CONSEIL SUPÉRIEUR DU NOTARIAT

PC Certificats d'Authentification – Format RFC 3647

Politique de Certification pour les Certificats d'authentification

PC REALAUTH

Statut du document : Standard
Version : 00.4
Date : 05/03/2018

PUBLIÉ

Entrée en vigueur le 03/05/2018

Ce document est la propriété du CSN et de REAL.NOT

Historique du document

05/03/2018

Version 0.4
Ajout du service OCSP suite à la levée de la non-conformité eIDAS phase 1

17/08/2017

Version 0.3
Prise en compte des remarques de l'audit eIDAS CSN et ajout OCSP

27/01/2017

Version 0.2
Prise en compte des remarques de l'audit à blanc CSN

08/11/2016

Version : 0.1
Création du document

Nouvelle chaîne d'AC avec mise en œuvre de l'AC REALAUTH en remplacement de l'AC REAL

Table des matières

1. Introduction

1.1. Présentation générale

Le présent document définit l'ensemble des exigences auxquelles le Conseil Supérieur du Notariat se conforme dans la mise en place et la fourniture de ses prestations de service de certification électronique à destination des Notaires de France à des fins d'authentification électronique.

Les exigences définies dans le présent document constituent « un sur » ensemble des spécifications techniques relatives aux prestataires de services de certification en vue de la reconnaissance de leur qualification définie dans le règlement européen [A3], et en particulier des exigences définies dans les documents [A8], [A9], [A10], [A11].

Le Conseil Supérieur du Notariat s'est positionné comme prestataire de service de certification électronique à destination des Notaires de France, en délivrant des certificats d'authentification 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 1.3. La présente politique de certification définit les exigences relatives à l'AC REALAUTH.

Sa structure est conforme au RFC 3647, [A1]. La couverture des exigences prises par l'AC dans le cadre de cette Politique de Certification permet d'être conforme au règlement eIDAS [A3]

1.2. Identification du document

Le numéro d'OID du présent document est 1.2.250.1.78.2.1.3.2.1.1.

Deux profils de certificats sont émis à travers la présente Politique de Certification. Il s'agit du profil pour :

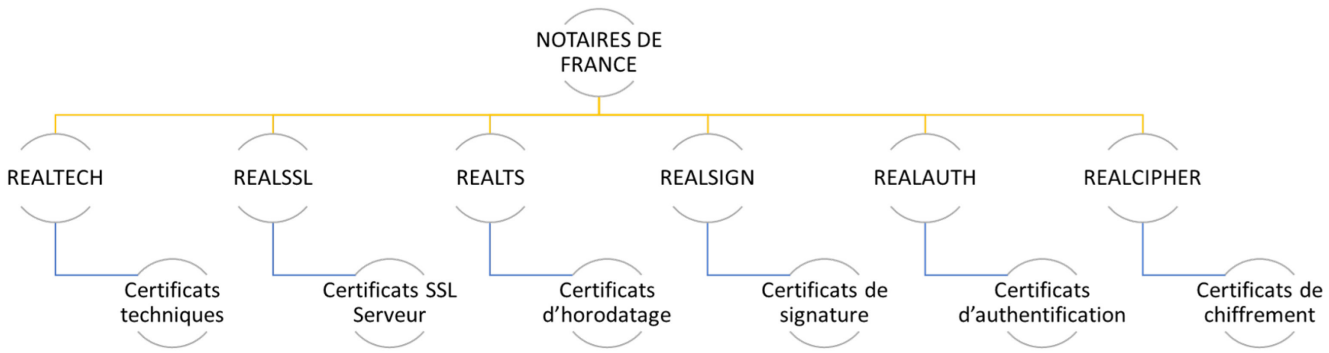
- Certificat d'authentification d'un collaborateur : 1.2.250.1.78.1.1.3.1.3.1.2.1.3.2
- Certificat d'authentification d'un notaire : 1.2.250.1.78.1.1.3.1.3.1.2.2.3.2

1.3. Entités intervenant dans l'IGC

L'AC REALAUTH émet des certificats d'authentification (classe 1 et 2) et son certificat permet de :

- Signer les demandes de certificats d'authentification à destination des Notaires
- Signer les demandes de certificats d'authentification à destination des collaborateurs des Notaires
- Signer les demandes de certificats de signature de réponse OCSP

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. Le CSN est également l'autorité de certification (AC), autorité à laquelle les utilisateurs des services de certification accordent leur confiance pour la création et l'émission des certificats.

Le CSN a recourt à REAL.NOT 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'AC fournit des prestations de gestion des certificats aux Notaires ainsi qu'à leurs collaborateurs, aux notaires des chambres départementales ainsi qu'à leurs collaborateurs, aux notaires et aux collaborateurs du CSN, à la profession notariale.

Les bi clés et certificats considérés dans le présent document sont utilisés en support de la fonction d'authentification. Ce sont :

- d'une part les bi clés et certificats utilisés par les Notaires pour l'authentification dans le cadre des échanges dématérialisés,
- et d'autre part les certificats utilisés par les collaborateurs des Notaires, les organismes rattachés et les organismes de l'écosystème notarial et leurs collaborateurs pour l'authentification dans le cadre des échanges dématérialisés.

Chaque certificat d'authentification 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 (cf. [R5]) et comme cela est décrit dans le paragraphe 1.2.

1.3.2. Opérateur de Service de Certification

L'opérateur de service de certification est REAL.NOT. Il est en charge des :

- Fonctions de génération des certificats
- Fonction de génération des éléments secrets du porteur
- Fonction de remise au porteur
- Fonction de publication
- Fonction de gestion des révocations
- Fonction d'information sur l'état des certificats

1.3.3. Autorité d'enregistrement nationale (AEN)

Le CSN est Autorité d'Enregistrement Nationale ; il vérifie les informations d'identification (rôle de vérificateur) du futur porteur d'un certificat avant de transmettre la demande à l'OSC. Cette vérification est déléguée aux mandataires de certification.

La fonction d'enregistrement est également réalisée par des mandataires de certification, désignés par :

- Un mandataire externe lorsque le rôle est rempli au niveau d'un office
- Un mandataire interne, lorsque le rôle est rattaché à l'AEN, à un organisme rattaché au CSN, à un conseil régional ou à une chambre départementale.

1.3.4. Mandataires de certification

Les mandataires de certification externes sont les Notaires associés ou titulaires des offices ; ils assurent la fonction de validation des informations de leurs collaborateurs au sein de l'étude. Ils peuvent également révoquer les certificats des collaborateurs de l'office.

Les notaires salariés ne peuvent assurer cette fonction de mandataire de certification.

Les mandataires de certification internes sont désignés par le responsable de la chambre ou le CSN, selon leur rattachement ; ils assurent la fonction de validation au sein de leur organisme ainsi qu'auprès des notaires de la compagnie, et peuvent révoquer les certificats des porteurs de l'organisme et des notaires et collaborateurs de la compagnie.

