CONSEIL SUPÉRIEUR DU NOTARIAT

DPC Signature Certificats Qualifiés – Format RFC 3647

Déclaration des Pratiques de Certification
Pour les Certificats Qualifiés Support au Service de Signature

DPC REALSIGN

Statut du document : Standard
Version : 01.4
Date de la dernière mise à jour: 01/03/2017

PUBLIÉ

Entrée en vigueur le 02/03/2017

Historique du document

01/03/2017

Version : 1.4, Standard
Prise en compte des remarques de l'audit eIDAS phase 1

08/02/2017

Version : 1.3, Standard
Prise en compte des remarques de l'audit à blanc CSN

27/01/2017

Version : 1.2, Standard
Prise en compte des remarques de l'audit à blanc CSN

13/12/2016

Version : 1.1, Standard
Prise en compte des remarques de l'audit à blanc

15/09/2007

Version : 01.0, Standard
Création du document et reprise du contenu de la DPC de l'AC REAL

Table des matières

1. Introduction

1.1. Présentation générale

Le présent document présente les pratiques suivies par le Conseil Supérieur du Notariat dans la mise en place et la fourniture de ses prestations de service de certification électronique à destination des Notaires de France et de leurs collaborateurs à des fins de signature électronique.

Sa structure est conforme au RFC 3647, [A1] et les exigences couvertes sont décrites dans le document [A2].

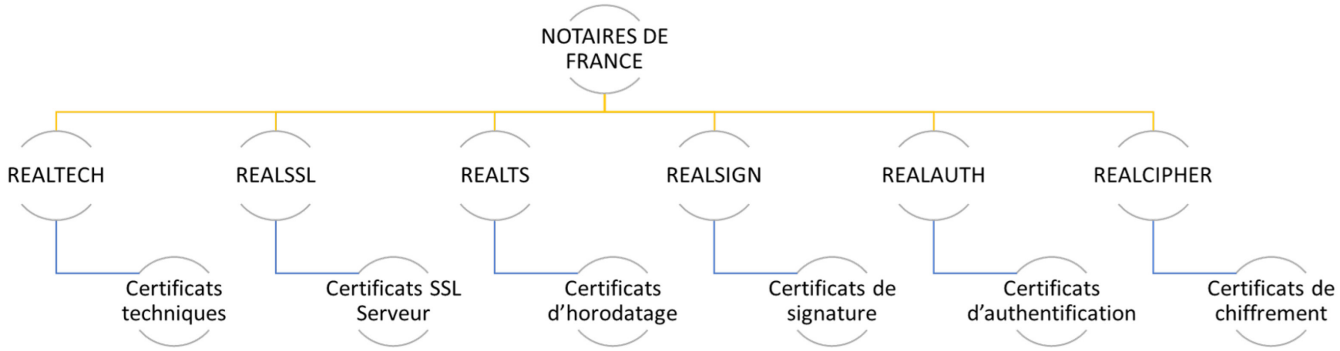
1.2. Identification du document

Le numéro d'OID de la présente DPC est 1.2.250.1.78.2.1.3.1.1.2

Le numéro d'OID de la PC correspondante est 1.2.250.1.78.2.1.3.1.1.1

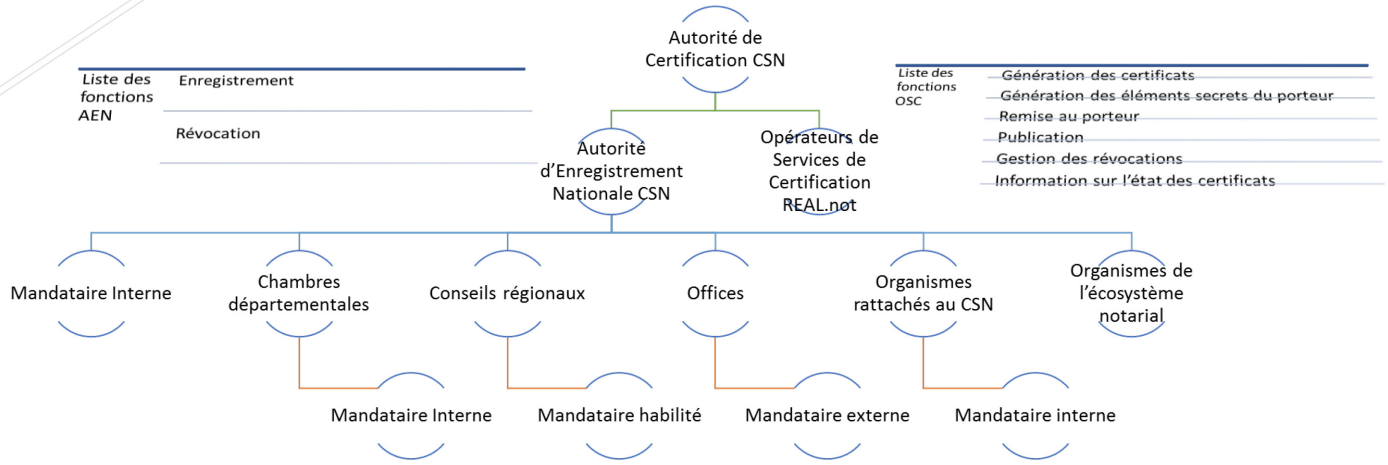
1.3. Entités intervenant dans l'IGC

Les certificats de signature des Notaires et de leurs collaborateurs sont générés par la composante dite AC-REALSIGN, dont les certificats de signature sont eux même générés par la composante AC-NOTAIRES DE FRANCE. Cette dernière composante est l'AC Racine. L'ensemble constitue une hiérarchie de certification présentée dans le schéma ci-dessous. La présente déclaration de pratiques correspond à l'AC REALSIGN.



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. Autorité de certification

L'Autorité de certification est le CSN. Elle est en charge de l'application des pratiques par les entités concernées.

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 de signature. Ce sont :

- d'une part les bi clés et certificats utilisés par les Notaires pour la signature des actes authentiques sur support électronique et les échanges dématérialisés,
- et d'autre part les certificats utilisés par les Notaires, leurs collaborateurs, ou le CSN, ses collaborateurs ainsi que les organismes rattachés et les organismes de l'écosystème notarial et leurs collaborateurs pour la signature de données électroniques.

Chaque certificat de signature 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]).

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.

1.3.6. Utilisateurs de certificats

La présente déclaration de pratiques recouvre la gestion des certificats de signature, destinés exclusivement à un usage interne, qui comportent deux sous-ensembles correspondant à une utilisation distincte :

- la signature des actes authentiques électroniques. Ces actes peuvent être échangés entre Notaires, ou enregistrés dans le minutier central (MICEN) ; ces certificats sont réservés aux Notaires;
- la signature de documents ; ces certificats sont distribués aux Notaires, à leurs collaborateurs, aux collaborateurs du CSN ou des organismes rattachés ;
- la signature de flux dématérialisés.

1.4. Usage des certificats

1.4.1. Domaines d'utilisation applicables

La présente déclaration de pratiques de certification traite des bi-clés et de certificats des porteurs identifiés par le KeyUsage « non-repudiation ».

Les domaines d'utilisation applicables, ainsi que les exigences relatives aux bi-clés et certificats d'AC et des composantes sont définis dans la PC relative à l'AC NOTAIRES DE FRANCE [A3].

