CONSEIL SUPÉRIEUR DU NOTARIAT

PC Signature Certificats Qualifiés – Format RFC 3647

Politique de Certification Pour les Certificats Qualifiés Support au Service de Signature

PC REAL

Référence du document : OBJ/PC/ACR/000100
Statut du document : Standard
Version : 01.17
Date 19/06/2015

PUBLIÉ

Historique du document

19/06/2015

Version: 1.17, Standard
Modification de la forme du formulaire de demande de clé REAL.
Suppression des mandataires internes délégués.
Possibilité de créer des clés REAL de test avec un profil collaborateur.

27/01/2015

Version: 1.16, Standard
Relecture 2015.

22/11/2013

Version: 1.15, Standard
Ajout du fait que la clé REAL n'est pas déblocable

06/06/2013

Version: 1.14, Standard
Mention du répondeur OCSP.
Ajout de la CDC (organisme de l'écosystème notarial).

07/03/2013

Version: 1.13, Standard
APPLI.NOT remplace REAL.NOT en tant qu'Opérateur de Service de Certification.
Plus de fourniture systématique d'un nouveau SSCD dans le cas d'un renouvellement.
Ajout de la procédure de traitement des réclamations chez REAL.NOT

11/08/2012

Version: 1.12, Standard
Précision apportée concernant le moyen de distinguer le certificat de signature et le certificat de signature authentique (paragraphe 2.3.1).
Précisions quant aux modalités de vérification de l'état du certificat (paragraphe 5.9.6).
Compléments concernant la continuité d'activité (6.7.4)
Compléments concernant les pièces justificatives du dossier d'enregistrement

02/11/2011

Version: 1.11, Standard
Complément concernant les organismes dépendant du CSN.

04/07/2011

Version: 1.10, Standard

Modification du paragraphe 5.9.9 concernant les engagements de temps de rétablissement du système.

01/03/2011

Version : 1.09, Standard

Modification du cycle de renouvellement de la clé REAL ;
Gestion de la copie numérisée de l'acte authentique de face à face.

11/08/2010

Version : 1.08, Standard

Passage de la durée légale de conservation des archives de 100 à 75 ans ;
Ajout du détail des évènements collectés ;
Ajout des url des crl;
Complément du paragraphe 5.9.9, concernant le délai de rétablissement du système de vérification de l'état des certificats en cas de défaillance ;
Ajout du paragraphe 6.7.5 concernant la compromission d'un algorithme ou d'un paramètre.
Mise à jour du paragraphe 4.2 concernant la validation de la demande initiale.

23/09/2009

Version : 01.07, Standard

Mise à jour destinée à spécifier :
- L'autorité ne permet pas la suspension de certificat émis ;
- Le remplacement de Real.not par REAL.NOT comme OSC ;
- L'archivage des évènements fonctionnels, certificats et CRL sur 6 ans ;
- La mise en place des nouveaux cheminements qui ne nécessitent plus d'approbation des demandes.

01/12/2008

Version : 01.06, Standard

Mise à jour destinée à spécifier :
- la procédure de délivrance d'une clé REAL de test de profil Notaire pour un collaborateur de l'ADSN ou d'une de ses filiales.

11/06/2008

Version : 01.05, Standard

Mise à jour destinée à spécifier :
- la procédure de consultation de la cause d'une révocation de carte par le seul titulaire de la carte.
- Les validations à effectuer par le mandataire lors d'un renouvellement sans face à face
- Mode de diffusion de nouvelles conditions générales d'utilisation

17/03/2008

Version : 01.04, Standard

Mise à jour destinée à spécifier le second mode d'approbation par robot informatique et le mode de validation des demandes de renouvellement de clé sans face à face.

20/07/2007

Version : 01.03, Standard

Mise à jour destinée à spécifier le renouvellement technique des certificats à l'initiative de l'AC.

30/05/2007

Version : 01.02, Préliminaire

Mise à jour suite à la revue interne 22 mai 2007.

Modifications mineures

05/03/2007

Version : 01.01, Draft

Création du document

Table des matières

-

1. Documents associés

1.1. Documents applicables

[A1] RFC 3647. Internet X509 PKI certificate policy and certificate practice statement framework

[A2] 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

[A3] AFNOR AC Z74-400. Exigences concernant la politique mise en œuvre par les autorités de certification délivrant des certificats qualifiés

[A4] CSN. PC Notaires

[A5] Infrastructure de Certification Notariale. Description des certificats et des CRL

[A6] ISO/IEC 9594. Distinguished name

[A7] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004

[A8] LOI n° 2008-696 du 15 juillet 2008 relative aux archives

1.2. Documents de référence

[R1] PRIS. Service de signature. Politique de certification type. Version 2.1

[R2] Analyse de risques sur l'infrastructure de gestion de clés REAL.NOT

[R3] CSN. DPC REAL.NOT

[R4] Politique de management de la sécurité. Site de Venelles

[R5] Infrastructure de Certification Notariale. Conditions Générales d'Utilisation

2. Introduction

2.1. Présentation générale

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

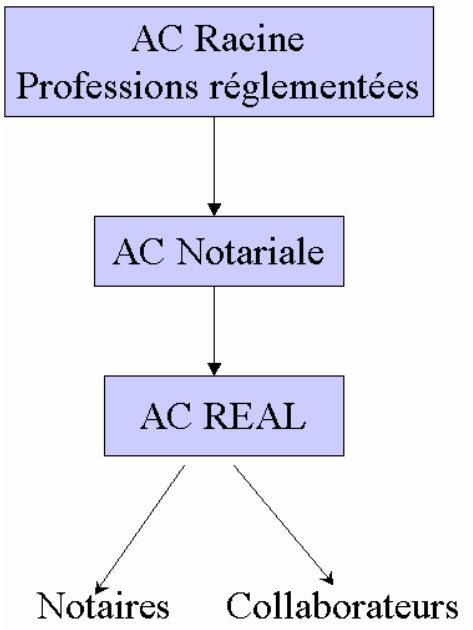
Sa structure est conforme à [A1].
Les exigences définies dans le présent document constituent « un sur » ensemble des spécifications techniques relatives aux prestataires de services de certification en vue de la reconnaissance de leur qualification définie dans l'annexe de l'arrêté du 26 juillet 2004 [A2], et en particulier des exigences définies dans le document [A3].