1.3.5. Porteurs de certificats

Un porteur de certificat peut être un collaborateur ou un Notaire d'un office, un collaborateur ou un Notaire d'une chambre départementale, un collaborateur ou un Notaire d'un conseil régional, un collaborateur ou un Notaire du CSN ou d'un organisme rattaché, un collaborateur d'un organisme de l'écosystème notarial. Il s'agit dans tous les cas d'une personne physique, agissant dans le cadre de ses activités professionnelles.

Les collaborateurs sont titulaires de certificats de classe 1 :
Cette classe est applicable aux employés des infrastructures de service du notariat et des offices ou études notariales, elle regroupe l'ensemble des certificats délivrés aux employés du CSN, ADSN, et des chambres, ainsi qu'aux employés des études notariales, des caisses de retraite, des caisses centrales de garantie, des caisses régionales de garantie, et des CRIDON.

Les notaires sont porteurs de certificats de classe 2 :
Cette classe est applicable aux notaires en exercice, elle regroupe l'ensemble des certificats délivrés aux notaires en exercice.

Le détenteur du rôle « Revocation Officer » fait office de porteur des certificats de signatures des réponses OCSP.

1.3.6. Utilisateurs de certificats

La présente politique recouvre la gestion des certificats d'authentification, destinés exclusivement à un usage interne au Notariat.

1.4. Usage des certificats

1.4.1. Domaines d'utilisation applicables

La présente politique de certification traite des bi-clés et des certificats des porteurs identifiés en 1.3.5, afin que ces porteurs puissent s'authentifier.

Les exigences relatives aux bi-clés et certificats d'AC et des composantes sont définies dans la PC relative à l'AC NOTAIRES DE FRANCE [R6].

L'AC émet également des certificats de signature de réponse OCSP.

1.4.2. Domaines d'utilisation interdits

L'utilisation des bi-clés et certificats est strictement limitée à la seule fonction d'authentification au sein de la communauté notariale.

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
Tél : 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
AEN	**A**utorité d'**E**nregistrement **N**ationale
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
OCSP	Protocole de vérification de certificat en ligne (**O**nline **C**ertificate **S**tatus **P**rotocol)
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
QSCD	Dispositif de Création de Signature Qualifié (**Q**ualified **S**ignature **C**reation **D**evice)

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, de la déclaration des pratiques de certification et des conditions générales d'utilisation.

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.

Ces informations sont également disponibles à travers le service OCSP mis en œuvre, accessible à l'adresse suivante : ocsp.preuve-electronique.org.

2.2. Informations devant être publiées

Les informations publiées sont les suivantes :

- La présente politique de certification ainsi que la Politique de Certification de l'AC NOTAIRES DE FRANCE [R6]
- Les formulaires nécessaires aux porteurs : enregistrement, renouvellement et révocation
- Le document présentant les profils des certificats et CRL [R5]
- La liste des certificats révoqués (CRL) pour les pour les porteurs et l'AC
- Les certificats de l'AC REALAUTH en cours de validité, ainsi que les certificats en cours de validité de l'AC NOTAIRES DE FRANCE (hiérarchie à laquelle est rattachée l'AC REALAUTH)
- 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)

Les formulaires d'enregistrement, de renouvellement et de révocation sont directement téléchargeables sur le site http://sacre.real.notaires.fr par les porteurs.

Les documents PC et CGU sont publiés :

- au format PDF/A
- en français.

2.3. Délais et fréquences de publication

Les politiques de certification doivent être 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 LCR, dans un délai de 24 heures.

La fréquence de publication des LCR doit être compatible avec un délai maximal de 24 heures entre la prise en compte d'une demande de révocation et sa publication. Les LCR sont publiées toutes les 24h au moins.

2.4. Contrôle d'accès aux informations publiées

Les informations publiées sont mises en ligne sur l'Intranet Notarial et accessibles en lecture à l'ensemble de la communauté. Les PC, LCR et ARL sont accessibles en lecture de manière internationale à toute personne souhaitant en prendre connaissance sur le site www.preuve-electronique.org.

Les ajouts, suppressions et modifications se font au travers d'un process automatique 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), [A5], 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.

Les informations portées dans le champ « Subject DN » du certificat sont décrites ci-dessous de manière explicite :

- Le Pays est positionné dans le champ « Country »
- La valeur « Professions Réglementées » dans un champ « Organization »
- La valeur « Notaires » dans un champ « Organization Unit »
- La valeur « AC Déléguée » dans un champ « Organization Unit »
- La valeur « REAL » dans un champ « Organization Unit »
- Le nom de famille est positionné dans le champ « SurName »
- Le prénom est positionné dans le champ « GivenName »
- L'unicité du certificat est portée dans le champ « CommonName » qui contient les informations : NOM Prénom (<Numéro de titulaire>)

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 [R6].

3.1.5. Unicité des noms

Un code distinctif ajouté dans le champ « CommoName » assure le caractère unique du DN en cas d'homonymie.
Le code d'unicité est le numéro de titulaire unique généré par le système.

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

Le demandeur saisit une demande électronique de création de certificat / QSCD en s'adressant à l'OSC par l'intermédiaire de l'application SACRE. Pour cela il se connecte via son navigateur à l'adresse : http://sacre.real.notaires.fr.

Le demandeur prépare les documents annexes à sa demande au format papier et contenant les CGU associées.

Les documents annexes sont :

- une photocopie d'un justificatif d'identité en cours de validité (Carte nationale d'identité, passeport ou titre de séjour)
- une attestation de l'employeur (si le demandeur est un collaborateur ne travaillant pas dans un office notarial)
- la copie de l'arrêté de nomination ou de la prestation de serment (si le demandeur est un notaire)

D'autres documents peuvent éventuellement être fournis :

- la signature manuscrite effectuée dans un cartouche (obligatoire si le demandeur est un notaire, et facultatif si le demandeur est un clerc)
- Le sceau du notaire imprimé dans un cartouche (obligatoire si le demandeur est un notaire)
- Le cas échéant, le cachet du collaborateur imprimé dans un cartouche, si le demandeur est un clerc habilité.

Le demandeur télécharge, complète et signe un formulaire papier contenant les CGU associées, auquel il annexe les documents annexes préparés. Il numérise l'ensemble de ces documents en un seul fichier PDF qu'il devra uploader dans SACRE.

Il renseigne les informations professionnelles suivantes dans le formulaire électronique de l'application SACRE :

- nom,
- prénom(s),
- rôle (notaire ou collaborateur)
- rôle spécifique : Notaire salarié d'un office / Mandataire interne délégué de chambre / Clerc habilité d'un office
- n° CRPCEN,
- téléphone(s) (facultatif)
- fax (facultatif)
- adresse de messagerie électronique
- Numéro de pièce d'identité (CNI, passeport ou carte de séjour)
- Date de fin de validité de la pièce d'identité

Il uploade le formulaire papier complété et signé avec toutes ses annexes.

L'application lui retourne un identifiant de demande. Il saisit un mot de passe qui lui permettra par la suite d'initialiser le QSCD à distance.

