Politique et pratiques de recouvrement par séquestre de 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

Les exigences présentées dans ce chapitre résultent de l'analyse de risques réalisée sur l'IGC [R1], et des exigences définies dans le SMSI du CSN validé par son comité de pilotage pour la composante OSC.

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

La localisation géographique des sites ne nécessite pas de mesures particulières face à des 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 du porteur et de gestion des révocations, toutes fonctions opérées par l'OSC, 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, DPC, documents d'applications).

5.1.3. Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre par l'OSC de manière à ce qu'une interruption de service d'alimentation électrique, ou une défaillance de climatisation ne portent pas atteinte aux engagements pris par l'AC 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 devront être 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'AC 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'AC 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'AC, l'OSC met en place des sauvegardes 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. 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

Les rôles de confiance suivant sont définis :

5.2.1.1. AC

Le Responsable Sécurité est chargé de la mise en œuvre de la PC, de ses évolutions, et de sa prise en compte par les différentes structures concernées. Il fait faire les contrôles de conformité, valide les plans d'action relatives aux mesures correctives, … Le Responsable Sécurité est le RSSI du CSN ou son représentant désigné, sous le contrôle direct du président du CSN.

5.2.1.2. AE

L'autorité d'enregistrement est sous la responsabilité du CSN.

5.2.1.3. OSC

Un **Comité de Pilotage** est mis en place, chargé de l'application opérationnelle de la PC au travers de la mise en œuvre des mesures définies dans la DPC concernant particulièrement l'OSC. Le Comité de Pilotage fait réaliser les analyses de risques sur le périmètre dont il a la charge, décide de la stratégie de gestion des risques, valide et suit les plans d'actions correspondants. Il fait réaliser les audits internes sur sa composante, et suit la mise en place des mesures correctives nécessaires.
Les demandes de certificats d'AC Filles sont validées au cours de **cérémonie de clés** qui réunissent :

- Le représentant de l'AC NOTAIRES DE FRANCE
- Le représentant de l'AC Fille
- Les porteurs de secrets correspondants au quorum
- Le responsable de sécurité
- Le maître de cérémonie
- L'administrateur de l'IGC
- L'huissier de justice.

Le **Responsable de la sécurité** est en charge de l'implémentation des pratiques de sécurité. Ce rôle est porté par différentes personnes qui ont en charge la sécurité logique ou la sécurité physique. Le RSSI, responsable de la sécurité globale de l'OSC, est le président de ADSN.
L'administrateur système est en charge de l'installation, la configuration et la maintenance des systèmes de confiance de l'IGC.
L'opérateur système est en charge des actions quotidiennes sur l'IGC, notamment les sauvegardes et les restaurations.
L'Auditeur système dispose d'un rôle qui lui permet d'accéder aux traces systèmes des composantes de l'IGC et de les analyser.
Le Responsable d'application IGC est en charge de la définition, la mise en œuvre, la gestion et le suivi des mesures de sécurité logiques au niveau du réseau et de l'application. Pour ce faire, il s'appuie sur les administrateurs système.
L'Administrateur de l'IGC est un chargé d'applications de ADSN disposant du rôle de confiance Ingénieur / Administrateur Système.

Des **porteurs de secrets** sont également définis pour l'AC NOTAIRES DE FRANCE. Chacun possède une part du secret permettant d'activer le HSM détenant la clé privée de l'AC.

5.2.2. Nombre de personnes requises par tâche

Toute tâche sensible est réalisée par deux personnes au moins. La reconstruction du secret de l'AC nécessite le regroupement de 3 personnes parmi 5 chacune 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.

5.2.4. Rôles exigeant une séparation des attributions

Certains rôles de confiance sont dissociés et séparés de tout autre rôle de confiance.
Un porteur de secrets ne peut détenir qu'une seule part 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 identifié comme sensible est soumis à une clause de confidentialité et de non conflit d'intérêts, gérée par ADSN. En outre les intervenants disposant d'un rôle de confiance attestent sur l'honneur n'avoir commis aucun délit en matière de cybercriminalité.
L'OSC s'assure que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles. Notamment les personnels de l'OSC 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 de confiance. Ces procédures de vérification ne sont pas nécessaires pour les Notaires du fait du caractère assermenté de la profession.