La politique de certification est disponible à l'adresse http://www.preuve-electronique.org

1.4.2. Domaines d'utilisation interdits

L'utilisation des bi-clés et certificats est strictement limitée à la seule fonction de signature des actes authentiques ou des autres types d'information, selon la catégorie considérée, au sein de la communauté notariale.

1.5. Gestion de la DPC

1.5.1. Entité gérant la DPC

La gestion de la DPC 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

L'approbation de la conformité de la DPC à la Politique de certification est prononcée par le CSN, au vu des audits internes effectués. REAL.NOT est en charge du suivi de l'audit interne (constitution de l'équipe, validation du plan d'audit, couverture des non-conformités éventuelles). REAL.NOT fait mention des résultats de l'audit interne au cours d'une réunion avec le CSN et le compte rendu de cette réunion mentionne les écarts et le plan d'action associé. L'approbation formelle de conformité sera prononcée par l'organisme en charge de l'évaluation du CSN en tant que prestataire de service de certification électronique qualifié.

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. L'approbation formelle de conformité sera prononcée par l'organisme en charge de l'évaluation du CSN en tant que prestataire de service de certification électronique qualifié.

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
OID	Identifiant d'objet (**O**bject **ID**entifier)
OSC	**O**pérateur de **S**ervice de **C**ertification
PC	**P**olitique de **C**ertification
PRIS	**P**olitique de **R**éférencement **I**ntersectorielle de **S**écurité

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)
REAL	**R**éseau **E**lectronique notari**AL**
SACRE	**S**uivi **A**dministratif des **C**lés **Re**al

1.7. Définitions

Authentification
Processus permettant de vérifier l'identité déclarée d'une personne ou de toute 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 la 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.

Dispositif de création de signature électronique Qualifié (QSCD)
Matériel ou logiciel, destinés à mettre en application les données de signature électronique, qui satisfait aux exigences définies par la règlementation

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.

Organismes de l'écosystème notarial
CDC (Caisse des dépôts) et CRN (Caisse de Retraite des Notaires) qui disposent uniquement de clés REAL collaborateurs. Les mandataires de ces organismes sont les membres du bureau du CSN.

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

Le CSN, responsable de l'AC, fournit la politique de certification, et les conditions générales d'utilisation auprès de l'OSC REAL.NOT.

L'OSC rend ces informations accessibles via Internet, sur le site https://www.preuve-electronique.org

L'OSC met à disposition les informations de gestion des certificats. Ces informations sont accessibles sur l'Intranet au travers de l'annuaire de publication des LCR par LDAP, sur l'adresse : ldap ://annuaire.real.notaires.fr:389 et ldaps://annuaire.real.notaires.fr :636, ou sur Internet sur le site https://www.preuve-electronique.org.

L'OSC est également en charge de la publication des formulaires à imprimer, accessibles au travers du portail sacre.real.notaires.fr.

2.2. Informations devant être publiées

Les informations publiées sont les suivantes :

- La politique de certification de l'AC REALSIGN [A2] ainsi que la Politique de Certification de l'AC NOTAIRES DE FRANCE [A3]
- La déclaration de pratiques de l'AC REALSIGN ainsi que les Conditions Générales d'Utilisation associées
- Le document présentant les profils des certificats et LCR [R25]
- La liste des certificats révoqués (LCR) pour les pour les porteurs et l'AC
- Les certificats de l'AC REALSIGN 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 REALSIGN)
- 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 https://sacre.real.notaires.fr par les porteurs.

Les documents PC, DPC et CGU sont publiés :

- au format PDF/A
- en français et en anglais.

2.3. Délais et fréquences de publication

Les politiques de certification sont remises à jour et publiées tous les deux ans.

Les formulaires peuvent être modifiés autant que de besoin.

Les certificats d'AC sont diffusés ou mis en ligne préalablement à toute diffusion de certificats porteurs ou CRL, dans un délai de 24 heures.

La publication des LCR est réalisée deux fois par jour à intervalle de 12h. Une LCR est également publiée après un lot de révocations proches dans le temps.

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 et LCR sont accessibles en lecture de manière internationale à toute personne souhaitant en prendre connaissance.

- Tous ces documents publiés sont en lecture seule par les utilisateurs y accédant par navigateur ;
- L'accès aux informations de l'annuaire est ouvert à modification après authentification (identifiant/mot de passe) auprès de l'annuaire ;
- Les fichiers LCRs sont mis à jour entre le serveur AC et le serveur de publication. Les accès au serveur de publication sont contrôlés par filtrage de flux et contrôle applicatif de l'origine du flux de mise à jour.

Les ajouts, suppressions et modifications se font au travers d'un process automatique qui fait l'objet d'une demande de changement par les personnes autorisées de l'AC ou de l'OSC. Ces demandes sont tracées dans l'outil de suivi des demandes de changement.

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) [A4], 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 »
- 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>)

Le champ pays est valorisé à FR (France) car les certificats sont émis par le Conseil Supérieur du Notariat français, dans le cadre des missions d'officier public ministériel des notaires, nommés par le ministère de la justice, et de leurs collaborateurs.

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 de description des certificats et LCR [R25]

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 par un navigateur à l'adresse : https://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.

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
- 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, en usant de sa compétence de notaire, 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 SSCD, ne nécessite donc pas de preuve de possession de la clé privée :

Le support utilisé est :

- la carte Oberthur COSMO V7.0.1-R2 IAS-ECC, certifiée EAL4+ et qualifiée QSCD.

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 du 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. L'enregistrement peut comporter également un formulaire de recueil de signature manuscrite, de sceau ou de 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 du CSN). 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.

Les demandes de clé REAL de tests sont effectuées par un opérateur SACRE disposant de droits particulier via une IHM spécifique. L'utilisateur autorisé se connecte sur SACRE ADMIN de manière sécurisée sur l'interface de l'outil de génération de clé Real de test.

Les informations du titulaire de la clé REAL de tests sont renseignées :

- Nom

- Prénom
- Profil (Notaire, Collaborateur)
- Email
- Mot de passe de la demande

Après validation, le système :

- Crée un nouvel utilisateur dans SACRE, sur le CRPCEN des clés de test défini en configuration, avec un numéro de titulaire respectant le format défini. En cas de doublon détecté, l'utilisateur existant est réutilisé,
- Crée une demande dans SACRE d'un nouveau type « Demande de clé de Test » associé à cet utilisateur
- La valide automatiquement
- Affiche à l'utilisateur :
    - Le numéro de titulaire
    - Le code d'activation

Les étapes suivantes consistent à initialiser la clé via l'applet d'initialisation et en positionnant un DN qui est, pour tous les certificats de signature produits de la forme suivante :

DN: CountryName=FR, SurName=NOM [FOR TEST ONLY], GivenName=Prénom, CommonName=NOM Prénom (N° de titulaire)

Les certificats sont signés par les AC de production au même titre que les clés standards. La clé est personnalisée graphiquement à la main. La clé ainsi générée est alors pleinement fonctionnelle.

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.

Les demandes de clé REAL de tests sont effectuées par un opérateur SACRE disposant de droits particulier via une IHM spécifique. L'utilisateur autorisé se connecte sur SACRE ADMIN de manière sécurisée sur l'interface de l'outil de génération de clé Real de test.