Le demandeur s'adresse ensuite au valideur (mandataire externe, mandataire interne) pour que ce dernier lui remette le code d'activation de sa demande en face à face. Il fournit pour cela le formulaire de demande papier complété et signé, une copie d'une pièce d'identité, les documents annexes au format papier, ainsi que son identifiant de demande.

Le valideur vérifie l'identité du demandeur et la conformité des documents. Il valide ensuite la demande de création de carte du demandeur auprès de l'OSC qui lui retourne le code d'activation de son futur QSCD ainsi que son numéro de titulaire. Le valideur imprime ces éléments à l'attention du demandeur. Le positionnement d'une demande d'initialisation dans le workflow déclenche l'impression graphique et l'envoi par courrier d'un QSCD vierge et non initialisé au demandeur.

Le formulaire papier de demande de clé REAL complété et signé par le demandeur, ainsi que les pièces justificatives, sont numérisées et versées par le demandeur dans SACRE au cours de la saisie de la demande de clé REAL. Le formulaire papier de demande de clé REAL complété et signé, avec toutes ses annexes, est conservé par le

mandataire de certification. Ce document est versé dans un acte de dépôt de pièces récapitulatif global au moins une fois par an par le mandataire. Cet acte est conservé par ce dernier au rang des minutes de son office.

Le CSN, dans son rôle d'Autorité d'Enregistrement Nationale procède régulièrement à des vérifications des formulaires de demande de clé REAL et des annexes correspondantes au travers une interface spécialisée dans SACRE.

La validation par le mandataire de certification lors du face à face autorise le futur titulaire à initialiser sa clé REAL.
Si le valideur juge, sur la base des éléments fournis par le demandeur, qu'il ne peut pas valider électroniquement la demande, il procèdera au refus électronique de cette demande. Le face à face n'aura pas lieu. Si le face à face de remise du code d'activation ne se déroule pas comme prévu, le mandataire procède à l'annulation de la demande qu'il a validée.

En cas de signature manuscrite, de sceau ou de cachet associés à la demande, le mandataire fait parvenir ces recueils à l'AEN. L'opérateur AEN s'adresse à l'OSC par l'intermédiaire de l'application SACRE après avoir scanner la signature, le sceau et le cachet du demandeur pour associer les images scannées au profil du demandeur dans SACRE.

Le demandeur reçoit son QSCD par courrier. A réception de celui-ci, il initialise son QSCD par l'intermédiaire de l'application SACRE, en s'identifiant avec le mot de passe (qu'il a saisi lors de sa demande), le code d'activation qui a été généré lors de la validation et son numéro de titulaire.

Le demandeur dispose d'une durée limitée (12 semaines) pour initialiser le QSCD avant que le code d'activation n'expire (Le délai d'activation du QSCD débute à l'instant de la validation de la demande par le mandataire). Passé ce délai, le demandeur doit ressaisir une demande.

Lors de cette initialisation, le demandeur choisit lui-même son code PIN et sa question de confiance qui sera utilisée pour l'identifier en cas de révocation d'urgence. Il accepte ensuite chacun des certificats avant que ceux-ci soient installés sur le QSCD.

3.2.1. Méthode pour prouver la possession de la clé privée

La clé privée est générée par le QSCD à l'initialisation du support ; la procédure de délivrance du certificat par l'OSC, effectuée lors de l'initialisation du QSCD, ne nécessite donc pas de preuve de possession de la clé privée :

Le niveau de qualification de la technologie utilisée permet de s'assurer de la possession de la clé privée par le QSCD du porteur, qui est protégée dès sa génération.

3.2.2. Validation de l'identité d'un organisme

Les certificats ne concernent que les porteurs notaires ou leurs collaborateurs (d'un office, d'une chambre, d'un conseil régional, du CSN, des organismes rattachés ou des organismes de l'écosystème notarial) ; la validation de l'identité de l'organisme de rattachement est présentée au chapitre suivant.

3.2.3. Validation de l'identité d'un porteur

La validation de l'identité d'un demandeur est effectuée lors du face à face entre le demandeur et le mandataire interne ou externe. Elle est basée sur :

- Le dossier électronique (nom prénom, n° CRPCEN de l'instance ou de l'office, adresse mail) validé par le mandataire
- Un justificatif d'identité (carte d'identité, titre de séjour ou passeport)

- La copie de l'arrêté de nomination ou prestation de serment ou tout autre justificatif de sa qualité de notaire en exercice pour un notaire, ou attestation d'emploi pour un collaborateur.

Le dossier d'enregistrement est déposé auprès du mandataire de certification.

3.2.3.1. Enregistrement d'un MC externe

L'enregistrement d'un mandataire externe est effectué lors d'un face à face avec un mandataire de la chambre dont dépend l'office employant le mandataire externe. La validation est effectuée sur la base des éléments recensés dans le paragraphe ci-dessus. La validation par le mandataire interne d'une demande de clé REAL d'un Notaire titulaire de charge ou associé engage de facto ce dernier à effectuer correctement les fonctions qui lui sont confiées (contrôle des dossiers des demandeurs de l'office, révocation des certificats) en tant que mandataire externe de ses collaborateurs.

3.2.3.2. Enregistrement d'un MC interne / chambre départementale, conseil régional CSN et organisme rattaché au CSN

L'enregistrement d'un mandataire interne est effectué lors d'un face à face avec le mandataire du CSN. La validation est effectuée sur la base des éléments recensés dans le paragraphe ci-dessus, complétée d'un mandat validé par le Notaire responsable de l'organisme confirmant le demandeur dans sa fonction de mandataire interne. La validation par le mandataire du CSN d'une demande de clé REAL d'un mandataire interne engage de facto ce dernier à effectuer correctement les fonctions qui lui sont confiées (contrôle des dossiers des demandeurs, révocation des certificats).

3.2.3.3. Enregistrement d'un porteur avec MC

L'enregistrement d'un porteur avec mandataire est effectué lors d'un face à face avec le mandataire de l'organisme auquel le porteur est rattaché : mandataire externe pour un office, mandataire interne rattaché à la chambre ou au conseil régional, mandataire interne du CSN, mandataire interne d'un organisme rattaché au CSN. La validation est effectuée sur la base des éléments recensés en introduction du paragraphe. Si le porteur est un Notaire ou un clerc habilité, l'enregistrement peut comporter également un formulaire de recueil de signature manuscrite, sceau ou cachet, pour des besoins purement fonctionnel métier, si le porteur le souhaite.

3.2.3.4. Enregistrement d'un porteur sans mandataire

L'enregistrement d'un porteur sans mandataire est effectué uniquement pour l'enregistrement du responsable de l'AEN (président). L'enregistrement est effectué lors de la sa prise de fonction.