2.2. Identification du document

Le numéro d'OID du présent document est 1.2.250.1.78.1.1.3.1.3.1.1.22

2.3. Entités intervenant dans l'IGC

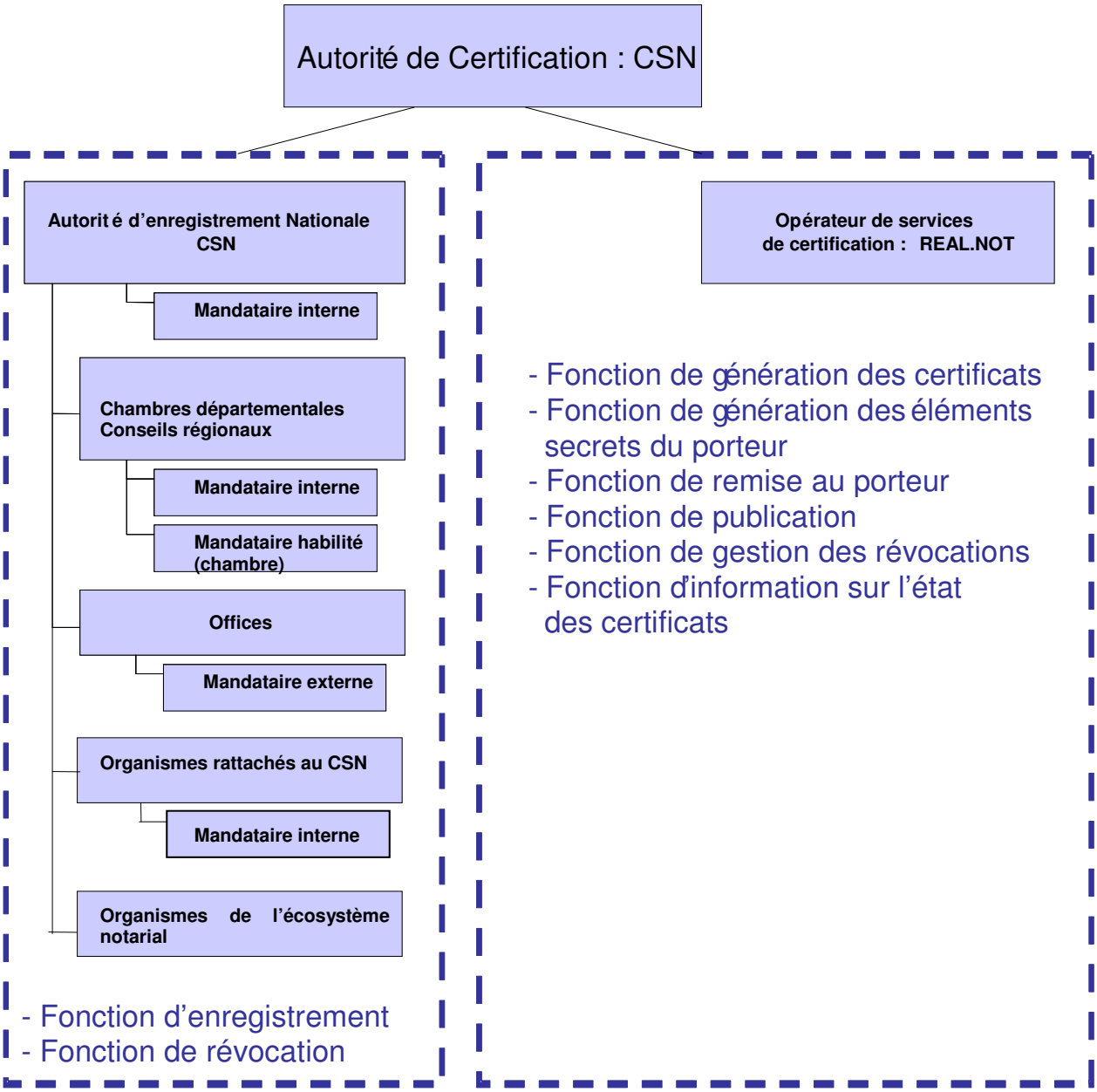
Les certificats des Notaires et de leurs collaborateurs sont générés par la composante dite AC-REAL, dont les certificats de signature sont eux même générés par la composante AC-Notaires. Cette dernière composante est rattachée à l'AC Racine dédiée aux professions réglementées. L'ensemble constitue une hiérarchie de certification présentée dans le schéma ci-dessous. La présente politique de certification correspond à l'AC REAL.



Le prestataire de service de certification électronique (PSCE) est le Conseil Supérieur du Notariat. Le CSN est également l'autorité de certification (AC) au sens de la norme AFNOR AC Z74-400 [A3],

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.



2.3.1. Autorité de certification

L'Autorité de certification est le CSN. Elle est en charge de l'application de la présente politique de certification.

L'AC fournit des prestations de gestion des certificats aux Notaires ainsi qu'à leurs collaborateurs, aux notaires des chambres départementales ainsi qu'à leurs collaborateurs, aux notaires et aux collaborateurs du CSN, à la profession notariale.

Les bi clés et certificats considérés dans le présent document sont utilisés en support de la fonction 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 d'autre part les certificats utilisés par les Notaires et 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.

Le Notaire dispose donc de deux certificats de signature sur sa clé REAL. Le collaborateur dispose quant à lui d'un seul certificat de signature sur sa clé REAL.

Il existe donc trois sous-ensembles de certificat de signature couvert par cette politique de certification :

- le certificat de signature du collaborateur,
- le certificat de signature du Notaire,
- le certificat de signature « authentique » du notaire.

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. [A5]).

- Certificat de signature d'un collaborateur : 1.2.250.1.78.1.1.3.1.3.1.2.1.3.1 ;
- Certificat de signature d'un notaire : 1.2.250.1.78.1.1.3.1.3.1.2.2.3.1 ;
- Certificat de signature « authentique » pour un notaire : 1.2.250.1.78.1.1.3.1.3.1.2.2.4.1

2.3.2. Opérateur de Service de Certification

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

- Fonction 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

2.3.3. Autorité d'enregistrement nationale

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 (sens PRIS v2, [R1]), désignés par :

- mandataire externe lorsque le rôle est rempli au niveau d'un office
- 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.

2.3.4. 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.

2.3.5. 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 ; les notaires sont porteurs de certificats de classe 2.

2.3.6. Utilisateurs de certificats

La présente politique 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 ainsi qu'à leurs collaborateurs, aux notaires des chambres départementales ainsi qu'à leurs collaborateurs, aux notaires des conseils régionaux ainsi qu'à leurs collaborateurs, aux notaires et aux collaborateurs du CSN ou des organismes rattachés.

2.4. Usage des certificats

2.4.1. Domaines d'utilisation applicables

La présente politique de certification traite des bi-clés et des certificats des porteurs identifiés en 2.3.5., afin que ces porteurs puissent signer des actes authentiques dématérialisés (premier sous-ensemble de certificat) ou d'autres types de données (deuxième sous-ensemble de certificat)

La politique traite également de la signature des réponses OCSP.

Les exigences relatives aux bi-clés et certificats d'AC et des composantes sont définies dans la PC relative à l'AC Notaires [A4].

2.4.2. 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.

2.5. Gestion de la PC

2.5.1. Entité gérant la PC

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

2.5.2. Point de contact

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

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

Le CSN est en charge des opérations internes de contrôle de conformité de la DPC à la PC. Ce contrôle de conformité pourra également être réalisé dans le cadre de la procédure de reconnaissance du CSN en tant que prestataire de service de certification électronique qualifié.

2.5.4. 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.