5.3.3. Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement.

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

Se reporter au règlement intérieur.

5.3.7. Exigences vis à vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées. La vérification de l'application des exigences par les prestataires fait l'objet d'audits réguliers.

5.3.8. Documentation fournie au personnel

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 l'infrastructure de gestion de clés disposent des procédures correspondantes.

5.4. Procédures de constitution des données d'audit

5.4.1. Type d'événement à enregistrer

Les événements suivants sont enregistrés :

- Les événements systèmes des différentes composantes de l'IGC (démarrage des serveurs, accès réseau, …) que ce soit sur le site actif ou le site de secours ;
- Les événements techniques des applications composant l'IGC, sur le site actif ou le site de secours ;
- Les événements fonctionnels des applications composant l'IGC (demande de certificats, validation, révocation, …) sur le site actif ou le site de secours ;
- Les évènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- La publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, etc.) ;
- Les opérations effectuées.

Ces journaux permettent d'assurer la traçabilité et l'imputabilité des actions effectuées (horodatage, affectation à l'intervenant).
En dehors de ces événements, l'AC NOTAIRES DE FRANCE maintient à jour un référentiel sur le site www.preuve-electronique.org détaillant :

- Le nom de l'AC NOTAIRES DE FRANCE ;
- Le nom de la personne responsable du certificat.

L'OSC conserve également dans un coffre sécurisé l'ensemble des documents signés durant la cérémonie des clés :

- Le script de cérémonie des clés ;
- Le PV de cérémonie des clés.

N°	Acteur	Description des tâches
1	Maître de cérémonie	Inscription des informations suivantes sur le Procès-verbal : - Nom de l'AC - Nom du responsable de l'AC
2	Maître de cérémonie	Signature du Procès-verbal

3	Porteur de secrets	Signature du Procès-verbal
4	Responsable de l'OSC	Conservation au coffre des éléments suivants : - Script de cérémonie - Procès-verbal signé

5.4.2. Fréquence de traitement des journaux d'événements

L'AC NOTAIRES DE FRANCE est hors-ligne en dehors des opérations de génération des clés d'AC ou des ARL, les journaux sont alors contrôlés à la fin de ces opérations.

5.4.3. Période de conservation des journaux d'événements

Les journaux de l'AC NOTAIRES DE FRANCE sont conservés hors-ligne tant que la base de données de l'IGC n'est pas pleine. Les journaux sont redondés sur deux sites géographiquement distants, la continuité est alors assurée.

5.4.4. Protection des journaux d'événements

Les journaux d'événements sont accessibles uniquement au personnel autorisé de l'OSC. Ils ne sont pas modifiables de manière non autorisée ; des alarmes sont remontées en cas de modification des journaux, ou des paramètres définissant le contenu des journaux.

5.4.5. Procédure de sauvegarde des journaux d'événements

Les évènements réalisés sur l'AC NOTAIRES DE FRANCE sont consignés dans le Procès-Verbal de 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.

5.4.8. Evaluation des vulnérabilités

Le contrôle des journaux des événements fonctionnels peut être réalisé à la demande en cas de litige, ou pour analyse de comportement de l'IGC.

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 et LAR publiés ;
- Formulaires d'engagement des demandes de génération ou de révocation de certificats ;
- 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
Certificats de l'AC NOTAIRES DE FRANCE	23 ans
LAR & Certificats d'AC Fille	23 ans
Evènements techniques	1 an
Evènements fonctionnels	23 ans
Documentation	10 ans
Demandes de génération ou de révocation de certificats	23 ans

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'OSC 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. La durée de conservation et les moyens mis en œuvre sont décrits dans [R4].

5.5.4. Procédure de sauvegarde des archives

Les archives sont sauvegardées de manière sécurisée, certaines en double enregistrement. 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 de l'IGC (hors HSM BULL Proteccio) sont synchronisés sur un même serveur synchronisé avec l'heure universelle.
Dans les cas des opérations hors-ligne l'administrateur PKI procède à la synchronisation manuelle du temps sur la base des informations fournies visuellement par le serveur de temps.