Les informations du titulaire de la clé REAL de tests sont renseignées :

- Nom
- Prénom
- Profil (Notaire, Collaborateur)
- Email
- Mot de passe de la demande

Après validation, le système :

- Crée un nouvel utilisateur dans SACRE, sur le CRPCEN des clés de test défini en configuration, avec un numéro de titulaire respectant le format défini. En cas de doublon détecté, l'utilisateur existant est réutilisé,
- Crée une demande dans SACRE d'un nouveau type « Demande de clé de Test » associé à cet utilisateur
- La valide automatiquement
- Affiche à l'utilisateur :

- Le numéro de titulaire
- Le code d'activation

Les étapes suivantes consistent à initialiser la clé via l'applet d'initialisation et en positionnant un DN qui est, pour tous les certificats de signature produits de la forme suivante :

DN: CountryName=FR, SurName=NOM [FOR TEST ONLY], GivenName=Prénom, CommonName=NOM Prénom (N° de titulaire)

Les certificats sont signés par les AC de production au même titre que les clés standards. La clé est personnalisée graphiquement à la main. La clé ainsi générée est alors pleinement fonctionnelle.

3.2.4. Informations non vérifiées du porteur

Sans objet.

3.2.5. Validation de l'autorité du demandeur

La validation de l'autorité d'un demandeur est effectuée lors du face à face entre le demandeur et le mandataire. Elle est basée sur l'ensemble du dossier décrit en 3.2.3

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

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.

3.2.7. Critères d'interopérabilité

Sans objet

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

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

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

Une demande de renouvellement des clés ne peut être effectuée qu'avec la possession d'un certificat valide du porteur.

Ce renouvellement donne systématiquement lieu à la fourniture d'un nouveau QSCD

Le demandeur saisit une demande électronique de renouvellement de certificat / QSCD en s'adressant à l'OSC par l'intermédiaire de l'application SACRE. Pour cela il se connecte par un navigateur à l'adresse : https://sacre.real.notaires.fr avec sa clé courante valide.

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 (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 collaborateur.

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

La demande de renouvellement est identifiée lorsque le porteur signe le formulaire de demande de renouvellement par l'intermédiaire de sa clé valide.

SACRE vérifie la validité de la signature du demandeur et place la demande à disposition du mandataire du demandeur.

L'application lui retourne un identifiant de demande de renouvellement. 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 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).

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.

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

3.3.2. Identification et validation pour un renouvellement après révocation

En cas de renouvellement après révocation, le titulaire procède 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. L'identification de la demande se fait alors conformément à une première demande.

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 au travers de l'application SACRE.

Si le demandeur est un notaire, il saisit une demande de révocation dans l'application SACRE en la signant électroniquement au moyen de son QSCD et clé associée.

La révocation d'urgence est à l'initiative du titulaire. Elle peut être effectuée sur l'intranet, à l'adresse https://sacre.real.notaires.fr. Le titulaire saisit une demande de révocation d'urgence dans l'application SACRE en s'identifiant au moyen de la question de confiance.

Elle peut être effectuée par Internet en se connectant à l'adresse http://revocation-carte-real.notaires.fr ou par téléphone au numéro 0820 88 77 63. 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'enregistrement. Cf. Procédure [R19].

La révocation d'un certificat suite à un renouvellement technique à l'initiative de l'AC 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 électronique correspondant, disponible dans l'application SACRE.

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

Le demandeur de certificat renseigne le formulaire correspondant par l'intermédiaire d'un navigateur, en se connectant sur le serveur web SACRE situé sur l'Intranet. Le demandeur se connecte sur le site intranet https://sacre.real.notaires.fr

La signature du formulaire papier de demande de clé REAL par le futur porteur signifie l'accord du porteur.

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 de l'office, téléphone, fax, et adresse de messagerie électronique, les fax et adresse postale n'étant pas systématiques.
- Un mot de passe
- Une pièce d'identité (carte nationale d'identité, passeport ou titre de séjour)
- Un document établissant le rattachement du futur porteur à l'organisme, validé par le responsable (attestation de l'employeur pour un collaborateur ou copie de l'arrêté de nomination ou de la prestation de serment pour 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 collaborateurs

Le dossier comporte également un formulaire papier de demande, contenant les CGU associées, 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

Les éléments constitutifs de la demande (papiers et formulaires électroniques) sont vérifiés par le mandataire. La validité des formulaires papiers ainsi que la validité des informations de la demande électronique est vérifiée.

Les éléments vérifiés par le mandataire sont (voir chapitre 3.2) :

- Le formulaire électronique de demande dans l'application SACRE
- Le formulaire papier complété et signé
- Les documents papier annexes

Les critères de refus d'une demande par le mandataire sont :

- La non validité de documents (document erroné, document caduque, suspicion de faux)
- L'incohérence entre le formulaire papier signé et les informations saisies dans SACRE
- L'incomplétude du dossier

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 ou 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.

La phase d'initialisation du QSCD est effectuée sans pause. La récupération du certificat sur le QSCD est faite séquentiellement après la génération du certificat.

4.3. Délivrance du certificat

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

L'AC ne peut être sollicitée par le demandeur que si le mandataire en a préalablement validé la demande.

L'AC n'est sollicitée par le porteur que durant la phase d'initialisation du QSCD (fourniture de la clé publique du demandeur à l'AC, qui fournit en retour le certificat).

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 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. C'est lors de la phase d'initialisation que l'AC notifie le porteur de la délivrance du certificat.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

Le certificat de signature est élaboré en ligne, et transmis lors de la phase d'initialisation du QSCD. Le certificat est présenté à l'utilisateur qui l'accepte 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 fait une nouvelle demande.
Les cas pour lesquels le QSCD est inutilisable sont décrits dans le document [R26].

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, par l'intermédiaire des fonctions d'administration de SACRE.

4.5. Usage de la bi-clé et du certificat

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

4.5.1.1. Catégorie signature d'acte authentique

L'utilisation de la clé privée par le porteur est limitée à la signature des actes authentiques. Cet usage est indiqué explicitement dans les extensions du certificat KeyUsage (KeyUsage = NonRepudiation) [R25].

4.5.1.2. Catégorie signature d'autres types de données

L'utilisation de la clé privée par le porteur est limitée aux signatures de données, mais n'est pas recevable pour la signature d'acte authentique. Cet usage est indiqué explicitement dans les extensions du certificat KeyUsage (KeyUsage = NonRepudiation) [R25].

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 des signatures apposées sur les actes authentiques dématérialisés, ou sur d'autres types de données selon la catégorie considérée.

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

En mode nominal, un courriel est envoyé 3 mois avant échéance au porteur, informant de la procédure. Si la demande de renouvellement n'est pas faite, un nouveau courriel est envoyé 2 mois, puis 1 mois avant échéance.

La demande de nouveau certificat est à l'initiative du porteur ; elle peut être effectuée à tout moment avant expiration du certificat en cours. Une fois la date d'expiration atteinte, le porteur procède comme pour une nouvelle demande de certificat.

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

L'identité du porteur demandant le renouvellement et sa connaissance des modalités applicables sont validées électroniquement par le mandataire externe ou interne dans le workflow applicatif avec face à face.