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

3.1. Informations devant être publiées

Les informations publiées sont les suivantes :
- La présente politique de certification ainsi que la politique de certification de l'AC Notaires [A4]
- Les formulaires nécessaires aux porteurs : enregistrement, renouvellement et révocation
- Le document présentant les profils des certificats et CRL [A5]
- La liste des certificats révoqués (CRL) pour les porteurs et l'AC
- Les certificats de l'AC en cours de validité, ainsi que les certificats en cours de validité de l'AC profession règlementée et de l'AC Notaires (hiérarchie à laquelle est rattachée l'AC REAL)
- Les informations permettant aux utilisateurs de s'assurer de l'origine et de l'état des certificats de l'AC profession règlementée (certificats autosignés)

3.2. Entités chargées de la mise à disposition des informations

L'AC est chargée de la mise à disposition de la politique de certification, et des conditions générales d'utilisation.
Ces informations sont accessibles via Internet, sur le site http://www.preuve-electronique.org.

La mise à disposition des informations de gestion des certificats est du ressort de l'OSC. Ces informations sont accessibles sur l'Intranet, au travers de l'annuaire de publication des CRL et ARL par LDAP, et sur Internet, sur le site http://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.

3.3. Délais et fréquences de publication

Les politiques de certification doivent être 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 fréquence de publication des CRL doit être compatible avec un délai maximal de 24 heures entre la prise en compte d'une demande de révocation et sa publication.

3.4. 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 CRL sont accessibles en lecture de manière internationale à toute personne souhaitant en prendre connaissance.

Les ajouts, suppressions et modifications sont limités aux personnes autorisées de l'AC ou de l'OSC, au travers d'un contrôle d'accès fort.

4. Identification et authentification

4.1. Nommage

4.1.1. Types de noms

Les noms utilisés dans un certificat sont décrits selon la norme ISO/IEC 9594 (distinguished names, [A6]), chaque titulaire ayant un nom distinct (DN).

4.1.2. 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

4.1.3. Anonymisation ou pseudonymisation des porteurs

Sans objet

4.1.4. Règles d'interprétation des différentes formes de noms

Les règles d'interprétation sont définies dans le document [A5].

4.1.5. Unicité des noms

Un code distinctif ajouté assure le caractère unique du DN en cas d'homonymie.

4.1.6. 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.

4.2. Validation initiale de l'identité

Le demandeur saisit une demande de création de certificat (par extension de SSCD) en s'adressant à l'OSC qui lui retourne un identifiant de demande. Le demandeur prépare les documents annexes à sa demande au format papier.

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 un formulaire de demande papier complété et signé, une copie d'une pièce d'identité, les documents annexes au format papier remplis et signés, ainsi que son identifiant de demande.

Le valideur vérifie l'identité du demandeur et la conformité des documents. Il valide ensuite la demande de création de carte du demandeur auprès de l'OSC qui lui retourne le code d'activation de son futur SSCD 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 SSCD au demandeur.

Ce processus électronique de validation peut être réalisé par le mandataire, avant le face à face de remise du code d'activation en main propre au demandeur. Dans ce cas, il appartiendra au mandataire d'assurer la sécurité (confidentialité et intégrité) du code d'activation imprimé jusqu'au face à face de remise en main propre 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 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.

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

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

4.2.1. Méthode pour prouver la possession de la clé privée

La clé privée est générée par le SSCD à l'initialisation du support ; la procédure de délivrance du certificat par l'OSC, effectuée lors de l'initialisation du SSCD et décrite dans la DPC, nécessite une preuve de possession de la clé privée.

4.2.2. 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.

4.2.3. Validation de l'identité d'un individu

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.

4.2.3.1. Enregistrement d'un MC externe

L'enregistrement d'un mandataire externe est effectué lors d'un face à face avec un mandataire de la chambre dont dépend l'office employant le mandataire externe. La validation est effectuée sur la base des éléments recensés dans le paragraphe ci-dessus. L'enregistrement comporte également un engagement du mandataire à effectuer correctement les fonctions qui lui sont confiées (contrôle des dossiers des demandeurs de l'office, révocation des certificats). Cet engagement est matérialisé par la signature d'un acte authentique (papier) lors du face à face. Le mandataire externe qui est aussi le chef d'entreprise de son office, s'engage de facto à effectuer correctement les fonctions qui lui sont confiées (contrôle des dossiers des demandeurs de l'office, révocation des certificats) vis-à-vis de ses collaborateurs.

4.2.3.2. 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 responsable de l'organisme auquel le mandataire est rattaché. 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. L'enregistrement comporte également un engagement du mandataire à effectuer correctement les fonctions qui lui sont confiées (contrôle des dossiers des demandeurs de l'office, révocation des certificats). Cet engagement est matérialisé par la signature d'un acte authentique (papier) lors du face à face, reçu par un notaire tiers.

4.2.3.3. Enregistrement d'un porteur avec MC

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

4.2.3.4. Enregistrement d'un porteur sans mandataire

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

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

Le porteur d'une clé notaire de test est 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.

L'enregistrement du porteur est effectué lors d'un face à face avec le mandataire de l'ADSN auquel le porteur est rattaché. La validation est effectuée sur la base des éléments recensés en introduction du paragraphe. Le mandataire validera notamment que le prénom du titulaire est compléter de la mention « - test » permettant d'identifier les porteurs de ce type de clé. L'enregistrement peut comporter également un formulaire de recueil de signature manuscrite et de sceau portant l'indication « test ».

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

Le porteur d'une clé collaborateur de test est 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.

L'enregistrement du porteur est effectué lors d'un face à face avec le mandataire de l'ADSN auquel le porteur est rattaché. La validation est effectuée sur la base des éléments recensés en introduction du paragraphe. Le mandataire validera notamment que le prénom du titulaire est compléter de la mention « - test » permettant d'identifier les porteurs de ce type de clé. L'enregistrement peut comporter également un formulaire de recueil de signature manuscrite et de sceau portant l'indication « test ».

4.2.4. Informations non vérifiées du porteur

Sans objet

4.2.5. 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 4.2.3

4.2.6. 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.

4.2.7. Critères d'interopérabilité

Sans objet

4.3. 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.

L'Autorité de Certification autorise le Titulaire à réaliser un seul renouvellement de sa clé REAL avec validation de sa demande sans face à face par son mandataire de certification (renouvellement courant).
Au renouvellement suivant, le Titulaire devra procéder comme pour une demande initiale (cf. paragraphe 4.2). Il saisira cependant uniquement le n° de titulaire de sa clé actuelle et joindra une copie numérisée du, formulaire papier de demande de clé REAL complété et signé.

4.3.1. Identification et validation pour un renouvellement courant

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

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

Le mandataire doit vérifier que l'impétrant réunit toujours les conditions pour demander une clé REAL pour l'instance et le profil mentionnés dans la demande : la personne travaille effectivement dans l'instance mentionnée en tant que notaire ou collaborateur. Cette vérification est opérée en consultant l'instance dont dépend le demandeur (l'office pour un collaborateur, la chambre pour un notaire de compagnie, la chambre pour les mandataires de certification).