5.5.6. Système de collecte des archives

Sans objet.

5.5.7. Procédure de récupération et de vérification des archives

La récupération et la vérification des archives sont effectuées dans un délai conforme à l'utilisation des certificats délivrés. Un délai d'une semaine est acceptable par la profession.

5.6. Changement de clés d'AC

La durée de vie des clés d'AC Fille est de 8 ans. La durée de vie des certificats émis par ces AC sont de 4 ans. Les clés de l'AC Fille devront être renouvelées au plus tard 4 ans moins 1 jour après la génération des clés de l'AC.
Le certificat de l'AC NOTAIRES DE FRANCE est valable 16 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 – est immédiatement signalé à l'AC. 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 des certificats des AC Filles et des certificats qui leur sont rattachés.
Les cas de compromission des éléments secrets des autres composantes sont traités dans le plan de continuité d'activité.
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'AC et plus particulièrement l'OSC se tiennent continuellement informés 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'AC et l'OSC déclenchent une cellule de crise afin de déterminer les actions à mener pour rétablir le service au plus tôt :

- Par mesure de précaution, l'AC : demande à l'OSC l'arrêt immédiat des services de dématérialisation exploitant la clé REAL ;
- demande à l'OSC de diffuser immédiatement l'information à tous les partenaires par mail.

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

L'OSC est en capacité de reprendre son activité selon le plan de reprise d'activité [R2].

5.8. Fin de vie de l'IGC

5.8.1. Transfert d'activité ou cessation d'activité affectant l'AC et l'OSC

Le CSN n'envisage la cessation de son activité d'Autorité de Certification que dans le cas où un dispositif de signature électronique qualifié et régalien viendrait à être mis en place. Le CSN n'envisage pas le transfert de son activité d'Autorité de Certification.

Dans le cas où ADSN cesserait son activité d'OSC à la demande du CSN, ADSN déroulera la procédure [R5] et maintiendra la disponibilité de la fonction de vérification de l'état des certificats portés par la Clé Real.

Dans le cas où ADSN transférerait son activité d'OSC à une autre société, à la demande du CSN, l'archivage des certificats et des informations relatives aux certificats mis en œuvre permettra de garantir un niveau de confiance constant.

5.8.2. Cessation d'activité affectant l'activité AC du CSN

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

5.8.3. Cessation d'activité affectant l'activité AE du CSN

Dans le cas de la cessation de son activité d'Autorité d'Enregistrement, le CSN s'engage à :

- mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des dossiers des porteurs et des informations relatives aux certificats qu'il détient) ;

- assurer la continuité de la révocation, conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC ;

- informer ses partenaires de cette fin d'activité.

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 NOTAIRES DE FRANCE

Les clés de l'AC NOTAIRES DE FRANCE sont générées lors de la cérémonie des clés, en présence du demandeur, de l'administrateur de l'AC NOTAIRES DE FRANCE, du tiers enregistrant la demande et du maître de cérémonie.
Cette cérémonie de clé se fait dans un environnement totalement hors-ligne. La clé privée de l'AC NOTAIRES DE FRANCE est générée dans un HSM dédié.

6.1.1.2. Clés des AC Filles signées par l'AC NOTAIRES DE FRANCE

Les clés de l'AC Fille sont générées lors de la cérémonie des clés, en présence du demandeur, de l'administrateur de l'AC NOTAIRES DE FRANCE et de l'AC fille, du tiers enregistrant la demande et du maître de cérémonie.
Les clés privées des AC filles sont générées dans un environnement online et la signature du certificat de l'AC fille est réalisée hors ligne par l'AC NOTAIRES DE FRANCE. Les clés privées des AC Filles sont générées dans un HSM partagé mais dans une partition dédiée.