3.2.3.5. Enregistrement d'un porteur de clé Notaire de test

Le porteur d'une clé notaire de test est :

- Soit un collaborateur (non notaire) de l'ADSN ou de l'une de ses filiales. L'usage de cette clé de test est strictement restreint aux cas de tests fonctionnels des plateformes de production.
- Soit un représentant d'une entité tierce souhaitant réaliser des tests d'intégrations des clés REAL et de ses certificats.
- Soit un représentant d'une entité tierce liée contractuellement à l'ADSN ou à l'une de ses filiales. L'usage de cette clé de test est strictement restreint aux cas de tests fonctionnels des plateformes de production.

L'enregistrement du porteur est effectué par un opérateur de l'OSC habilité à créer des certificats de tests. Les informations suivantes du titulaire de la clé REAL de tests sont renseignées :

- Nom
- Prénom
- Profil (Notaire, Collaborateur)
- Email

- Mot de passe de la demande

Le certificat généré contient alors les informations suivantes :
- Le Pays est positionné dans le champ « Country »
- La valeur « Professions Réglementées » dans un champ « Organization »
- La valeur « Notaires » dans un champ « Organization Unit »
- La valeur « AC Déléguée » dans un champ « Organization Unit »
- La valeur « REAL » dans un champ « Organization Unit »
- Le nom de famille est positionné dans le champ « SurName » et construit de la manière suivante « NOM [FOR TEST ONLY]
- Le prénom est positionné dans le champ « GivenName »
- L'unicité du certificat est portée dans le champ « CommonName » qui contient les informations : NOM Prénom (<Numéro de titulaire>)

3.2.3.6. Enregistrement d'un porteur de clé Collaborateur de test

Le porteur d'une clé collaborateur de test est :
- soit un collaborateur de l'ADSN ou de l'une de ses filiales. L'usage de cette clé de test est strictement restreint aux cas de tests fonctionnels des plateformes de production.
- Soit un représentant d'une entité tierce souhaitant réaliser des tests d'intégrations des clés REAL et de ses certificats.
- Soit un représentant d'une entité tierce liée contractuellement à l'ADSN ou à l'une de ses filiales. L'usage de cette clé de test est strictement restreint aux cas de tests fonctionnels des plateformes de production.

L'enregistrement du porteur est effectué par un opérateur de l'OSC habilité à créer des certificats de tests. Les informations suivantes du titulaire de la clé REAL de tests sont renseignées :
- Nom
- Prénom
- Profil (Notaire, Collaborateur)
- Email
- Mot de passe de la demande

Le certificat généré contient alors les informations suivantes :
- Le Pays est positionné dans le champ « Country »
- La valeur « Professions Réglementées » dans un champ « Organization »
- La valeur « Notaires » dans un champ « Organization Unit »
- La valeur « AC Déléguée » dans un champ « Organization Unit »
- La valeur « REAL » dans un champ « Organization Unit »
- Le nom de famille est positionné dans le champ « SurName » et construit de la manière suivante « NOM [FOR TEST ONLY]
- Le prénom est positionné dans le champ « GivenName »
- L'unicité du certificat est portée dans le champ « CommonName » qui contient les informations : NOM Prénom (<Numéro de titulaire>)

3.2.4. Informations non vérifiées du porteur

Sans objet

3.2.5. Validation de l'autorité du demandeur

Le dossier d'enregistrement est déposé par le mandataire de certification dans un acte de dépôt de pièces récapitulatif au moins une fois par an. L'AEN procède à des vérifications régulières des formulaires de demandes de clé REAL indexés dans SACRE en regard des demandes de clés REAL correspondantes.

La validation par le mandataire de certification lors du face à face autorise le futur titulaire à initialiser sa clé REAL.

3.2.6. Certification croisée d'AC

L'AC n'a aucun accord de reconnaissance avec une AC extérieure au domaine de sécurité auquel elle appartient. Les certificats qu'elle émet à travers la présente PC sont à des fins d'utilisation interne du notariat.

Si une autre AC formule une demande d'accord, ou si les responsables de l'AC REALAUTH émettent le besoin de mettre en place un accord de reconnaissance avec une autre AC, le comité de pilotage de l'AC diligentera une série d'investigations (audits / analyse de risques) pour déterminer si l'AC à reconnaître émet bien des certificats de même qualité, avec le même niveau de sécurité, que ceux de la présente AC.

Notamment, l'AC REALAUTH pourra attendre des AC demandant un accord de certification de respecter les formats des certificats suivant la norme [A9], [A10], [A11].

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

Un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la clé REAL.

Le Porteur devra procéder comme pour une demande initiale (cf. paragraphe 3.2).

3.3.1. Identification et validation pour un renouvellement courant

Le porteur est averti de l'arrivée à expiration de son certificat par courriel ; Il renseigne et signe avec son certificat actif, le formulaire électronique de demande de renouvellement pour que la demande soit prise en compte.

Le demandeur s'adresse ensuite au valideur (mandataire externe, mandataire interne) pour que ce dernier lui remette le code d'activation de sa demande de renouvellement en face à face. Il fournit pour cela un formulaire de demande papier, contenant les CGU associées, complété et signé, une copie d'une pièce d'identité, les documents annexes au format papier remplis et signés, ainsi que son identifiant de demande.

Le valideur vérifie l'identité du demandeur et la conformité des documents. Il valide ensuite la demande de renouvellement de carte du demandeur auprès de l'OSC qui lui retourne le code d'activation de son futur QSCD ainsi que son numéro de titulaire. Le valideur imprime ces éléments à l'attention du demandeur.
Ce renouvellement donne systématiquement lieu à la fourniture d'un nouveau QSCD.
Le positionnement d'une demande d'initialisation dans le workflow déclenche l'impression graphique et l'envoi par courrier d'un QSCD vierge et non initialisé au demandeur.

Le formulaire papier de demande de clé REAL contenant les CGU associées, complété et signé par le demandeur, ainsi que les pièces justificatives, sont numérisés et versés par le demandeur dans SACRE au cours de la saisie de la demande de renouvellement de clé REAL. Le formulaire papier de demande de renouvellement de clé REAL complété et signé est conservé par le mandataire de certification. Ce document est versé dans un acte de dépôt de pièces récapitulatif global au moins une fois par an par le mandataire. Cet acte est conservé par ce dernier au rang des minutes de son office.

Le CSN, dans son rôle d'Autorité d'Enregistrement Nationale procède régulièrement à des vérifications des formulaires de demande de clé REAL et des annexes correspondantes au travers une interface spécialisée dans SACRE.

La validation par le mandataire de certification lors du face à face autorise le titulaire à initialiser sa clé REAL. Si le valideur juge, sur la base des éléments fournis par le demandeur, qu'il ne peut pas valider électroniquement la demande, il procèdera au refus électronique de cette demande. Le face à face n'aura pas lieu. Si le face à face de remise du code d'activation ne se déroule pas comme prévu, le mandataire procède à l'annulation de la demande qu'il a validée.

La demande électronique de clé REAL peut être complétée par la suite par l'AEN, avec la numérisation des recueils de signature manuscrite, sceau et cachet fournis par le demandeur.