Le mandataire valide alors électroniquement la demande sans face à face en la signant avec son certificat actif. Le code d'activation est généré et l'utilisateur est seul capable de le retirer au moyen de la clé qui lui a permis de signer sa demande.

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

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

4.3.2. Identification et validation pour un renouvellement après révocation

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

4.3.3. Identification et validation pour un renouvellement technique

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 SSCD.

4.4. 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 interne selon les cas. La demande de révocation est effectuée en ligne ; L'identité du demandeur et l'intégrité de la demande sont contrôlées sur la base du certificat d'authentification utilisé pour authentifier la demande.

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

La révocation technique à l'initiative de l'AC suite au renouvellement technique du certificat est effectuée en automatique lors du processus de renouvellement assisté. L'identification du titulaire et la validation de la demande sont contrôlées au moyen des certificats d'authentification et de chiffrement présents sur le SSCD.

5. Exigences opérationnelles sur le cycle de vie des certificats

5.1. Demande de certificat

5.1.1. Origine d'une demande de certificat

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

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

La demande de certificat comporte dans tous les cas :

- Les informations professionnelles : nom, prénom, numéro CRPCEN de l'office ou de l'instance, adresse postale, téléphone, fax, et adresse de messagerie électronique, les fax et adresse postale n'étant pas systématiques.
- Un mot de passe
- Dans le cas d'un collaborateur ne travaillant pas pour un office notarial, un document établissant le rattachement du futur porteur à l'organisme, validé par le responsable (attestation de l'employeur)
- La copie de l'arrêté de nomination ou de la prestation de serment dans le cas d'un notaire
- Un exemplaire de signature manuscrite et de sceau pour les Notaires
- Un exemplaire de signature manuscrite et de cachet pour les clercs habilités.

Pour les demandes initiales, le dossier comporte également un formulaire papier de demande signé par le porteur et numérisé, avec ses annexes.

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

5.2. Traitement d'une demande de certificat

5.2.1. 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.

5.2.2. Acceptation ou rejet de la demande

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

5.2.3. Durée d'établissement du certificat

La durée d'établissement du certificat dépend essentiellement du porteur qui est à l'origine de l'initialisation du SSCD. Une durée limitée, paramétrée par défaut à 3 mois par l'OSC, permet de contrôler le temps octroyé au porteur pour l'initialisation.
Ce délai court à compter de la date de validation par le mandataire de certification.

5.3. Délivrance du certificat

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

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

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

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

5.4. Acceptation du certificat

5.4.1. Démarche d'acceptation du certificat

Le certificat de signature est élaboré en ligne, et transmis lors de la phase d'initialisation du SSCD. Le titulaire peut accepter ou refuser le certificat lors de cette phase d'initialisation. La participation du futur titulaire à cette phase d'initialisation vaut acceptation du certificat.
En cas d'erreur technique lors de la phase d'initialisation du SSCD, le titulaire pourra recommencer cette phase sans émettre de nouvelle demande de certificat, en utilisant les informations de sa demande initiale.

5.4.2. Publication du certificat

Sans objet.

5.4.3. 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.

5.5. Usage de la bi-clé et du certificat

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

Catégorie signature d'acte authentique
L'utilisation de la clé privée par le porteur doit être limitée à la signature des actes authentiques. Cet usage est indiqué explicitement dans les extensions du certificat [A5].

Catégorie signature d'autres types de données
L'utilisation de la clé privée par le porteur doit être 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 [A5].

5.5.2. 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.

5.6. Renouvellement d'un certificat

La notion de renouvellement de certificat, au sens RFC 3647 [A1], correspondante 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.

5.6.1. Causes possibles de renouvellement d'un certificat

Sans objet

5.6.2. Origine d'une demande de renouvellement

Sans objet

5.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet

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

Sans objet

5.6.5. Démarche d'acceptation du nouveau certificat

Sans objet

5.6.6. Publication du nouveau certificat

Sans objet

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

Sans objet

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

5.7.1. Cause possible de changement de bi-clé

Les bi-clés sont renouvelées systématiquement tous les 2 ans. La délivrance d'un nouveau certificat avant la fin de vie ne peut être que la conséquence d'une révocation ou d'un renouvellement technique à l'initiative de l'AC suite à l'évolution de la qualification de l'AC et du gabarit des certificats.

5.7.2. 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 doit procéder comme pour une nouvelle demande de certificat.

Dans le cadre d'un renouvellement technique, la demande est effectuée au travers d'un outil dédié qui automatise le cycle de renouvellement après obtention de l'acceptation du porteur.

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

Dans le cas nominal : l'identité du porteur demandant le renouvellement et sa connaissance des modalités applicables sont validées électroniquement par le mandataire dans le workflow applicatif sans face à face. La demande est préalablement signée électroniquement par le titulaire au moyen de son certificat actuel attestant de la qualité de ce titulaire. La demande doit ensuite être vérifiée puis approuvée (cf. 4.2).

Cf. 5.2.2. pour l'acceptation ou le rejet de la demande, et 5.2.3 pour la durée d'établissement du certificat.

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

Dans le cas nominal : Cf. 5.3 sinon sans objet.

5.7.5. Démarche d'acceptation du nouveau certificat

Cf. 5.4.1

5.7.6. Publication du nouveau certificat

Cf. 5.4.2

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

Cf. 5.4.3.

5.8. Modification du certificat

La modification d'un certificat n'est pas autorisée.

5.8.1. Cause possible de modification d'un certificat

sans objet.

5.8.2. Origine d'une demande de modification de certificat

sans objet.

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

sans objet.

5.8.4. Notification au porteur de l'établissement du certificat modifié

sans objet.

5.8.5. Démarche d'acceptation du certificat modifié

sans objet.

5.8.6. Publication du certificat modifié

Sans objet

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

sans objet.

5.9. Révocation et Suspension des certificats

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

5.9.1. Causes possibles d'une révocation

5.9.1.1. 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
- Destruction, altération du SSCD ou de ses fonctions
- Perte ou vol de support, compromission de clés
- Renouvellement technique

5.9.1.2. Certificat d'une composante de l'IGC

Voir PC Notaires [A4].

5.9.2. Origine d'une demande de révocation

Les personnes pouvant demander une révocation sont les suivantes :
- le porteur au nom duquel le certificat a été émis
- un mandataire interne ou externe pour l'ensemble des porteurs qui lui sont rattachés
- le Président du CSN pour les porteurs qui lui sont rattachés

5.9.3. Procédure de traitement d'une demande de révocation

5.9.3.1. Certificats de porteur

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

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

5.9.3.2. Certificat d'une composante de l'IGC

Voir PC Notaires [A4].

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

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

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

5.9.5.1. Certificats de porteur

Le délai maximum de traitement est de 24 heures.

5.9.5.2. Certificat d'une composante de l'IGC

Voir PC Notaires [A4].

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

Les certificats sont utilisés pour vérifier la signature d'actes authentiques dématérialisés, ou la signature de données. Les utilitaires retenus par la profession doivent rendre cette vérification obligatoire.