La demande est ensuite validée, vérifiée puis approuvée (cf. 3.2).

Cf. 4.2.2. pour l'acceptation ou le rejet de la demande par le CSN, et 4.2.3 pour la durée d'établissement du certificat.

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

Dans le cas nominal : Cf. 4.3.2 sinon sans objet.

4.7.5. Démarche d'acceptation du nouveau certificat

Cf. 4.4.1

4.7.6. Publication du nouveau certificat

Cf. 4.4.2

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

Cf. 4.4.3.

4.8. Modification du certificat

La modification d'un certificat n'est pas autorisée

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

L'autorité ne permet pas la suspension de certificat. Seule la révocation de certificat est permise.

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 REALSIGN
- Cessation d'activité de l'AC NOTAIRES DE FRANCE

4.9.1.2. Certificat d'une composante de l'IGC

Voir PC de l'AC NOTAIRES DE FRANCE [A3]

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 certificats qui lui sont rattachés
- un Notaire pour les certificats 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

Le système de révocation est synchronisé par rapport à l'heure UTC à la seconde près.

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 à l'adresse http://revocation-carte-real.notaires.fr ou par téléphone au N° indigo 08 20 88 77 63 pour la révocation d'urgence.

Un porteur peut révoquer son certificat en indiquant son nom et prénom, son numéro de titulaire et la réponse à la question de confiance.

Le notaire peut révoquer la carte d'un collaborateur de l'office. Le notaire saisit une demande de révocation dans le système informatique en la signant électroniquement avec son QSCD.

4.9.3.2. Certificat d'une composante de l'IGC

Voir PC de l'AC NOTAIRES DE FRANCE [A3]

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. Une fois la demande de révocation traitée la publication dans la LCR intervient au maximum 60 minutes après.

4.9.5.2. Certificat d'une composante de l'IGC

Voir PC de l'AC NOTAIRES DE FRANCE [A3]

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

L'utilisateur d'un certificat (par exemple les logiciels de signature et de vérification de signature d'actes authentique, le logiciel SACRE lors de la signature des demandes de renouvellement) est tenu de vérifier l'état du certificat et des certificats constituant la chaîne de confiance (AC REALSIGN // AC NOTAIRES DE FRANCE).

L'utilitaire de signature retenu par la profession rend la vérification obligatoire.

Pour vérifier l'état du certificat, l'utilisateur s'appuie sur les LCR publiées régulièrement pour les différentes AC (cf 4.10.1).

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

Les LCR sont rendues publiques et visibles de manière internationale dans un délai maximal de 60 minutes.

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

Les systèmes de révocation et de vérification ont un taux de disponibilité de 99,5 pour cent, et sont disponibles sous 24 heures. . 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. Cf. Procédures [R23] et [R16].
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

Cf. 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 par la Politique de Certification.

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

4.10.2. Disponibilité de la fonction

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

4.10.3. Dispositifs optionnels

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 [R28]).

4.11. Fin de la relation entre le porteur et l'AC

La fin de la relation entre le porteur et l'AC est une cause de révocation.

4.12. Séquestre de clé et recouvrement

4.12.1. Politique et pratiques de recouvrement par séquestre de clés

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

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

Sans objet

5. Mesures de sécurité non techniques

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

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

La localisation géographique des sites (Venelles et Clichy pour l'OSC, Paris pour l'AEN) 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, 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, et par la mise en place d'un contrôle d'accès électronique par badge ou clé.

La traçabilité des accès est assurée par l'enregistrement des utilisations des badges électroniques.

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

L'accès physique aux fonctions de génération des éléments secrets du porteur est strictement limité au porteur par la possession du QSCD nominatif et la connaissance de l'authentifiant au QSCD.

Des mesures de sécurité physique sont également mises en place pour limiter les accès aux supports sensibles (dossier d'enregistrement, documents d'applications) en plaçant les documents dans des armoires sécurisées ou locaux fermés.

Les procédures de génération, de renouvellement et de révocation technique d'un certificat sont opérées directement sur les interfaces de la PKI. Seules des personnes habilités à pénétrer dans les salles serveurs de la PKI et ayant le rôle d'opérateurs de la PKI peuvent réaliser ces actions. Le nombre de ces personnes est extrêmement restreint et l'habilitation d'une nouvelle personne nécessite la validation du responsable de l'OSC et du RSSI. Ce rôle de confiance est formalisé dans un document signé par le président de 'REAL.NOT et le titulaire en question.

Les responsables des organismes (chambres, conseils régionaux, CSN et organismes rattachés) et les titulaires d'office 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 (mise en œuvre de moyens techniques tels que des onduleurs et groupes électrogènes, avec redondance des équipements), ou une défaillance de climatisation (redondance climatiseurs, alarmes de dysfonctionnement), 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 sont mis en œuvre pour parer les risques résiduels (installation sur un plancher en surélévation pour parer une rupture de canalisation par exemple). Cette exigence est prise en considération par l'OSC pour les aspects archivage des enregistrements, relatifs aux documents papiers qui sont stockés dans une salle choisie en conséquence. Chaque notaire responsable de l'archivage des papiers relatifs à la demande de certificat protège les documents papiers dans les lieux non sensibles au risque de dégâts des eaux (coffres, armoires).

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, en mettant en œuvre de moyen de prévention (sensibilisation et formation du personnel), de détection (détecteur fumée et incendie) et de lutte contre l'incendie (signalisation et disposition d'extincteur dans les lieux sensibles).

Les documents d'enregistrement des demandes conservés par les Notaires bénéficient des protections déjà disponibles dans les offices relatives à la conservation des actes notariés.

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. Les archives et supports électroniques d'archivage sont placés et conservés en armoires fortes. Cette exigence est prise en considération par l'OSC ainsi que par les Notaires pour les aspects archivage des enregistrements.

5.1.7. Mise hors service des supports

Les supports recensés comme sensibles en termes de confidentialité font l'objet de mesures de destruction lorsqu'ils parviennent en fin de vie (broyage sécurisé pour le papier, effacement des données). Cf. Procédure [R6].

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 nominal des informations et fonctions critiques.

L'OSC dispose de trois salles informatiques disjointes, hébergeant chacune les fonctions et données afférentes à la gestion des révocations et à l'information sur l'état des certificats (les données sont synchronisées en permanence entre les trois salles).

Une sauvegarde des clés des AC, sous la forme d'un export chiffré par le HSM, est aussi conservée dans un coffre situé dans une banque.

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance

Les rôles de confiance sont établis dans le document [R8]. 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 : OSC, AEN, mandataires internes et externes. Il fait faire les contrôles de conformité, valide les plans d'action relatives aux mesures correctives, … Le Responsable Sécurité est le RSSI du CSN ou son représentant désigné, sous le contrôle direct du président du CSN.

5.2.1.2. AEN

L'Opérateur est chargé de la numérisation des signatures manuscrites, des sceaux et des 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 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.

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. Il saisit les demandes de certificat techniques sur l'IGC et les valide au cours d'une cérémonie de clés. Il saisit également les demandes de révocation de ces certificats sous la supervision du responsable de la sécurité.