A réception de son QSCD, le demandeur s'adresse à l'OSC pour l'initialiser. Le demandeur dispose d'une durée limitée pour initialiser le QSCD avant que le code d'activation n'expire. Le délai d'activation du QSCD débute à l'instant de la validation de la demande de renouvellement par le mandataire.

Si la demande n'a pas été formulée avant la date d'expiration du certificat courant, le titulaire procéde comme pour une première demande.

3.3.2. Identification et validation pour un renouvellement après révocation

En cas de renouvellement après révocation, le titulaire procéde comme pour une première demande.

En cas de renouvellement pour un motif technique et à l'initiative de l'AC, le titulaire est averti par alerte logiciel qu'il doit procéder rapidement au renouvellement de son certificat et ce avant son expiration. La demande est assistée au travers d'un logiciel dédiée et sécurisé à l'aide des certificats de chiffrement et d'authentification présents sur le QSCD.

3.4. Identification et validation d'une demande de révocation

Il existe trois modes au travers desquels peut être effectuée une demande de révocation : révocation standard, révocation d'urgence ou révocation suite à un renouvellement technique.

La révocation standard est effectuée par le Notaire titulaire ou associé, en charge de l'office ou de l'organisme, ou par le mandataire selon les cas. La demande de révocation est effectuée en ligne ; L'identité du demandeur et l'intégrité de la demande sont contrôlées sur la base du certificat d'authentification utilisé pour authentifier la demande.

La révocation d'urgence est à l'initiative du titulaire. Elle peut être effectuée par Internet, ou par téléphone. L'identification du titulaire et la validation de la demande sont contrôlées par la réponse à une question de confiance connue du seul titulaire, déposée lors de la phase d'initialisation du QSCD.

La révocation technique à l'initiative de l'AC suite au renouvellement technique du certificat est effectuée en automatique lors du processus de renouvellement assisté.

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 toujours du futur porteur, qui renseigne le formulaire correspondant. La signature du formulaire papier de demande de clé REAL par le futur porteur signifie l'accord du porteur.

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

La demande de certificat comporte dans tous les cas :

- Les informations professionnelles : nom, prénom, numéro CRPCEN de l'office ou de l'instance, adresse postale, téléphone, fax, et adresse de messagerie électronique, les fax et adresse postale n'étant pas systématiques.
- Un mot de passe
- Un document établissant le rattachement du futur porteur à l'organisme, validé par le responsable (attestation de l'employeur)
- La copie de l'arrêté de nomination ou de la prestation de serment dans le cas d'un notaire
- Les CGU de la clé REAL signées

La demande peut être accompagnée de :

- Un exemplaire de signature manuscrite et de sceau pour les Notaires
- Un exemplaire de signature manuscrite et de cachet pour les clercs habilités.

Le dossier comporte également un formulaire papier de demande signé par le porteur et numérisé, avec ses annexes.

Les éléments papiers du dossier sont conservés par le mandataire de certification et versés au moins une fois par an dans un acte de dépôt de pièces récapitulatif.

4.2. Traitement d'une demande de certificat

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

L'identité du porteur, les justificatifs présentés et la connaissance des modalités applicables par le futur porteur sont validés lors du face à face.

Le dossier papier est conservé par le mandataire de certification et versé au moins une fois par an dans un acte de dépôt de pièces récapitulatif.

4.2.2. Acceptation ou rejet de la demande

Le mandataire informe le porteur en cas de rejet de la demande, en justifiant le rejet. Cette notification de refus est transmise au porteur par courriel ; elle peut être également formulée par le mandataire lors du face à face.

4.2.3. Durée d'établissement du certificat

La durée d'établissement du certificat dépend essentiellement du porteur qui est à l'origine de l'initialisation du QSCD. Une durée limitée, paramétrée par défaut à 12 semaines par l'OSC, permet de contrôler le temps octroyé au porteur pour l'initialisation.
Ce délai court à compter de la date de validation par le mandataire de certification.

4.3. Délivrance du certificat

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

Le passage de la demande à l'état validé (par le mandataire) dans le workflow applicatif déclenche les processus de génération et de préparation des éléments destinés au porteur : élaboration et émission du code d'activation et du numéro de titulaire.

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

Le QSCD est transmis par voie postale, le code d'activation est remis au demandeur lors de la validation de la demande en face à face. Un courriel est envoyé au porteur pour lui indiquer la validation de sa demande, qui autorise l'initialisation du QSCD reçu.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

Le certificat d'authentification est élaboré en ligne, et transmis lors de la phase d'initialisation du QSCD. Le titulaire peut accepter ou refuser le certificat lors de cette phase d'initialisation. Le certificat est présenté à l'utilisateur qui doit l'accepter formellement.

En cas d'erreur technique lors de la phase d'initialisation du QSCD, suivant le type d'erreur, le titulaire pourra recommencer cette phase sans émettre de nouvelle demande de certificat, en utilisant les informations de sa demande initiale. Dans les autres cas, le QSCD est rendu inutilisable et le titulaire doit faire une nouvelle demande. Les cas pour lesquels le QSCD est rendu inutilisable sont décrits dans la DPC [R3].

4.4.2. Publication du certificat

Les certificats des porteurs ne sont pas publiés.

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

Un service d'état des demandes en ligne accessible aux personnes autorisées est fourni par l'OSC.

4.5. Usage de la bi-clé et du certificat

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

L'utilisation de la clé privée par le porteur est limitée à l'authentification de données ou de transactions. Cet usage est indiqué explicitement dans les extensions du certificat [R5].

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

L'utilisation du certificat est limitée à la vérification de l'authentification du porteur.

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

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

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

4.9.1.1. Certificats de porteur

Les causes de révocation sont les suivantes :

- Obsolescence des informations relatives au porteur figurant dans le certificat
- Décision du titulaire ou d'un notaire titulaire ou associé de l'office, ou du responsable de la chambre ou du CSN à l'encontre d'un de leur collaborateur ou d'un notaire.
- Erreur dans le dossier d'enregistrement
- Erreur technique irrécupérable durant la phase d'initialisation du QSCD
- Destruction, altération du QSCD ou de ses fonctions
- Décision suite à un échec de contrôle de conformité remonté par l'audit interne
- Compromission, suspicion de compromission, perte ou vol de clé privée
- Fin programmée d'utilisation de l'algorithme de condensation mis en œuvre
- Révocation de l'AC REALAUTH
- Cessation d'activité de l'AC NOTAIRES DE FRANCE

4.9.1.2. Certificats d'AC

Voir PC de l'AC NOTAIRES DE FRANCE [R6]

4.9.2. Origine d'une demande de révocation

Les personnes pouvant demander une révocation sont les suivantes :

- le porteur au nom duquel le certificat a été émis
- un mandataire interne ou externe pour l'ensemble des porteurs qui lui sont rattachés
- le Président du CSN pour les porteurs qui lui sont rattachés
- la personne intervenant dans la procédure de révocation d'urgence, sur sollicitation du porteur du certificat

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Certificats de porteur

La fonction de gestion des révocations est accessible par l'Intranet pour le mode nominal, au travers d'Internet via l'URL http://revocation-carte-real.notaires.fr ou par téléphone N° indigo 08 20 88 77 63 pour la révocation d'urgence.