L'utilisateur d'un certificat est tenu de vérifier l'état du certificat et des certificats constituant la chaîne de confiance (AC REAL // AC Notaires // AC Professions réglementées). Il doit pour cela s'appuyer sur les CRL publiées régulièrement pour les différentes AC (cf. 5.10.1).

5.9.7. Fréquence d'établissement des CRL

Les CRL doivent être établies et publiées sur l'Intranet toutes les heures, et rendues publiques sur Internet toutes les deux heures.

5.9.8. Délai maximum de publication d'une CRL

Les CRL doivent être rendues publiques et visibles de manière internationale dans un délai maximal de 24 heures.

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

Les systèmes de révocation et de vérification doivent avoir un taux de disponibilité de 99,5 pour cent, et doit être disponible 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 24h.

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

Cf. 5.9.6

5.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet

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

Cf. 5.9.4

5.9.13. Causes possibles d'une suspension

Sans objet

5.9.14. Origine d'une demande de suspension

Sans objet

5.9.15. Procédure de traitement d'une demande de suspension

Sans objet

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

Sans objet

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

5.10.1. Caractéristiques opérationnelles

Les CRL sont au format v2, publiées :

- dans un annuaire LDAP v3 accessible au sein de la communauté notariale : ldap//annuaire.real.notaires.fr:389;
- sur le site internet www.preuve-electronique.org :
  http://www.preuve-electronique.org/ListeRevocations/real.crl
  http://www.preuve-electronique.org/ListeRevocations/real2014.crl
  http://www.preuve-electronique.org/ListeRevocations/real2016.crl
  http://www.preuve-electronique.org/ListeRevocations/real2017.crl

5.10.2. Disponibilité de la fonction

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

5.10.3. Dispositifs optionnels

Sans objet

5.11. 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.

5.12. Séquestre de clé et recouvrement

5.12.1. Politique et pratiques de recouvrement par séquestre de clés

Sans objet

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

Sans objet

6. Mesures de sécurité non techniques

Les exigences présentées dans ce chapitre résultent de l'analyse de risques réalisée sur l'IGC [R2], et de la stratégie de gestion de risques définie par le comité de pilotage pour la composante OSC.

6.1. Mesures de sécurité physique

6.1.1. Situation géographique et construction des sites

La localisation géographique des sites (Venelles et Levallois 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.

6.1.2. Accès physique

L'accès physique aux fonctions de génération des certificats, génération des éléments secrets du porteur et de gestion des révocations, toutes fonctions opérées par l'OSC, doit être strictement limité aux seules personnes nominativement autorisées.
L'accès physique aux composantes de l'IGC supportant ces fonctions doit être limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique ; la définition de ce périmètre contribue à la séparation des rôles entre les différents intervenants.
La traçabilité des accès doit être assurée.
En dehors des heures ouvrables, des mesures de détection d'intrusion physique doivent être mises en œuvre.

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

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

6.1.3. Alimentation électrique et climatisation

Des mesures de secours doivent être mises en œuvre par l'OSC de manière à ce qu'une interruption de service d'alimentation électrique, ou une défaillance de climatisation ne porte 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).

6.1.4. Exposition aux dégâts des eaux

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

6.1.5. Prévention et protection incendie

Les moyens de prévention et de lutte contre l'incendie doivent permettre 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.

6.1.6. Conservation des supports

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

6.1.7. Mise hors service des supports

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

6.1.8. Sauvegarde hors site

Afin de permettre une reprise après incident conforme aux engagements pris par l'AC, l'OSC doit mettre en place des sauvegardes hors site des informations et fonctions critiques. La confidentialité des informations, et l'intégrité des applications sauvegardées doivent être garantie de manière homogène sur le site opérationnel et sur le site de sauvegarde. Cela concerne en particulier les fonctions de gestion des révocations et d'information sur l'état des certificats.

6.2. Mesures de sécurité procédurales

6.2.1. Rôles de confiance

Les rôles de confiance suivants sont définis :

6.2.1.1. 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 relatifs aux mesures correctives, … Le Responsable Sécurité est le DSI, sous le contrôle direct du président du CSN.

6.2.1.2. AEN

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

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

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

6.2.1.3. OSC

Un Comité de Pilotage est mis en place, chargé de l'application opérationnelle de la PC au travers de la mise en œuvre des mesures définies dans la DPC [R3] concernant particulièrement l'OSC. Le Comité de Pilotage fait réaliser les analyses de risques sur le périmètre dont il a la charge, décide de la

stratégie de gestion des risques, valide et suit les plans d'actions correspondants. Il fait réaliser les audits internes sur sa composante, et suit la mise en place des mesures correctives nécessaires.
Le Responsable des Services Généraux est en charge de la définition, la mise en œuvre, la gestion et le suivi des mesures de sécurité physiques.
Le responsable OSC 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 systèmes, réseau et applications.Il est également chargé de la gestion du système de management de la sécurité. Il est enfin responsable des audits internes.

6.2.2. Nombre de personnes requises par tâche

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

6.2.3. 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.

6.2.4. Rôles exigeant une séparation des attributions

Tout rôle de confiance doit être dissocié et séparé de tout autre rôle de confiance.

6.3. Mesures de sécurité vis à vis du personnel

6.3.1. 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 ou contractualisée dans le cas des mandataires.
L'Autorité d'enregistrement et l'OSC s'assurent que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles.
Le personnel d'encadrement de l'AEN et de l'OSC 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.

6.3.2. 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.

6.3.3. 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.

6.3.4. 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.

6.3.5. Fréquence et séquence de rotations entre différentes attributions

Sans objet

6.3.6. 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

6.3.7. 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.

6.3.8. 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.

6.4. Procédures de constitution des données d'audit

6.4.1. Type d'événements à enregistrer

Il est nécessaire d'enregistrer les événements suivants :
- événements systèmes des différentes composantes de l'IGC (démarrage des serveurs, accès réseau, …) que ce soit sur le site actif ou le site de sauvegarde
- événements techniques des applications composant l'IGC, sur le site actif ou le site de sauvegarde
- événements fonctionnels des applications composant l'IGC (demande de carte, validation, révocation, …) sur le site actif ou le site de sauvegarde

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

6.4.2. Fréquence de traitement des journaux d'événements

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

6.4.3. Période de conservation des journaux d'événements

La période de conservation des journaux d'événements doit être :
- D'un mois pour les événements systèmes
- D'un an pour les événements techniques
- De six ans pour les événements fonctionnels

6.4.4. Protection des journaux d'événements

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

6.4.5. Procédure de sauvegarde des journaux d'événements

Les procédures de sauvegarde des journaux sont quotidiennes par delta avec la sauvegarde précédente, et globale de manière hebdomadaire.

6.4.6. Système de collecte des journaux d'événements

Un système de collecte des journaux d'événements doit être mis en place afin de collecter les évènements techniques et fonctionnels afférents au cycle de vie des clés REAL et des certificats délivrés.

6.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement

Sans objet

6.4.8. Evaluation des vulnérabilités

Le contrôle des journaux d'événements système et technique doit être continu et quotidien 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.