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

Les rôles de confiance définis et le nombre de personnes disposant de ce rôle de confiance pour l'OSC sont maintenus à jour dans [R15].

5.2.2. Nombre de personnes requises par tâche

Toute tâche sensible est réalisée par deux personnes au moins, chacune possédant une partie du secret.

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 autorisées conformément à leur besoin d'en connaître.

Les rôles attribués sont notifiés par écrit aux personnes concernées dans la description de poste, ou contractualisés pour les mandataires.

Les porteurs de secrets disposent également d'un code PIN personnel leur permettant d'activer la carte à puce concernant une part du secret.

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 [R8]. Une même personne ne peut disposer que d'un seul rôle de confiance.

Les rôles de confiance définis et le nombre de personnes disposant de ce rôle de confiance pour l'OSC sont maintenus à jour dans [R15].

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, gérée par l'employeur.

L'OSC s'assure que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles.

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 (hotline et processus de suivi).

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. Pour cette population, se reporter au règlement intérieur [A10]

5.3.7. Exigences vis à vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées. Il s'agit essentiellement du personnel de surveillance du site de Venelles et du site de secours de Clichy.

Les types d'engagement sont des contrats relatifs à la réalisation d'une prestation, des engagements de confidentialité et une charte d'utilisations des moyens informatiques.

5.3.8. Documentation fournie au personnel

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

5.4. Procédures de constitution des données d'audit

5.4.1. Type d'événement à enregistrer

Les événements suivants sont enregistrés :

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

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

En dehors de ces événements, l'AC maintient à jour un référentiel sur le site www.preuve-electronique.org détaillant :

- Le nom de l'AC REALSIGN ;
- L'empreinte du certificat d'AC REALSIGN ;
- La date de fin de validité du certificat ;
- Le nom de la personne responsable du certificat.

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

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

L'ensemble de la cérémonie des clés se fait sous le contrôle d'un huissier.

N°	Acteur	Description des tâches
1	Maître de cérémonie	Inscription des informations suivantes sur le Procès-verbal : - Nom de l'AC - Nom du responsable de l'AC
2	Maître de cérémonie	Signature du Procès-verbal
3	Porteur de secrets	Signature du Procès-verbal
4	Responsable de l'OSC	Conservation au coffre des éléments suivants : - Script de cérémonie - Procès-verbal signé

5.4.2. Fréquence de traitement des journaux d'événements

Les journaux d'événements sont exploités de manière quotidienne, et systématiquement en cas de remontée d'événement anormal.

5.4.3. Période de conservation des journaux d'événements

Les journaux de l'AC REALSIGN sont conservés en ligne pendant 1 an. Les journaux sont redondés sur deux sites géographiquement distants, la continuité est alors assurée. Les journaux de plus d'un an sont archivés conformément à la politique d'archivage décrite dans le paragraphe 5.5.

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 : Les évènements sont signés et chaînés.

La protection des journaux d'événements est effectuée par la protection physique du serveur dans une zone protégée et uniquement accessible par un personnel de confiance disposant de moyens d'authentification pour y accéder.

5.4.5. Procédure de sauvegarde des journaux d'événements

Les procédures de sauvegarde des journaux sont quotidiennes. La procédure est documentée dans [R13].

5.4.6. Système de collecte des journaux d'événements

Un système de collecte des journaux d'événements est mis en place. Les évènements concernés sont les suivants :

- Evènements fonctionnels afférents au cycle de vie des demandes dans SACRE (demande initiale de clé REAL, demande de renouvellement, demande de révocation, initialisation d'une clé REAL) ;
- Evènements fonctionnels afférents au cycle de vie des certificats dans la PKI (demande de certificat, révocation d'un certificat) ;
- Evènements systèmes SACRE : journaux des serveurs d'applications et des frontaux ;
- Evènements systèmes PKI : journaux des services et syslog ;
- Evènements systèmes LDAP

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 effectué de façon continue et quotidienne afin de permettre une anticipation des vulnérabilités, et des remontées d'alerte en cas de vulnérabilités.

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

5.5. Archivage des données

5.5.1. Types de données à archiver

Les données à archiver sont les suivantes :

- logiciels exécutables et fichiers de configuration
- PC, DPC et CGU
- Certificats et CRL publiés
- Dossiers d'enregistrement des porteurs
- Journaux d'événements
- Journaux de l'IGC

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 REAL	**23 ans**
CRL & Certificats clients	**23 ans**
Evènements techniques	**1 an**
Evènements fonctionnels	**23 ans**
Documentation	**10 ans**
Dossier d'enregistrement (demandes papier de certificats)	**75 ans, par le notaire**

Les dossiers d'enregistrement papier (demandes de certificats) sont archivés pendant 75 ans [A7]. Au-delà de 75 ans, les archives sont conservées 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 procède à des contrôles réguliers et assure une veille sur les formats de données pour s'assurer que ces données resteront lisibles dans le temps.

5.5.4. Procédure de sauvegarde

Le tableau suivant précise la fréquence et le support de sauvegarde par type de données.

TYPE DE DONNEES	FREQUENCE	SUPPORT D'ARCHIVAGE
Logiciels	A chaque mise en production	Bibliothèque des supports définitifs
Configurations des logiciels	A chaque mise en production	Bibliothèque des supports définitifs
Certificats de l'AC REALSIGN	A chaque cérémonie de clés	Serveur d'archivage
LCR	A chaque émission	Serveur d'archivage
Certificats clients (OT-PKI)	A chaque émission	Base de données PKI Base de données SACRE
Evènements système	Tous les jours	Serveur d'archivage
Evènements techniques	Tous les jours	Serveur d'archivage
Evènements fonctionnels	Tous les jours	Base de données PKI Base de données SACRE
Documentation	A chaque mise à jour	ARIANE
Documents papier	A chaque production	Armoire PKI

Les certificats sont archivés dans la base de données de la PKI et dans la base de données de SACRE. Aucune purge n'est prévue.

Les évènements sont journalisés, signés et chaînés dans la base de données de la PKI. Aucun évènement n'est purgé. Les évènements sont journalisés et signés (évènements d'initialisation) dans la base de données de SACRE.

Les bases de données de la PKI et de SACRE sont sauvegardées tous les soirs.

Le serveur d'archivage est sauvegardé tous les soirs également.

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. La fourniture de l'heure universelle est assurée par un service NTP fourni par le serveur d'horodatage. Ce système offre une précision de l'heure à 1 seconde.

5.5.6. Système de collecte des archives

Sans objet.

5.5.7. Procédure de récupération et de vérification des archives

La récupération et la vérification des archives sont effectuées dans un délai conforme à l'utilisation des certificats délivrés – signature d'actes authentiques. Un délai d'une semaine est acceptable par la profession. Toute vérification nécessite une demande de consultation. Cf. Procédure [R7].
Concernant les journaux de l'IGC, si la demande concerne un évènement inférieur à 1 an, les journaux sont consultables en ligne depuis les informations contenues en base de données de l'IGC, si la demande concerne un événement supérieur à 1 an, les journaux sont consultables depuis les données archivées. Les durées nécessaires pour obtenir les informations souhaitées sont :

- Sous 48 heures ouvrées pour les données en ligne
- Sous une semaine pour les données archivées.

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 est de 8 ans. La durée de vie des certificats des titulaires est de 3 ans.