Les informations demandées lors de la révocation standard sont les nom et prénom, ainsi que le numéro de titulaire du porteur ; la connaissance d'un secret (réponse à une question déposée) est demandée en plus lors de la révocation d'urgence.

4.9.3.2. Certificats d'AC

Voir PC de l'AC NOTAIRES DE FRANCE [R6]

4.9.4. Délai accordé au porteur pour formuler la demande de révocation

La demande de révocation est formulée au plus tôt dès lors que le porteur ou son responsable a connaissance d'une cause effective de révocation.

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

4.9.5.1. Certificats de porteur

Le délai maximum de traitement est de 24 heures.

4.9.5.2. Certificats d'AC

Voir PC de l'AC NOTAIRES DE FRANCE [R6]

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

Les certificats sont utilisés pour vérifier l'authentification d'un porteur.

L'utilisateur d'un certificat est tenu de vérifier l'état du certificat et des certificats constituant la chaîne de confiance (AC REALAUTH // AC NOTAIRES DE FRANCE). Il s'appuie pour cela sur les LCR publiées régulièrement pour les différentes AC, ou le service OCSP mis à disposition à l'adresse ocsp.preuve-electronique.org..

4.9.7. Fréquence d'établissement des LCR

Les LCR sont émises à minima toutes les 12h, ou dès révocation d'un certificat.

4.9.8. Délai maximum de publication d'une LCR

La publication d'une LCR se fait dans un délai maximum de 60 minutes après sa génération.

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 d'au moins 99,5 pour cent, et sont disponibles sous 24 heures. 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 48h.

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

Dans le cadre de la révocation d'un certificat d'AC, 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 LCR 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 www.preuve-electronique.org

Un service OCSP conforme à la RFC 6277 est aussi disponible à l'adresse : ocsp.preuve-electronique.org (cf 7).
Le service OCSP met en oeuvre l'extension « archive cutoff », comme prévu par la RFC 6960, avec une date identique à la date de début de validité du certificat de l'AC et maintient disponible le statut de révocation du certificat après son expiration.
Si la requête OCSP contient une demande pour un numéro de série non émis par l'AC REALAUTH, alors le serveur OCSP indiquera dans la réponse correspondante le statut « unknow » si l'AC REALAUTH est toujours valide, et « unauthorized » si cette dernière est expirée.

4.10.2. Disponibilité de la fonction

Les fonctions d'information sur l'état des certificats sont disponibles 24 heures sur 24, 7 jours sur 7.

4.10.3. Dispositifs optionnels

Le statut d'expiration d'un certificat sera fourni de manière automatisée au porteur de certificat via une information portée par la LCR lors de l'expiration du premier certificat émis.
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 Titulaires, envoyée par mail à l'adresse exploitation.carte.real@notaires.fr.
Les modalités de demandes sont décrites sur le site www.preuve-electronique.org (cf [R7]).

4.11. Fin d'abonnement

En cas de fin d'abonnement au service REAL, la clé REAL du porteur est désactivée et les certificats associés sont révoqués.

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

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 de la stratégie de gestion de risques définie par le 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, documents d'applications).

Les responsables des organismes (chambres, conseil régionaux, CSN et organismes rattachés) et les titulaires d'offices mettent également en place des mesures physiques ou logiques de contrôle d'accès afin de limiter l'accès aux moyens de validation et aux dossiers d'enregistrement aux seuls mandataires.

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 DNSI ou son représentant désigné, sous le contrôle direct du président du CSN.

5.2.1.2. AEN

L'Opérateur est chargé de la numérisation des recueils de signatures manuscrites, de sceaux et de cachets. Il est aussi en charge du contrôle régulier des formulaires de demandes de clé REAL numérisés dans SACRE, accompagnés de leurs annexes justifiant du face à face entre le mandataire et le porteur.

Il intervient depuis le site du CSN.

L'Autorité d'Enregistrement s'appuie sur des mandataires internes, rattachés aux chambres départementales, aux conseils régionaux ou directement au CSN. Les mandataires internes des chambres valident les demandes des Notaires du département, et des employés des chambres. Les mandataires internes des conseils régionaux valident les demandes des employés des conseils régionaux. La validation est réalisée lors d'un face à face à la chambre, au conseil régional ou à l'office du mandataire pour les demandes initiales. Les mandataires internes rattachés au CSN valident les demandes des employés du CSN.

Les mandataires internes ou externes peuvent également intervenir dans la fonction de révocation des certificats pour les porteurs qui leurs sont rattachés.

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 [R3] 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.

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 REAL.NOT.

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.

L'officier d'enregistrement est en charge de vérifier les informations contenues dans la demande de certificat et de procéder à son approbation. Ce rôle est tenu par le responsable de l'AEN.

L'officier de révocation est en charge de traiter les demandes de révocation. Ce rôle est tenu par le responsable de l'OSC.

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 REAL.NOT disposant du rôle de confiance Administrateur Système.

Des porteurs de secrets sont également définis pour l'AC REALAUTH. 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. Une liste d'exclusion est maintenue dans [R3]. Une même personne ne peut disposer que d'un seul rôle de confiance.
Un rôle de confiance peut également être porteur d'une part de secret. Un porteur de secrets ne peut détenir qu'une seule part.

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 REAL.NOT. 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 sensible.

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. Cela concerne essentiellement le personnel de l'OSC opérant sur les composantes de l'IGC, mais également les opérateurs et mandataires pour l'utilisation 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 les conditions d'agrément (contractualisation) des mandataires
- Dans la définition de poste ou la charte de sécurité du personnel pour les rôles sensibles tenus par le personnel de l'OSC et de l'AC.

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

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

Il est nécessaire d'enregistrer les événements suivants :

- événements systèmes des différentes composantes de l'IGC (démarrage des serveurs, accès réseau, …) que ce soit sur le site actif ou le site de sauvegarde
- événements techniques des applications composant l'IGC, sur le site actif ou le site de sauvegarde
- événements fonctionnels des applications composant l'IGC (demande de certificats, validation, révocation, …) sur le site actif ou le site de sauvegarde
- évènements liés aux clés de signature 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, etc.)
- opérations effectuées

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

Les journaux d'événements sont exploités :

- De manière quotidienne dans le cadre de processus automatisé de contrôle
- Systématiquement en cas de remontée d'événement anormal

5.4.3. Période de conservation des journaux d'événements

La période de conservation des journaux d'événement est :

- de un mois pour les événements systèmes
- de un an pour les événements techniques
- conforme aux obligations légales pour les événements fonctionnels

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 procédures de sauvegarde des journaux sont quotidiennes par delta avec les sauvegardes précédentes, et globales de manière hebdomadaire.