6.5. Archivage des données

6.5.1. Types de données à archiver

Les données à archiver sont les suivantes :
- logiciels exécutables et fichiers de configuration
- PC et DPC
- Certificats et CRL publiés
- Engagements signés des mandataires internes et externes
- Dossiers d'enregistrement des porteurs
- Journaux d'événements

6.5.2. Période de conservation des archives

Les dossiers d'enregistrement (demandes de certificats) sont archivés pendant 75 ans [A8], localement, par le mandataire ou le notaire tiers en charge de recevoir l'acte authentique. Passé ce délai, ils seront versés aux archives départementales sans limitation de durée.
Les copies numérisées des actes de face à face sont archivées pendant 6 ans.
Les certificats et CRL sont archivés pendant 6 ans
Les journaux d'événements sont archivés pendant 6 ans

6.5.3. Protection des archives

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

6.5.4. Procédure de sauvegarde des archives

Les archives sont sauvegardées de manière sécurisée.

6.5.5. Exigences d'horodatage des données

L'horodatage des données des événements journalisés doit être synchrone en dehors des opérations hors ligne. Pour cela, les composants de l'IGC doivent être synchronisés sur un même serveur synchronisé avec l'heure universelle.

6.5.6. Système de collecte des archives

Sans objet.

6.5.7. Procédure de récupération et de vérification des archives

La récupération et la vérification des archives doivent pouvoir être effectuées dans un délai conforme à l'utilisation des certificats délivrés – signature d'actes authentiques ou signature d'autres types de données. Un délai d'une semaine est acceptable par la profession.

6.6. Changement de clés d'AC

La durée de vie des clés d'AC est de 4 ans. La durée de vie des certificats est de 2 ans.

6.7. Reprise suite à compromission et sinistre

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

Des procédures et des moyens de remontée et de traitement des incidents (sensibilisation, formation des personnels, et analyse des différents journaux d'événements) doivent être mis en œuvre.
Un incident majeur – perte, suspicion de compromission, compromission ou vol de clé privée de gestion des certificats par exemple – doit être immédiatement signalé à l'AC. La publication de révocation du certificat, si elle s'avère nécessaire, doit être effectuée dans la plus grande urgence par tout moyen nécessaire.

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

Un plan de continuité doit être mis en place 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.

6.7.3. 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 et le cas échéant, la régénération d'une nouvelle clé d'AC et des certificats des porteurs en suivant la pyramide des responsabilités.

6.7.4. Capacité de continuité d'activité suite à un sinistre

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
Accèssibilité des locaux	**Oui**	**Partiellement (sauf production des clés REAL et Hotline)**
Pandémie	Oui	Oui
Empêchement du président	Oui	N/A

L'autorité de certification et l'opérateur de service de certification disposent tous les deux d'un site de repli différent pour leurs activités.

REAL.NOT dispose d'une procédure de gestion de crise qui implique le CSN quand cela est nécessaire.
Le CSN ne dispose par 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.

6.7.5. Actions à mener en cas de compromission d'un algorithme ou d'un paramètre associé

Ce paragraphe traite 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 des éléments sus mentionnés, 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 ;

- 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.

6.8. Fin de vie de l'IGC

6.8.1. Transfert d'activité ou cessation d'activité affectant l'OSC

L'archivage des dossiers d'enregistrement, des certificats des porteurs et des informations relatives aux certificats mis en œuvre doit permettre de garantir un niveau de confiance constant en cas de transfert d'activité de l'OSC.

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

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

1. La clé privée d'émission des certificats ne sera transmise en aucun cas
2. Toutes mesures nécessaires seront prises pour la détruire ou la rendre inopérante
3. Le certificat d'AC sera révoqué

4. Tous les certificats émis encore en cours de validité seront révoqués
5. Tous les mandataires et porteurs de certificats révoqués ou à révoquer seront tenus informés.

7. Mesures de sécurité techniques

7.1. Génération et installation de bi clés

7.1.1. Génération de bi clé

7.1.1.1. Clés d'AC

Voir PC Notaire [A4].

7.1.1.2. Clés porteurs générées par l'AC

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

7.1.1.3. Clés porteurs générées par le porteur

La génération des bi clés du porteur est effectuée directement dans le SSCD, qui répond aux exigences formulées par la réglementation française.

7.1.2. Transmission de la clé privée à son propriétaire

Sans objet.

7.1.3. Transmission de clé publique à l'AC

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

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

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

7.1.5. Tailles des clés

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

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

Cf document profils [A5].

7.1.7. Objectifs d'usages de la clé

L'utilisation de la clé privée d'AC et du certificat associé est limitée à la signature de certificats et de CRL, comme définie dans le document description des certificats et des CRL [A5]. La clé privée d'AC n'est utilisée que dans un environnement sécurisé.
Bi-clés et certificats « actes authentiques »
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 CRL [A5].

Bi-clés et certificats de signature des autres types de données
L'utilisation de la clé privée du porteur et du certificat de la catégorie est limitée à la signature de données à l'exclusion des actes authentiques, comme définie dans le document description des certificats et des CRL [A5].

7.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

7.2.1. Standards et mesures de sécurité pour les modules cryptographiques

7.2.1.1. Module cryptographique de l'AC

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

7.2.1.2. Module cryptographique des porteurs

Les dispositifs de création de signature mis à la disposition des porteurs doivent être évalués EAL 4+.

7.2.2. 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 doit y avoir un contrôle de la clé privée de l'AC par au moins deux personnes.

7.2.3. Séquestre de la clé privée

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

7.2.4. 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 doivent faire l'objet de copie de secours par l'AC.

7.2.5. Archivage de la clé privée

Ni les clés privées d'AC ni les clés privées de porteurs ne font l'objet d'archivage.

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

Le transfert de la clé privée de l'AC vers ou depuis le module cryptologique doit être réalisé par au moins 2 personnes.

7.2.7. Stockage de la clé privée dans le module cryptographique

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

7.2.8. Méthode d'activation de la clé privée

La clé privée est activée à l'aide d'un code PIN.

7.2.9. Méthode de désactivation de la clé privée

La clé privée est désactivée à partir du module cryptographique.

7.2.10. Méthode de destruction des clés privées

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

7.2.11. Niveau d'évaluation sécurité du module cryptographique

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

7.3. Autres aspects de la gestion des bi clés

7.3.1. 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.

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

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

7.4. Données d'activation

7.4.1. Génération et installation des données d'activation

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

Voir PC Notaire [A4].

7.4.1.2. 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 SSCD par le porteur lui-même.

7.4.2. Protection des données d'activation

Seul le document remis par le mandataire au porteur lors du face à face de validation de la demande initiale doit contenir les éléments d'activation du SSCD.

Dans le cas d'un renouvellement, les données d'activation du SSCD sont retirées seulement par le demandeur au moyen de sa clé active.

7.4.3. Autres aspects liés aux données d'activation

Sans objet.

7.5. Mesures de sécurité des systèmes informatiques

7.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

7.5.1.1. Identification et authentification

Les systèmes, applications et bases de données doivent identifier et authentifier et de façon unique les utilisateurs. Toute interaction entre le système et un utilisateur ne doit être possible qu'après une identification et une authentification réussies. Pour chaque interaction, le système doit pouvoir établir l'identité de l'entité.
Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles par des utilisateurs autorisés.