6.1.2. Transmission de la clé privée à son propriétaire

La clé privée de l'AC NOTAIRES DE FRANCE est hébergée sur un module HSM dédié aux cérémonies des clés de l'AC NOTAIRES DE FRANCE.
La clé privée des AC Filles est stockée dans un HSM mutualisé par l'ensemble des AC Filles.

6.1.3. Transmission de clé publique à l'AC

La demande de certificat technique est transmise à l'AC 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

Les clés publiques de vérification de signature de l'AC sont diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et en garantit l'authentification d'origine.

6.1.5. Tailles des clés

Les clés de l'AC NOTAIRES DE FRANCE ont une taille de 4096 bits.
Les clés des certificats des AC Filles ont une taille de 4096 bits.

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

Voir 7.

6.1.7. Objectifs d'usages de la clé

L'utilisation de la clé privée pour l'AC NOTAIRES DE FRANCE et du certificat associé est limitée à la signature de certificats d'AC Filles, de LAR, comme définie dans le document description des certificats et des CRL [A4].
La clé privée de l'AC NOTAIRES DE FRANCE 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

6.2.1.1. Module cryptographique de l'AC NOTAIRES DE FRANCE

Le module cryptographique de signature de l'AC NOTAIRES DE FRANCE est évalué EAL 4+.

6.2.1.2. Modules cryptographiques des certificats d'AC Fille

Le module cryptographique de signature des AC Filles signées par l'AC NOTAIRES DE FRANCE est évalué EAL 4+.

6.2.2. Contrôle des clés privées par plusieurs personnes

6.2.2.1. Module cryptographique de l'AC

Il y a un contrôle de la clé privée de l'AC NOTAIRES DE FRANCE par au moins trois personnes.

6.2.2.2. Module cryptographique des AC Filles

Il y a un contrôle de la clé privée de l'AC NOTAIRES DE FRANCE par au moins trois personnes.

6.2.3. Séquestre de la clé privée

La clé privée de l'AC NOTAIRES DE FRANCE ne fait pas l'objet de séquestre.

6.2.4. Copie de secours de la clé privée

La clé privée de l'AC NOTAIRES DE FRANCE fait l'objet d'une réplication sur l'ordinateur dédié aux cérémonies de clés qui se trouve dans un coffre-fort. Cette copie est chiffrée par le HSM et ne peut être mise en œuvre que sur le même HSM dont le contexte cryptographique est initialisé à partir du secret de l'AC.

6.2.5. Archivage de la clé privée

Les clés privées des AC font l'objet d'un archivage chiffré dans un coffre sécurisé.

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

6.2.6.1. Transfert de la clé privée de l'AC NOTAIRES DE FRANCE

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 trois personnes, et est effectué de manière à ce que ne subsiste aucune information sensible sur le serveur.

6.2.6.2. Transfert de la clé privée d'un certificat d'AC Fille

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 trois personnes, et est effectué de manière à ce que ne subsiste aucune information sensible sur le serveur.

6.2.7. Stockage de la clé privée dans le module cryptographique

6.2.7.1. Stockage de la clé privée de l'AC NOTAIRES DE FRANCE

Le stockage de la clé privée de l'AC NOTAIRES DE FRANCE est réalisé par le module cryptographique dans les conditions de sécurité définies par le profil de protection support à l'évaluation EAL 4+ et par les exigences support à la qualification renforcée de l'ANSSI.

6.2.7.2. Stockage de la clé privée d'un certificat d'AC Fille

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

6.2.8. Méthode d'activation de la clé privée

6.2.8.1. Activation de la clé privée de l'AC NOTAIRES DE FRANCE

L'activation de la clé privée de l'AC NOTAIRES DE FRANCE ne peut être effectuée que par la personne autorisée, et nécessite la présence de trois personnes au moins.

6.2.8.2. Activation de la clé privée d'un certificat d'AC Fille

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

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Désactivation de la clé privée de l'AC NOTAIRES DE FRANCE

La clé privée est désactivée à partir du module cryptographique.

6.2.9.2. Désactivation de la clé privée d'un certificat d'AC Fille

La clé privée est désactivée à partir du module cryptographique.