5.4.6. Système de collecte des journaux d'événements

Les événements enregistrés au sein de l'IGC sont centralisés au sein d'un SIEM.

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 d'événement système et technique est continu et quotidien afin de permettre une anticipation des vulnérabilités, et des remontées d'alerte en cas de vulnérabilités. Ces contrôles sont réalisés via des processus automatiques qui permettent de détecter des anomalies.

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

Une revue mensuelle des événements anormaux est réalisée par le comité de pilotage de l'AC à travers une séance de revue de processus.

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 et CGU
- Certificats et LCR publiés
- Engagements signés des mandataires internes et externes
- Dossiers d'enregistrement des porteurs
- 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 REALAUTH	23 ans
LCR & Certificats clients	23 ans
Evènements système	1 mois
Evènements techniques	1 an
Evènements fonctionnels	23 ans
Documentation	10 ans
Dossier d'enregistrement (demandes de certificats)	75 ans
Requêtes et réponses OCSP	10 ans

Les dossiers d'enregistrement (demandes de certificats) sont archivés pendant 75 ans, localement, par le mandataire ou le notaire tiers sous la forme d'un acte authentique de dépôt. Passé ce délai, ils seront versés aux archives départementales sans limitation de durée.

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 [R3].

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 sont synchronisés sur un même serveur synchronisé avec l'heure universelle.

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 peuvent être effectuées dans un délai conforme à l'utilisation des certificats délivrés. Un délai de 2 jours ouvrés est nécessaire pour récupérer les archives.

5.5.8. Accès aux archives des dossiers d'enregistrement

Afin d'avoir accès aux données des dossiers d'enregistrement le concernant, le porteur doit s'adresser au responsable du traitement :

- le Conseil Supérieur du Notariat, Autorité de certification, 60 boulevard de La Tour-Maubourg, 75007 PARIS
- Tel : +33 1 44 90 30 00, Fax : +33 1 44 90 31 42
- mail : autorite-certification@notaires.fr

5.6. Changement de clés d'AC

La durée de vie des clés d'AC REALAUTH est de 8 ans. La durée de vie des certificats est de 3 ans pour les certificats émis par l'AC REALAUTH.

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'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 du certificat correspondant. 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 ou les certificats d'horodatage, 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 mandataires et 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 d'indentification 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 Real.not cesserait son activité d'OSC à la demande du CSN, Real.not déroulera la procédure [R8] et maintiendra la disponibilité de la fonction de vérification de l'état des certificats portés par la Clé Real.

Dans le cas où Real.not 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. L'AC organisera alors la reprise des activités d'OSC par un nouvel opérateur [R9].

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 mesures nécessaires seront prises pour la détruire ou la rendre inopérante ;
3. Le certificat d'AC sera révoqué ;
4. Tous les certificats émis encore en cours de validité seront révoqués et les mandataires et les porteurs correspondants seront prévenus ;
5. 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 pour les RC et les utilisateurs de certificats ;
6. L'AC tiendra informée l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus

En cas de cessation d'activité de l'AC dans le cas d'un renouvellement de la chaîne d'AC ou dans une cessation totale, le CSN s'engage à fournir les statuts des certificats de la manière suivante :
- Pour chaque AC, une dernière LCR sera publiée avec une date d'expiration positionnée à la valeur 99991231235959Z
- Pour chaque certificat, une dernière réponse OCSP sera pré-générée avec une date de fin de validité positionnée à la valeur 99991231235959Z

5.8.3. Cessation d'activité affectant l'activité AEN 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 REALAUTH

Voir PC AC NOTAIRES DE FRANCE [R6]

6.1.1.2. Clés porteurs générées par l'AC

Sans objet

6.1.1.3. Clés porteurs générées par le porteur

La génération des bi clés du porteur est effectuée directement dans le QSCD, qui répond aux exigences formulées par la réglementation européenne [A3].
Le processus d'initialisation de la clé REAL, déclenché à distance par le porteur, s'assure que le dispositif à initialiser est un QSCD reconnu par l'AC, en effectuant la mise en place d'un canal sécurisé basé sur des clés sécrètes échangées entre l'OSC et le fournisseur des QSCD.

6.1.2. Transmission de la clé privée à son propriétaire

Sans objet

6.1.3. Transmission de clé publique à l'AC

Le protocole utilisé pour la transmission de la clé publique du porteur à l'AC est accompagné de mesures garantissant l'intégrité et l'authentification d'origine. La procédure de délivrance du certificat est liée de manière sécurisée à l'enregistrement associé ou au changement de bi-clé, ainsi qu'à la fourniture de la clé publique par le porteur.

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

4096 bits pour la taille des clés AC
2048 bits pour la taille des clés des porteurs

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

Cf. document profils [R5].

6.1.7. Objectifs d'usages de la clé

L'utilisation de la clé privée d'AC et du certificat associé est limitée à la signature de certificats et de LCR, comme définie dans le document description des certificats et des LCR [R5]. La clé privée d'AC n'est utilisée que dans un environnement sécurisé.

L'utilisation de la clé privée du porteur et du certificat associé est limitée à l'authentification du porteur comme définie dans le document description des certificats et des LCR [R5].

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

Le module cryptographique de l'AC pour la génération et la mise en œuvre des clés de signature répond aux exigences énoncées par la réglementation.

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

Le module cryptographique de signature de certificat et des informations de révocation ne fait pas l'objet de manipulation non autorisée lors de son stockage.

Le module cryptographique de signature de certificat et des informations de révocation fonctionne dans les conditions prévues par le fournisseur.

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

6.2.1.2. Module cryptographique des porteurs

Les dispositifs d'authentification mis à la disposition des porteurs sont évalués 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 par au moins trois personnes.

6.2.2.2. Module cryptographique des porteurs

Le module cryptographique du porteur est sous son contrôle exclusif.

6.2.3. Séquestre de la clé privée

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

6.2.4. Copie de secours de la clé privée

6.2.4.1. Clés de l'AC

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

6.2.4.2. Clés des porteurs

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

6.2.5. Archivage de la clé privée

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

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

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

6.2.6.2. Transfert de la clé privée des porteurs

Les clés privées des porteurs ne peuvent pas être transférées en dehors du QSCD.

6.2.7. Stockage de la clé privée dans le module cryptographique

6.2.7.1. Stockage de la clé privée de l'AC

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

6.2.7.2. Stockage de la clé privée des porteurs

Le stockage de la clé privée est réalisé par le QSCD 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

6.2.8.1. Activation de la clé privée de l'AC

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

6.2.8.2. Activation de la clé privée des porteurs

La clé privée est activée à l'aide d'un code PIN personnel et connu exclusivement du porteur.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Désactivation de la clé privée de l'AC

La clé privée est désactivée à partir du module cryptographique.

6.2.9.2. Désactivation de la clé privée des porteurs

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

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

6.2.10.2. Destruction de la clé privée des porteurs

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

6.2.11. Niveau d'évaluation sécurité du module cryptographique

6.2.11.1. Module cryptographique de l'AC

Les modules cryptographiques de l'AC ont fait l'objet d'une évaluation EAL 4+.