La procédure de changement des clés d'AC nécessite de réaliser les actions suivantes :

1) Avertir l'ANSSI du besoin de renouvèlement
2) Procéder à la cérémonie des clés conformément au document [R3]
3) Fournir le certificat de la nouvelle AC à l'ANSSI qui se charge de l'inscrire dans la TrustedList par l'ANSSI (1 publication tous les 28 du mois)
5) Attendre la publication effective du certificat d'AC dans la TL
6) Mettre en production le nouveau certificat d'AC.

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 sont mis en œuvre : sensibilisation, formation des personnels, et analyse des différents journaux d'événements, procédure de gestion des incidents. Cf. Procédure [R2].

La procédure de gestion des incidents précise les différentes phases de constatation de l'incident, l'information de personnes compétentes, la traçabilité, la qualification, la mise en œuvre de la procédure d'escalade, la résolution et la phase de clôture de l'incident.

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 et à l'ANSSI. La publication de révocation du certificat, si elle s'avère nécessaire, est effectuée dans la plus grande urgence par tout moyen nécessaire (cf. chapitre 4.9)

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

Un plan de continuité / reprise d'activité est mis en place (Cf. Procédure [R17]) permettant de répondre aux exigences de disponibilité des différentes composantes de l'IGC ; cette exigence concerne uniquement la composante opérée par l'OSC, puisque la fonction d'enregistrement ou de révocation peut être opérée à partir de n'importe quel poste de travail connecté à l'Intranet, voire par l'Internet ou le téléphone pour la révocation.
Ce plan est testé une fois par an.

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 et des certificats qui lui sont rattachés. Cf. Procédure [R4].

L'AC REALSIGN procède dans ce cas à :

- La révocation de l'ensemble des certificats finaux émis par l'AC REALSIGN. Pour cela, le CSN demande aux mandataires (internes et externes) la révocation en cascade des certificats émis. Cette révocation est effectuée en cascade : les notaires révoquent les collaborateurs, les mandataires internes révoquent les certificats des notaires les mandataires du CSN révoquent les certificats des mandataires internes, le président révoque son propre certificat.
- La destruction de l'ensemble des clés privées correspondantes à l'AC REALSIGN ;
- La destruction de l'ensemble des copies de clés s'il en existe ;

L'AC NOTAIRES DE FRANCE procède ensuite à la révocation du certificat d'AC REALSIGN et à la génération d'une nouvelle ARL.

L'AC NOTAIRES DE FRANCE régénère un nouveau certificat d'AC REALSIGN.

Dès lors, L'AC peut reprendre l'émission des certificats en commençant par celui du président et ceux des mandataires du CSN.

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 clients, l'AC et l'OSC déclenche une cellule de crise afin de déterminer les actions à mener pour rétablir le service au plus tôt cf. [R4];

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 reprise d'activité suite à un sinistre

L'autorité de certification dispose d'une procédure de continuité d'activité couvrant son périmètre d'Autorité d'enregistrement [R24].

L'opérateur de service de certification dispose également de procédure de continuité d'activité [R16] [R17].
Les sinistres couverts par le plan de continuité d'activité sont les suivants :

Sinistres	**Autorité de Certification**	**Opérateur de Certification**
Erreur de maintenance	Oui	Oui
Incendie	Oui	Oui
Inondation	Oui	Oui
Panne électrique	Oui	Oui
Panne réseau	Oui	Oui
Accessibilité des locaux	**Oui**	**Partiellement (sauf production des clés REAL et Hotline)**
Pandémie	Oui	Oui
Empêchement du président	Oui	N/A

L'autorité de certification peut se replier sur la chambre des notaires de Paris en cas de besoin.

L'opérateur de service de certification dispose d'un site de secours informatique à Clichy.

REAL.NOT dispose d'une procédure de gestion de crise [R23] qui implique le CSN quand cela est nécessaire.

Le CSN ne dispose pas de procédure de gestion de crise à part entière mais pour les cas qui concerneraient la partie PSCE, le CSN avertira REAL.NOT du repli éventuel vers son site de secours et fera partir le cas échéant une communication auprès des offices pour les informer de la situation notamment pour le traitement des demandes initiales.

La communication vers les offices sera effectuée à partir de la base d'emails commune CSN / REAL.NOT, chacune des deux entités ayant la capacité d'envoyer des emails en masse à destination des offices.

5.8. Fin de vie de l'IGC

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

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

Dans le cas où Real.not cesserait son activité d'OSC à la demande du CSN, Real.not déroulera la procédure [R18] 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 a défini dans la procédure [R29] les conditions de transferts des activités de l'opérateur actuel vers un nouvel opérateur.

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

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. Tous les certificats émis encore en cours de validité seront révoqués ;
4. Le certificat d'AC sera révoqué ;

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 les utilisateurs de certificats ;

6. L'AC tiendra informée l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

Cf. Procédure [R18].

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 d'AC

Voir PC NOTAIRES DE FRANCE [A3]

6.1.1.2. Clés porteurs générées par l'AC

La bi clé du porteur n'est pas générée par l'AC.

6.1.1.3. Clés porteurs générées par le porteur

La génération des bi clés du porteur est effectuée directement dans le QSCD.
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.

La technologie du QSCD est la carte Oberthur COSMO V7.0.1-R2 IAS-ECC.

Le support répond aux exigences formulées par la réglementation française dans la génération des clés par le porteur.

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 basé sur SSL entre les équipements informatiques du porteur et de l'AC, utilisé pour la transmission de la clé publique du porteur à l'AC, ainsi que l'utilisation du bi clé de chiffrement embarqué sur le QSCD garantit 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

La clé publique de l'AC est publiée sous forme de certificat, signée par l'AC NOTAIRES DE FRANCE.

6.1.5. Tailles des clés

La taille des clés d'AC est de 4096 bits.
La taille des clés des porteurs est de 2048 bits.

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

Cf document profils [A5].

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 de LCR, comme définie dans le document description des certificats et des LCR. La clé privée d'AC n'est utilisée que dans un environnement sécurisé.

L'utilisation de la clé privée du porteur et du certificat est limitée à la signature des actes authentiques, des copies authentiques et des copies exécutoires comme définie dans le document description des certificats et des LCR.

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

Cf. Procédure [R20].

6.2.1.1. Module cryptographique de l'AC

Le module cryptographique est fourni par le HSM BULL PROTECCIO, évalué EAL 4+.

- 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 peut pas faire 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 correctement.

6.2.1.2. Module cryptographique des porteurs

Les dispositifs de création de signature mis à la disposition des porteurs sont fournis par la carte Oberthur COSMO V7.0.1-R2 IAS-ECC et sont évalués EAL 4+.

Le module cryptographique est fourni par l'une ou l'autre des technologies :

- la technologie COSMO V7.0.1-R2 IAS-ECC

6.2.2. Contrôle de la clé privée par plusieurs personnes

Il n'y a pas de contrôle de la clé privée du porteur par plusieurs personnes.

Il y a un contrôle de la clé privée de l'AC par au moins deux personnes.

6.2.3. Séquestre de la clé privée

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

6.2.4. Copie de secours de la clé privée

Les clés privées de porteur ne font pas l'objet de copie de secours par l'AC.