6.2.10. Méthode de destruction des clés privées

6.2.10.1. Destruction de la clé privée de l'AC NOTAIRES DE FRANCE

La clé privée est détruite à partir du module cryptographique à l'aide des commandes décrites par l'éditeur. La destruction signifie dans ce cadre l'impossibilité de réutiliser par la suite les éléments secrets préalablement générés.

6.2.10.2. Destruction de la clé privée d'un certificat d'AC Fille

La clé privée est détruite à partir du module cryptographique à l'aide des commandes décrites par l'éditeur. La destruction signifie dans ce cadre l'impossibilité de réutiliser par la suite les éléments secrets préalablement générés.

6.2.11. Niveau d'évaluation sécurité du module cryptographique

6.2.11.1. Module cryptographique de l'AC NOTAIRES DE FRANCE

Le module cryptographique a fait l'objet d'une évaluation EAL 4+ et d'une qualification renforcée de l'ANSSI.

6.2.11.2. Module cryptographique d'un certificat d'AC Fille

Le module cryptographique a fait l'objet d'une évaluation EAL 4+ et d'une qualification renforcée de l'ANSSI.

6.3. Autres aspects de la gestion des bi clés

6.3.1. Archivage des clés publiques

Les clés publiques de l'AC NOTAIRES DE FRANCE 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'AC NOTAIRES DE FRANCE ont une durée de vie de seize ans.
Les bi-clés de et les certificats des AC Filles ont une durée de vie de huit ans.

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

6.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC NOTAIRES DE FRANCE

Les éléments nécessaires à l'activation de la clé privée de l'AC NOTAIRES DE FRANCE sont générés de manière sécurisée, et uniquement accessibles aux personnes autorisées à procéder à cette activation.

6.4.1.2. Génération et installation des données d'activation correspondant à la clé privée des AC Filles

Les éléments nécessaires à l'activation des clés privées des AC Filles sont générés de manière sécurisée, et uniquement accessibles aux personnes autorisées à procéder à cette activation.

6.4.2. Protection des données d'activation

Les données d'activation des clés d'AC ne sont délivrées qu'à la personne autorisée sous la forme d'un support cryptographique (démarrage de HSM) ou de code pin (création de bi-clé).

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, applications et bases de données 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 réussies. Pour chaque interaction, le système peut établir l'identité de l'entité.
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'OSC 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 du PSCE sans l'accompagnement d'une personne habilitée.
Les systèmes [Applications et bases de données] 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'OSC 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.
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 mesures sont décrites dans la DPC [R4].
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 du PSCE afin de fournir une protection contre les logiciels malveillants.
Les composantes du réseau local (OSC) 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'OSC.

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 entités intervenant dans le processus.

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. Le détail des événements concernés sont décrits dans la DPC [R4].

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 usagers du PSCE sont mises en œuvre.
Lorsqu'une faille de sécurité est observée sur une des composantes de l'OSC, les personnes concernées sont mise 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'AC.

6.6.1. Mesures liées à la gestion de la sécurité

L'IGC est suivie dans le cadre de la mise en place du système de management de la sécurité de l'OSC. Le comité de pilotage gère la remontée d'information vers l'AC qui est averti de toute modification significative.
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

Des revues de processus mensuelles permettent de s'assurer du maintien du niveau de sécurité et des améliorations à apporter.

6.7. Mesures de sécurité réseau

Les mesures mises en place répondent à l'analyse de risques effectuée sur le système d'information [R1].
Les communications réseau véhiculant des informations confidentielles font l'objet de mesures de protection contre l'écoute des informations. Les composants réseaux correspondants sont hébergés dans un environnement sûr.
Des scans périodiques de détection de vulnérabilités sur les équipements du PSCE accessibles depuis l'Intranet ou l'Internet sont conduits.
Des passerelles de sécurité sont mises en place afin de protéger la composant locale du système d'information des accès non autorisés depuis l'Intranet et Internet.
La redondance des accès sur les services du PSCE exposés sur Internet est assurée.

6.8. Horodatage / système de datation

Cf. 5.5.5.