6.2.11.2. Module cryptographique des porteurs

Les modules cryptographiques de l'AC ont fait l'objet d'une évaluation EAL 4+.

6.3. Autres aspects de la gestion des bi clés

6.3.1. Archivage des clés publiques

Les clés publiques de l'AC et des porteurs 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 ont une durée de vie de huit ans.

Les clés d'authentification et les certificats des porteurs ont une durée de vie de trois ans.

Les clés de signature et les certificats des réponses OCSP ont une durée de vie de trois 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

Voir PC NOTAIRES DE FRANCE [R6].

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

L'AC ne génère pas la clé privée du porteur ; les données d'activation sont nécessaires à l'initialisation du QSCD par le porteur lui-même.

6.4.2. Protection des données d'activation

Seul le document remis par le mandataire au porteur lors du face à face de validation de la demande initiale ou de renouvellement contient les éléments d'activation du QSCD.

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 [R3].

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 [R3].

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

6.5.1.7. Supervision et contrôle

Une surveillance permanenteest 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.

6.5.1.9. Exigences spécifiques au QSCD

La préparation du QSCD fait l'objet d'un contrôle de sécurité par l'OSC.

Le stockage et la diffusion du QSCD sont sécurisés.

Les désactivations et réactivations du QSCD font l'objet d'un contrôle de sécurité.

Les données d'activation sont établies de façon sécurisées et diffusées séparément du QSCD.

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

Les profils des certificats et des LCR sont décrits dans un document intitulé « description des certificats et des LCR [A4] ».
Ce document est publié par REAL.NOT sur le site https://www.preuve-electronique.org.

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

Le service OCSP est conforme à la RFC 6277 et la RFC 2560.
Le service est accessible aux serveurs du système d'informations de REAL.NOT et sur Internet.

7.3.1. Numéro de version

La demande et la réponse OCSP sont en version 1.

7.3.2. Extensions OCSP

Demande OCSP :

- Les condensats fournis dans la demande OCSP doivent être calculés avec l'algorithme SHA256 ou SHA512 en fonction du contenu de la demande.

Réponse OCSP :

- La réponse contient le nom de l'AC signataire.

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 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

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 :
- Les clés privées de porteurs et d'AC
- Les codes d'initialisation des QSCD
- Les journaux d'événements
- Les dossiers d'enregistrement des porteurs
- 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

Les informations à caractère personnel sont les suivantes :

- Les causes de révocation qui restent confidentielles et ne sont pas publiées ; elles ne sont accessibles qu'au porteur, uniquement sur demande écrite et authentifiée auprès de l'autorité de certification. Le porteur peut utiliser le formulaire de demande qui est indexé sur le portail intranet des notaires ou bien adresser une demande datée et signée, sur papier libre, en mentionnant les éléments d'identification suivants : nom, prénom, adresse postale, n° de titulaire de clé REAL, date de fin de validité de la clé REAL révoquée et n° de CRPCEN de l'instance dont dépend la clé REAL révoquée.
- les informations d'enregistrement.

9.4.3. Informations à caractère non personnel

Pas d'exigence spécifique.

9.4.4. Responsabilité en terme de protection des données personnelles

Il est entendu que toute collecte de données à caractère personnel par l'AC est réalisée dans le strict respect des lois et règlements en vigueur, en particulier de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [A6].

L'AC reconnaît avoir procédé aux formalités déclaratives qui leur incombent au titre de la présente PC et des traitements de données à caractère personnel qui seraient réalisés.

9.4.5. Notification et consentement d'utilisation des données personnelles

Le futur porteur a notification d'utilisation des données personnelles [R4], et donne son consentement lors de la phase d'enregistrement. Le porteur peut avoir accès aux informations d'enregistrement.

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

Le porteur a le devoir de :

- Communiquer des informations exactes et à jour lors de sa demande ou du renouvellement du certificat
- Protéger sa clé privée par des moyens adaptés à son environnement
- Protéger ses données d'activation et les mettre en œuvre
- Protéger l'accès à sa base de certificat
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant
- Informer l'AC de toute modification des informations contenues dans son certificat
- Faire sans délai une demande de révocation auprès du mandataire ou de l'OSC en cas de perte, de compromission ou de suspicion de compromission de sa clé privée
- Interrompre immédiatement et définitivement l'usage de sa clé privée en cas de compromission

La relation entre l'AC et le porteur est formalisée par un engagement du porteur.

9.6.4. 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 du certificat du porteur jusqu'à l'AC NOTAIRES DE FRANCE et contrôler la validité des certificats

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 en vertu de la présente Politique Certification sont des certificats dont les conditions d'utilisation sont définies par la présente Politique Certification et par les conditions générales d'utilisation qui définissent les relations entre AC REAL et les notaires ainsi que leurs collaborateurs.

Les relations entre le CSN et le porteur du certificat sont régies par les conditions générales d'utilisation du certificat.

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 soumis 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.

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

Les conditions générales d'utilisation [R4] sont diffusées et acceptées par les porteurs de clé REAL au moment de la saisie de leur demande de clé REAL dans SACRE.

Une nouvelle version des conditions générales d'utilisation fera apparaître les évolutions afin de faciliter la lecture des nouvelles dispositions par le porteur de clé REAL.

10. Documents associés

10.1. Documents applicables

[A1]	RFC 3647. Internet X509 PKI certificate policy and certificate practice statement framework
[A3]	Règlement Européen eIDAS 910/2014
[A4]	Infrastructure de Certification Notariale. Description des certificats et des CRL
[A5]	ISO/IEC 9594. Distinguished name
[A6]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004
[A8]	EN 319401 « General Policy Requirements for Trust Service Providers »
[A9]	EN 319411-1 « General requirements »
[A10]	EN 319412-1 « Overview and common data structures »
[A11]	EN 319412-2 « Certificate profile for certificates issued to natural persons »

10.2. Documents de référence

[R1]	Analyse de risques sur l'infrastructure de gestion de clés de Real.not
[R2]	Plan de reprise d'activité
[R3]	Déclaration des Pratiques de Certifications de l'AC REALAUTH
[R4]	Conditions Générales d'Utilisation des certificats de l'AC REALAUTH
[R5]	Profils des certificats et LCR
[R6]	Politique de Certification de l'AC NOTAIRES DE FRANCE
[R7]	Répondre à une demande de statut de certificat périmé
[R8]	Procédure de cessation d'activité
[R9]	Transfert des activités OSC

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
00.1	08/11/2016	Y. Thomassier	D. Lefèvre	Membres du bureau CSN
00.2	27/01/2017	Y. Thomassier	D. Lefèvre	Membres du bureau CSN
00.3	17/08/2017	P.Pellegrin	Y. Thomassier	Membres du bureau CSN
00.4	05/03/2018	P.Pellegrin	Y. Thomassier	Membres du bureau CSN