Les clés privées d'AC font l'objet de copie de secours par l'AC. Cette copie est retracée dans la procédure de cérémonie des clés, où chaque HSM de production détient une copie des clés d'AC

6.2.5. Archivage de la clé privée

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

Les clés privées d'AC sont extraites des HSM sous la forme d'un fichier électronique chiffré par un secret partagé. L'export chiffré par le HSM des clés privées des AC est inscrit sur un support archivé dans un coffre sécurisé.

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

Il n'y a pas de transfert de clé privée en dehors de celui réalisé vers le HSM de secours : ce transfert nécessite la présence d'au moins deux personnes, et être effectué de manière à ce que ne subsiste aucune information sensible sur le serveur, tel que décrit dans le document de cérémonie des clés [R3].

6.2.7. Stockage de la clé privée dans le module cryptographique

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

6.2.8. Méthode d'activation de la clé privée

La clé privée de l'AC est activée par l'intermédiaire de l'application PKI, par la saisie d'un code PIN de déblocage de la carte Administrateur du HSM.

La clé privée des porteurs est activée par la saisie du code PIN sur le logiciel de gestion des cartes REAL.

6.2.9. Méthode de désactivation de la clé privée

La clé privée est désactivée à partir du module cryptographique.

Le module de gestion des clés privées des porteurs est l'application IAS ECC embarquée sur le QSCD Oberthur.

6.2.10. Méthode de destruction des clés privées

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

Le module de gestion des clés privées des porteurs est l'application IAS ECC embarquée sur le QSCD Oberthur.

6.2.11. Niveau d'évaluation sécurité du module cryptographique

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

Les modules cryptographiques des porteurs font 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.
Les certificats des porteurs sont contenus dans la base de données de la PKI.

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

Les bi-clés et les certificats des porteurs ont une durée de vie de trois ans.
Les clés de signature et les certificats de l'AC ont une durée de vie de huit ans

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

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

Voir PC NOTAIRE DE FRANCE [A3]

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

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

La combinaison du code d'activation et du numéro de titulaire contenus dans l'accusé de réception remis par le mandataire au porteur lors du face à face de validation de la demande initiale, et du mot de passe saisi par le porteur lors de la demande initiale de certificat permettent la protection des 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 établit l'identité de l'entité.

Différents modes d'authentifications sont utilisés selon les applications de la plate-forme OSC : par mot de passe sur la plupart des applicatifs ; l'accès à la PKI est contrôlé par certificat. Les informations d'authentification sont stockées de façon telle qu'elles sont seulement accessibles par des utilisateurs autorisés (personnel de confiance).

L'accès aux interfaces de gestion des certificats nécessitent une authentification forte basée sur au moins deux facteurs. Pour cela les administrateurs utilisent le certificat d'authentification installé sur leur clé REAL.

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 le document « Procédure de Gestion des droits OSC» [R5].

Les systèmes [Applications et bases de données] distinguent et administrent 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

Un ensemble cohérent de procédures et de documentation sous la responsabilité de l'OSC permettent l'administration et l'exploitation sécurisée de l'AC :

- 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 conditions de fin de vie (destruction et mise au rebut) des équipements sont documentées afin de garantir la non divulgation des informations sensibles qu'ils peuvent détenir.
- L'ensemble des matériels sensibles de l'IGC est maintenu afin de garantir la disponibilité des fonctions et des informations.

- Les personnels concernés par ces procédures sont désignés, conformément au document « Rôles et responsabilités, guide de l'OSC » [R8]
- 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, par l'intermédiaire des plateformes Sécurité de Rennes, fournissant les fonctions de passerelle entre l'Intranet et l'Internet, et disposant de moyen de filtrage de flux (pare-feu) et d'anti-virus.

Les composantes du réseau local (OSC) sont maintenues dans un environnement physiquement sécurisé par l'intermédiaire d'une architecture à base de pare-feux ; des vérifications périodiques de conformité de leur configuration sont effectuées.

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 avec les mandataires et autres entités intervenant dans le processus d'enregistrement.

6.5.1.6. Journalisation et audit

Un suivi d'activité est effectué au travers des journaux d'événements. Les événements journalisés sont les événements système et les événements applicatifs, tels que décrit dans le document « Procédure de journalisation des événements » [R9].
Les systèmes sont synchronisés sur l'heure UTC à la seconde près.

6.5.1.7. Supervision et contrôle

Une surveillance permanente est mise en place et des systèmes d'alarme installés pour détecter enregistrer et réagir rapidement face à toute tentative non autorisée et ou irrégulière d'accès aux ressources physique (détection d'intrusion physique dans bâtiment de l'OSC à Venelles et de Clichy) et logique (passerelles de filtrages de flux) des systèmes informatiques

6.5.1.8. Sensibilisation

Des procédures appropriées de sensibilisation des usagers du PSCE sont mises en œuvre.

Les sensibilisations concernent à la fois le personnel intervenant sur le site de l'OSC, que les personnels participant aux opérations d'enregistrement, validation et révocation des certificats.

6.5.1.9. Exigences spécifiques au QSCD

La préparation du QSCD fait l'objet d'un contrôle de sécurité par l'OSC, par le choix d'une technologie évaluée EAL4+.

Le stockage et la diffusion du QSCD sont sécurisés, tel que défini dans le document « Mode opératoire de la personnalisation des cartes » [R11].

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 : trois plateformes sont utilisées : une plateforme de développement, une plateforme de pré-production, et une plateforme de production.

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 mis en production. Cf. Procédure [R22].

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 (cf. 6.5). cf. Procédure [R21].

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 effectués 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 sur la base du protocole SSL.

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 composante locale du système d'information des accès non autorisés depuis l'Intranet et Internet ; l'infrastructure utilisée pour la délivrance de certificat de signature qualifiée est composée d'un ensemble de plateformes disposées dans des DMZ dédiées.

Les utilisateurs qui se connectent aux fonctionnalités de l'IGC peuvent provenir de plusieurs zones :

- depuis les sites des mandataires, chambre ou office
- depuis le CSN à Paris, où se situent les opérateurs,
- depuis les offices Notariaux, d'où les titulaires effectuent l'ensemble de leurs demandes auprès de l'IGC,
- depuis Internet, d'où les titulaires peuvent effectuer des demandes de révocation de certificat.

Le réseau Intranet notarial (ou réseau REAL) dispose d'une infrastructure de communication et de transport des informations sécurisée.

Un ensemble d'équipements de filtrage protègent l'IGC en scindant l'infrastructure en plusieurs zones fonctionnelles protégées.

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 dédié, intitulé description des certificats et des CRL [A5].

7.1. Profils des certificats utilisateurs

7.1.1. Numéro de version

7.1.2. Extensions de certificat

7.1.3. OID des algorithmes

7.1.4. Forme des noms

7.1.5. Contrainte sur les noms

7.1.6. OID des PC

7.1.7. Utilisation de l'extension contraintes de politique

7.1.8. Sémantique et syntaxe des qualifiants de politique

7.1.9. Sémantiques de traitement des extensions critiques de la PC

7.2. Profil des listes de certificats révoqués

7.2.1. Numéro de version

7.2.2. Extensions de CRL et d'entrées de CRL

7.3. Profil OCSP

7.3.1. Numéro de version

7.3.2. Extensions OCSP

8. Audit de conformité et autres évaluations

8.1. Fréquences et / ou circonstances des évaluations

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

Dans tous les cas, un contrôle annuel est mis en place.