7. Profils des certificats, OCSP et des CRL

7.1. Profils des certificats

7.1.1. Numéro de version

7.1.2. Extensions de certificat

7.1.3. OID des algorithmes

7.1.4. Forme des noms

7.1.5. Contrainte sur les noms

7.1.6. OID des PC

7.1.7. Utilisation de l'extension contraintes de politique

7.1.8. Sémantique et syntaxe des qualifiants de politique

7.1.9. Sémantiques de traitement des extensions critiques de la PC

7.2. Profil des listes de certificats révoqués

7.2.1. Numéro de version

7.2.2. Extensions de CRL et d'entrées de CRL

7.3. Profil OCSP

7.3.1. Numéro de version

7.3.2. Extensions OCSP

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 annuel.

8.2. Identités : qualification des évaluateurs

Le contrôleur sont 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

Le contrôleur est désigné par l'AC. Il est indépendant de l'AC, de l'AE et de l'OSC.

8.4. Périmètre des évaluations

Le contrôleur procède de manière régulière 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

8.5. Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit 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 à l'AC 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.

9. Autres problématiques métiers et légales

9.1. Tarifs

L'AC peut imposer des frais notamment pour :

- L'émission ou le renouvellement des certificats
- La mise à disposition d'un annuaire référençant les certificats

La mise à disposition des LCR n'est jamais facturée.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

Les risques susceptibles d'engager la responsabilité du CSN sont couverts par une assurance appropriée.

9.2.2. Autres ressources

Le CSN reconnaît disposer d'une garantie financière suffisante spécialement affectée à la couverture des risques financiers.

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

Le CSN et l'OSC mettent en place un inventaire de tous les biens informationnels et procéder 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 :

- La DPC ;
- Les clés privées des certificats d'AC Fille et de l'AC NOTAIRES DE FRANCE ;
- Les données d'activation ;
- Les journaux d'événements ;
- Les formulaires d'engagement des partenaires externes ;
- Les causes de révocation des certificats.

9.3.2. Informations hors du périmètre des informations confidentielles

Sans objet

9.3.3. Responsabilités en terme de protection des informations confidentielles

Le CSN s'engage à traiter les informations confidentielles recueillies dans le respect des lois et règlements en vigueur.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

Des mesures techniques, procédurales et organisationnelles sont mises en place pour garantir la protection des données personnelles recueillies lors de l'enregistrement.

9.4.2. Informations à caractère personnel

Sans objet

9.4.3. Informations à caractère non personnel

Pas d'exigence spécifique.

9.4.4. Responsabilité en terme de protection des données personnelles

Sans objet

9.4.5. Notification et consentement d'utilisation des données personnelles

Sans objet

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

Les enregistrements peuvent être mis à disposition en cas de besoin pour servir de preuve à la certification en justice.

9.4.7. Autres circonstances de divulgation d'informations personnelles

Pas d'exigence spécifique.

9.5. Droits sur la propriété intellectuelle et industrielle

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

9.6. Interprétations contractuelles et garanties

9.6.1. Autorités de certification

Le CSN est responsable :

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

Le CSN fait son affaire de toute conséquence dommageable résultant du non-respect du présent document par elle-même ou l'une des entités de l'IGC.

Sauf à démontrer qu'il n'a commis aucune faute intentionnelle ou de négligence, le CSN 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 par le porteur
- L'AC ou l'OSC n'a pas fait procéder à l'enregistrement de la révocation d'un certificat, et publié cette information conformément à ses engagements.

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

Enfin, le CSN 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 par les porteurs.

9.6.2. Service d'enregistrement

Cf. ci-dessus

9.6.3. Porteurs de certificats

Sans objet.

9.6.4. Utilisateurs de certificats

Les utilisateurs de certificats se doivent de vérifier le statut d'un certificat à partir des points de distribution de la LCR définis dans la présente PC.
Pour cela ils peuvent demander au point de contact défini au paragraphe 1.5.2 la fourniture de la LAR et des certificats d'AC applicables au moment de la vérification, si ces derniers ne sont plus accessibles publiquement.
L'opération consiste alors à vérifier :

- Que le numéro de série du certificat concerné n'était pas présent dans la LCR applicable
- Que le certificat utilisé était bien émis par la chaîne de certification applicable.