7.5.1.2. Contrôle d'accès

Les profils et droits d'accès aux équipements du PSCE doivent être définis et documentés, ainsi que les procédures d'enregistrement et de désenregistrement des utilisateurs.
Les systèmes [Applications et bases de données] doivent pouvoir distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. Il doit être 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 doit pas pouvoir accorder ou retirer des droits d'accès à un objet. De même, seuls des utilisateurs autorisés doivent pouvoir introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.

Les supports utilisés par les intervenants autorisés de l'OSC doivent être manipulés conformément aux exigences du plan de classification

7.5.1.3. Administration et exploitation

L'utilisation de programmes utilitaires doit être restreinte et contrôlée.
Les procédures opérationnelles d'administration et exploitation de l'IGC doivent être documentées, suivies et régulièrement mises à jour.
Les conditions de mise en service (paramétrage initial de sécurité des serveurs) doivent être documentées.
Les conditions de fin de vie (destruction et mise au rebus) des équipements doivent être documentés afin de garantir la non divulgation des informations sensibles qu'ils peuvent détenir.
L'ensemble des matériels sensibles de l'IGC doit faire l'objet de procédure de maintenance afin de garantir la disponibilité des fonctions et des informations. Les procédures doivent être documentées.
Les personnels concernés par ces procédures doivent être désignés.
Des mesures de contrôles des actions de maintenance doivent être mises en application.

7.5.1.4. Intégrité des composantes

Des mesures de maîtrise de détection et de prévention doivent être mises en œuvre sur l'ensemble des composants du PSCE afin de fournir une protection contre les logiciels malveillants.
Les composantes du réseau local (OSC) sont maintenues dans un environnement physiquement sécurisé ; des vérifications périodiques de conformité de leur configuration sont effectuées.

7.5.1.5. 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.

7.5.1.6. Journalisation et audit

Un suivi d'activité est possible au travers des journaux d'événements.

7.5.1.7. Supervision et contrôle

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

7.5.1.8. Sensibilisation

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

7.5.1.9. Exigences spécifiques au SSCD

La préparation du SSCD doit faire l'objet d'un contrôle de sécurité par l'OSC
Le stockage et la diffusion du SSCD doivent être sécurisés
Les désactivations et réactivations du SSCD doivent faire l'objet d'un contrôle de sécurité
Les données d'activation doivent être établies de façon sécurisées et diffusées séparément du SSCD

7.5.2. Niveau d'évaluation sécurité des systèmes informatiques

7.6. Mesures de sécurité liées au développement des systèmes

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

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

7.6.1. 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 [R4]. 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.

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

Sans objet

7.7. Mesures de sécurité réseau

Les mesures mises en place répondent à l'analyse de risques effectuée sur le système d'information [R2].
Les communications réseau véhiculant des informations confidentielles doivent faire l'objet de mesures de protection contre l'écoute des informations.

Des scans périodiques de détection de vulnérabilités sur les équipements du PSCE accessibles depuis l'Intranet ou l'Internet doivent être conduits.
Des passerelles de sécurité sont mises en place afin de protéger la composant locale du système d'information des accès non autorisés depuis l'Intranet et Internet.

7.8. Horodatage / système de datation

Cf. 6.5.5

8. Profils des certificats, OCSP et des CRL

Les profils des certificats et des CRL sont décrits dans un document propre, intitulé description des certificats et des CRL [A5].

8.1. Profils des certificats

8.1.1. Numéro de version

8.1.2. Extensions de certificat

8.1.3. OID des algorithmes

8.1.4. Forme des noms

8.1.5. Contrainte sur les noms

8.1.6. OID des PC

8.1.7. Utilisation de l'extension contraintes de politique

8.1.8. Sémantique et syntaxe des qualifiants de politique

8.1.9. Sémantiques de traitement des extensions critiques de la PC

8.2. Profil des listes de certificats révoqués

8.2.1. Numéro de version

8.2.2. Extensions de CRL et d'entrées de CRL

8.3. Profil OCSP

Le service OCSP est conforme à la RFC 6277 et la RFC 2560.
Le service est accessible uniquement aux serveurs du système d'informations de REAL.NOT.
Le service ne traite qu'un certificat par demande.

8.3.1. Numéro de version

La demande et la réponse OCSP sont en version 1.

8.3.2. Extensions OCSP

Demande OCSP :
- Il est nécessaire de renseigner le champ RequestorName de la demande OCSP avec le nom de l'application appelante.
- Les condensats fournis dans la demande OCSP doivent être calculés avec l'algorithme SHA256.

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

9. Audit de conformité et autres évaluations

9.1. 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.

9.2. 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.

9.3. 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.

9.4. 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

9.5. 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

9.6. Communication des résultats

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

10. Autres problématiques métiers et légales

10.1. Tarifs

L'AC peut imposer des frais notamment pour :
- L'émission ou le renouvellement d'un SSCD
- La mise à disposition d'un annuaire référençant les certificats
- La mise à disposition des CRL

10.2. Responsabilité financière

10.2.1. Couverture par les assurances

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

10.2.2. Autres ressources

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

10.2.3. Couverture et garantie concernant les entités utilisatrices

Pas d'exigence spécifique.

10.3. Confidentialité des données professionnelles

10.3.1. Périmètre des informations confidentielles

Le CSN (AE) et l'OSC doivent mettre en place un inventaire de tous les biens informationnels et procéder à une classification de manière à définir des exigences de protection en accord avec les besoins.

En particulier, les informations suivantes sont traitées comme confidentielles [R2] :

- La DPC
- Les clés privées de porteurs et d'AC
- Les codes d'initialisation des SSCD
- Les journaux d'événements
- Les dossiers d'enregistrement des porteurs
- Les causes de révocation des certificats

10.3.2. Informations hors du périmètre des informations confidentielles

Sans objet

10.3.3. 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.

10.4. Protection des données personnelles

10.4.1. 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.

10.4.2. Informations à caractère personnel

Les informations à caractère personnel sont les suivantes :

- Les causes de révocation qui restent confidentielles et ne sont pas publiées ; elles ne sont accessibles qu'au porteur, uniquement sur demande écrite et authentifiée auprès de l'autorité de certification. Le porteur peut utiliser le formulaire de demande qui est indexé sur le portail intranet des notaires ou bien adresser une demande datée et signée, sur papier libre, en

mentionnant les éléments d'identification suivants : nom, prénom, adresse postale, n° de titulaire de clé REAL, date de fin de validité de la clé REAL révoquée et n° de CRPCEN de l'instance dont dépend la clé REAL révoquée.

- les informations d'enregistrement.

10.4.3. Informations à caractère non personnel

Pas d'exigence spécifique

10.4.4. Responsabilité en terme de protection des données personnelles

Il est entendu que toute collecte de données à caractère personnel par l'AC est réalisée dans le strict respect des lois et règlements en vigueur, en particulier de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [A7].
L'AC reconnaît avoir procédé aux formalités déclaratives qui leur incombent au titre de la présente PC et des traitements de données à caractère personnel qui seraient réalisés.