8.2. Identités : qualification des évaluateurs

Le contrôleur se doit d'être 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'AEN 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

Les conditions tarifaires qui sont appliquées relativement à l'émission ou au renouvellement d'un QSCD, la mise à disposition d'un annuaire référençant les certificats, sont indiquées dans les conditions générales d'utilisation (CGU) [R12].

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 (AE) et l'OSC mettent en place un inventaire de tous les biens informationnels, conformément au document « Inventaire des biens » [R14] et procèdent à une classification de manière à définir des exigences de protection en accord avec les besoins.

En particulier, les informations suivantes sont traitées comme confidentielles (cf. analyse de risques) :

- 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.

Un notaire tiers conserve et protège l'acte notarié ainsi que les documents d'enregistrement de la demande de clé REAL, suite à la validation de la demande par le mandataire.

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. Cette demande est ensuite transmise par l'autorité de certification au service OSC qui effectuera les recherches nécessaires et lui fournira en retour la raison de révocation.
- 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

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 procède aux formalités déclaratives qui lui incombent et effectue les traitements appropriés des données à caractère personnel.

9.4.5. Notification et consentement d'utilisation des données personnelles

Le futur porteur, par la signature des Condition Générales d'Utilisation lors de la phase s'enregistrement de la demande, donne son accord d'utilisation des données personnelles. Le porteur peut avoir accès aux informations d'enregistrement, sur le site de l'application SACRE.

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

Les enregistrements sont 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 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 terme 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 de certificat :

- Communique des informations exactes et à jour lors de sa demande ou du renouvellement du certificat
- Protège sa clé privée par des moyens adaptés à son environnement
- Protège ses données d'activation
- Protège l'accès à sa base de certificat
- Respecte les conditions d'utilisation de sa clé privée et du certificat correspondant
- Informe l'AC de toute modification des informations contenues dans son certificat
- Fait 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
- Interrompt 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 :

- Vérifient l'usage pour lequel le certificat a été émis
- Contrôlent que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application

- Vérifient la signature du certificat du porteur jusqu'à l'AC profession règlementée et contrôlent la validité des certificats

9.6.5. Autres participants

Pas d'exigence particulière

9.7. Limite de garantie

9.8. 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 SSCD, des CRL 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 SSCD 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 SSCD, 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.

9.9. Indemnités

Sans objet

9.10. Durée et fin anticipée de validité de la DPC

9.10.1. Durée de validité

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

9.10.2. Fin anticipée de validité

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

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

Sans objet.

9.11. Notifications individuelles et communications entre les participants

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

9.12. Amendements à la DPC

9.12.1. Procédures d'amendements

Le CSN contrôle que tout changement apporté au présent document reste conforme aux objectifs de conformité aux exigences règlementaires en matière de certification de PSCE.

9.12.2. Mécanisme et période d'information sur les amendements

Pas d'exigence spécifique.

9.12.3. Circonstances selon lesquelles l'OID doit être changé

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

9.13. Dispositions concernant la résolution de conflits

Conformément aux textes législatifs et à la réglementation en vigueur, les certificats émis en vertu de la présente Politique 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.

REAL.NOT applique le cas échéant une procédure permettant de traiter les réclamations qui lui seront formulées.

9.14. Juridictions compétentes

Le présent document est soumis au droit français.

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

9.15. Conformité aux législations et règlementations

La présente DPC est conforme aux exigences énoncées dans les textes législatifs et règlementaires indiqués au chapitre 10.

9.16. Dispositions diverses

9.16.1. Accord global

Pas d'exigence spécifique

9.16.2. Transfert d'activités

Cf. PC

9.16.3. Conséquences d'une clause non valide

Pas d'exigence spécifique

9.16.4. Application et renonciation

Pas d'exigence spécifique

9.16.5. Force majeure

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

9.17. Autres dispositions

Sans objet

9.18. Conditions générales d'utilisation

Les conditions générales d'utilisation [R12] 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.

Toute nouvelle version de ce document annule et remplace la précédente version qui devient caduque.

Lors du renouvellement de la clé REAL les Conditions Générales d'Utilisation sont présentées et validées par le demandeur.

10. Documents associés

10.1. Documents applicables

[A1]	RFC 3647. Internet X509 PKI certificate policy and certificate practice statement framework
[A2]	CSN PC REALSIGN
[A3]	CSN. PC NOTAIRES DE France
[A4]	ISO/IEC 9594. Distinguished name
[A5]	Infrastructure de Certification Notariale. Description des certificats et des CRL
[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
[A7]	Loi n° 2008-696 du 15 juillet 2008 relative aux archives
[A8]	Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation
[A9]	Règlement Européen eIDAS 910/2014
[A10]	Règlement Intérieur REAL.NOT

10.2. Documents de référence

[R1]	Analyse de risques : eIDAS-AR2016-PSCE
[R2]	Gestion des incidents OSC/OSH
[R3]	Cérémonie des clés
[R4]	Procédure de gestion des compromissions et suspicions de compromissions de clé d'AC
[R5]	Gestion des droits OSC
[R6]	Gestion des destructions des données sensibles
[R7]	Gestion des archives OSC
[R8]	Rôles et responsabilités
[R9]	Journalisation des événements
[R11]	Personnaliser les clés REAL
[R12]	Conditions Générales d'Utilisation des clés REAL et de leurs Certificats
[R13]	Gestion des sauvegardes OSC
[R14]	Inventaire des actifs
[R15]	Lien entre individus et rôles
[R16]	Gestion du Plan de Reprise d'Activité
[R17]	Gestion de la bascule OSC
[R18]	Cessation d'activité
[R19]	Prise en compte d'une demande de révocation d'urgence par téléphone.
[R20]	Gestion des clés cryptographiques
[R21]	Maîtrise de la documentation
[R22]	Gestion des changements
[R23]	Procédure de Gestion de crise au sein de REAL.NOT
[R24]	Plan de continuité d'activités de l'AC sur son périmètre d'Autorité

	d’Enregistrement
[R25]	Description des certificats et CRL de la chaine d’AC Notaires De France
[R26]	Matrice CMS-Cartes v2
[R28]	Répondre à une demande de statut de certificat périmé
[R29]	Transfert des activités OSC

Editions successives

Version / Edition	Date	Emetteur	Valideur	Approbateur
01.0	15/09/2016	P.PELLEGRIN	D. Lefèvre Y. Thomassier	Membres du bureau CSN Direction OSC
01.1	13/12/2016	P.PELLEGRIN	D. Lefèvre Y. Thomassier	Membres du bureau CSN Direction OSC
01.2	27/01/2017	P.PELLEGRIN	D. Lefèvre Y. Thomassier	Membres du bureau CSN Direction OSC
1.3	08/02/2017	P.PELLEGRIN	D. Lefèvre Y. Thomassier	Membres du bureau CSN Direction OSC
1.4	01/03/2017	P.PELLEGRIN	D. Lefèvre Y. Thomassier	Membres du bureau CSN Direction OSC

Liste de diffusion

Publique