9.6.5. Autres participants

Pas d'exigence particulière

9.7. Limite de responsabilité

Le CSN ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation du QSCD, des LCR ainsi que de tout autre équipement ou logiciel mis à disposition.
Le CSN décline en particulier sa responsabilité pour tout dommage résultant d'un emploi du QSCD pour un usage autre que ceux prévus.
Le CSN décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans le QSCD, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le porteur.
Le CSN ne pourra pas être tenu 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. Indemnités

Sans objet.

9.9. Durée et fin anticipée de validité de la PC

9.9.1. Durée de validité

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

9.9.2. 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.

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

Sans objet

9.10. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, le CSN fera valider ce changement au travers d'une expertise technique, et analysera l'impact en termes de sécurité et de qualité de service offert.

9.11. Amendements à la PC

9.11.1. Procédures d'amendements

Le CSN s'engage à contrôler que tout changement apporté au présent document reste conforme aux objectifs de conformité aux exigences réglementaires en matière de certification de PSCE.

9.11.2. Mécanisme et période d'information sur les amendements

Pas d'exigence spécifique.

9.11.3. 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.

9.11.4. Informations aux utilisateurs

Toute nouvelle version de la présente Politique de Certification fera l'objet d'une information sur le site https://www.preuve-electronique.org 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.

9.12. Dispositions concernant la résolution de conflits

Conformément aux textes législatifs et à la réglementation en vigueur, les certificats émis sont des certificats dont les conditions d'utilisation sont définies par la présente Politique Certification.

9.13. 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 soumise aux tribunaux compétents de la cour d'appel de Paris.

9.14. Conformité aux législations et réglementations

La présente PC est conforme aux exigences énoncées dans les textes législatifs et réglementaires indiqués au chapitre 10 pour la partie relative à la gestion des certificats de l'AC NOTAIRES DE FRANCE.

9.15. Dispositions diverses

9.15.1. Accord global

Pas d'exigence spécifique

9.15.2. Transfert d'activités

Cf. chapitre 5.8

9.15.3. Conséquences d'une clause non valide

Pas d'exigence spécifique

9.15.4. Application et renonciation

Pas d'exigence spécifique

9.15.5. 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.

9.16. Autres dispositions

Sans objet

9.17. Conditions générales d'utilisation

Sans objet.

10. Documents associés

10.1. Documents applicables

[A1]	RFC 3647. Internet X509 PKI certificate policy and certificate practice statement framework
[A3]	ISO/IEC 9594. Distinguished name
[A4]	Infrastructure de Certification Notariale. Description des certificats et des CRL

10.2. Documents de référence

[R1]	Analyse de risques : eIDAS-AR2016-PSCE
[R2]	Gestion du plan de reprise d'activité
[R4]	Déclaration des pratiques de Certification de l'AC NOTAIRES DE FRANCE
[R5]	Procédure de cessation d'activité

11. Annexe 1 : exigences de sécurité du module cryptographique de l'AC

11.1. Exigences sur les objectifs de sécurité

Le module cryptographique utilisé pour la génération des certificats et des LCR répond aux exigences de sécurité suivantes :

- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et leur destruction sûre en fin de vie
- Etre 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
- Etre 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 des clés privées
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité
- 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
- Détecter les tentatives d'altération physique et entrer dans un état sûr quand une tentative d'altération est détectée

11.2. Exigences sur la certification

Le module est certifié conformément aux exigences ci-dessus, et avoir fait l'objet d'une qualification (EAL4+ avec une résistance élevée des mécanismes).

12. Editions successives

Version / Edition	Date	Emetteur	Valideur	Approbateur
01.0	21/09/2016	A compléter	D. Lefèvre	Membres du bureau CSN
01.1	13/12/2016		D Lefèvre	Membres du bureau CSN
01.2	21/02/2017		D Lefèvre	Membres du bureau CSN
01.3	16/05/2019	M. Porporat	P Pellegrin	Membres du bureau CSN