10.4.5. Notification et consentement d'utilisation des données personnelles

Le futur porteur a notification d'utilisation des données personnelles [R5], et donne son consentement lors de la phase d'enregistrement. Le porteur peut avoir accès aux informations d'enregistrement.

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

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

10.4.7. Autres circonstances de divulgation d'informations personnelles

Pas d'exigence spécifique.

10.5. 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.

10.6. Interprétations contractuelles et garanties

10.6.1. Autorités de certification

Le CSN est responsable :

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

Le CSN fait son affaire de toute conséquence dommageable résultant du non-respect du présent document par elle-même ou l'une des entités de l'IGC.
Sauf à démontrer qu'il n'a commis aucune faute intentionnelle ou de négligence, le CSN est responsable de tout préjudice causé à toute personne physique ou morale qui s'est fiée raisonnablement aux certificats délivrés dans chacun des cas suivants :

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

Le CSN n'est pas responsable du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation.
Enfin, le CSN engage sa responsabilité en cas de faute ou de négligence dans les précautions à prendre en termes de confidentialité des données personnelles qui lui sont confiées par les porteurs.

10.6.2. Service d'enregistrement

Cf. ci-dessus.

10.6.3. Porteurs de certificats

Le porteur a le devoir de :

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

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

10.6.4. Utilisateurs de certificats

Les utilisateurs des certificats doivent :

- Vérifier l'usage pour lequel le certificat a été émis
- Contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application
- Vérifier la signature du certificat du porteur jusqu'à l'AC profession règlementée et contrôler la validité des certificats

10.6.5. Autres participants

Pas d'exigence particulière

10.7. Limite de garantie

10.8. 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.

10.9. Indemnités

10.10. Durée et fin anticipée de validité de la PC

10.10.1. Durée de validité

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

10.10.2. 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.

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

Sans objet

10.11. Notifications individuelles et communications entre les participants

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

10.12. Amendements à la PC

10.12.1. Procédures d'amendements

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

10.12.2. Mécanisme et période d'information sur les amendements

Pas d'exigence spécifique.

10.12.3. 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.

10.13. 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.

10.14. Juridictions compétentes

La présente Politique de Certification est soumise au droit français.
Tout litige relatif à la validité, l'interprétation, l'exécution de la présente Politique de Certification sera soumise aux tribunaux compétents de la cour d'appel de Paris.

10.15. Conformité aux législations et règlementations

La présente PC est conforme aux exigences énoncées dans les textes législatifs et règlementaires indiqués au chapitre 1.

10.16. Dispositions diverses

10.16.1. Accord global

Pas d'exigence spécifique.

10.16.2. Transfert d'activités

Cf. chapitre 6.8

10.16.3. Conséquences d'une clause non valide

Pas d'exigence spécifique.

10.16.4. Application et renonciation

Pas d'exigence spécifique.

10.16.5. 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.

10.17. Autres dispositions

Sans objet

10.18. Conditions générales d'utilisation

Les conditions générales d'utilisation [R5] 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.

11. Annexe 2 : exigences de sécurité du module cryptographique de l'AC

11.1. Exigences sur les objectifs de sécurité

Le module cryptographique utilisé pour la génération des certificats et des CRL doit répondre aux exigences de sécurité suivantes :

- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et leur destruction sûre en fin de vie
- Etre capable d'identifier et d'authentifier ses utilisateurs
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné
- Etre capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur
- Permettre de créer une signature électronique sécurisée pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance des clés privées
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité
- Si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration
- Détecter les tentatives d'altération physique et entrer dans un état sûr quand une tentative d'altération est détectée

11.2. Exigences sur la certification

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

12. Annexe 3 : exigences de sécurité du dispositif de création de signature

12.1. Exigences sur les objectifs de sécurité

Le SSCD utilisé par le porteur pour stocker et mettre en œuvre sa clé privée, et générer sa bi clé doit répondre aux exigences de sécurité suivante :

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

- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif
-

Le SSCD ne peut pas être débloqué quelque soit la raison de ce blocage (comme par exemple en cas de saisie successive de 3 codes PIN erronés).

12.2. Exigences sur la certification

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

13. Abréviations

AC	**A**utorité de **C**ertification
AEN	**A**utorité d'**E**nregistrement **N**ationale
AFNOR	**A**ssociation **F**rançaise de **N**ormalisation
CRL	Liste de révocation des certificats (**C**ertificate **R**evocation **L**ist)
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
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
SSCD	Dispositif Sécurisé de Création de Signature (**S**ecure **S**ignature **C**reation **D**evice)

14. Glossaire

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

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

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

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

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 sécurisé de création de signature électronique (SSCD)
Matériel ou logiciel, destiné à mettre en application les données de création 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 relatives à l'applicabilité d'un certificat à une communauté et / ou à une classe d'applications ayant des besoins de sécurité communs.

Editions successives

Version / Edition	Date	Emetteur	Valideur	Approbateur
01.01	05/03/2007	JP. Lacombe, Fidens	Comité Stratégique TIC, Y. Thomassier, B. Duquesnoy, A. Barry	D. Lefèvre
01.02	30/05/2007	JP. Lacombe, Fidens	Comité Stratégique TIC, Y. Thomassier, B. Duquesnoy, A. Barry	Membres du bureau CSN
01.03	20/07/2007	Y. Thomassier	Comité Stratégique TIC,	Membres du bureau CSN
01.04	17/03/2008	Y. Thomassier	Comité Stratégique TIC	Membres du bureau CSN
01.05	15/07/2008	Y. Thomassier	Comité Stratégique TIC	Membres du bureau CSN
1.06	01/12/2008	Y.Thomassier	Comité Stratégique TIC	Membres du bureau CSN
1.07	23/09/2009	Y.Thomassier	Comité Stratégique TIC	Membres du bureau CSN
1.08	11/08/2010	Y.Thomassier	Comité Stratégique TIC	Membres du bureau CSN
1.09	01/03/2011	Y.Thomassier	Comité Stratégique TIC	Membres du bureau CSN
1.10	04/07/2011	Y.Thomassier	Comité Stratégique TIC	Membres du bureau CSN
1.11	02/11/2011	Y.Thomassier	Comité Stratégique TIC	Membres du bureau CSN
1.12	Xx/08/2012	Y.Thomassier	Comité Stratégique TIC	Membres du bureau CSN
1.13	07/03/2013	Y.Thomassier	D. Lefèvre	Membres du bureau CSN

1.14	06/06/2013	Y.Thomassier	D. Lefèvre	Membres du bureau CSN
1.15	22/11/2013	Y.Thomassier	D. Lefèvre	Membres du bureau CSN
1.16	27/01/2015	Y.Thomassier	D. Lefèvre	Membres du bureau CSN
1.17	19/06/2015	P.Pellegrin	D. Lefèvre Y.Thomassier	Membres du bureau CSN