CONSEIL SUPÉRIEUR DU NOTARIAT

PC Gestion des certificats émis par l'AC REALTS – Format RFC 3647

Politique de Certification pour les Certificats Techniques émis par l'autorité de certification REALTS

PC REALTS

Statut du document : Standard
Version : 1.6
Date d'approbation : 11/02/2025

PUBLIÉ

60 Bd de La Tour-Maubourg - 75007 Paris
Tél. : 01 44 90 30 00 - notaires.fr

Historique du document

11/02/2025

Version : 1.6, Standard

- Précisions apportées sur la durée de publication et de disponibilités des dernières CRL et jetons OCSP pré-générés (paragraphe 5.8.2)
- Précisions apportées sur la conservation des journaux évènements en cas de cessation d'activité (paragraphe 5.8.1)
- Précisions apportées sur la date d'activation des jetons OCSP pré-générés (paragraphe 5.8.2)
- Précisions apportées sur la durée de publication des certificats et CRL (paragraphe 2.2)

12/03/2024

Version 1.5, Standard

- Modification de la taille des clés RSA
- Nouvelle charte du CSN
- Anonymisation du tableau des éditions successives

18/10/2022

Version 1.4, Standard

- Modification du point de contact
- Rationalisation des dates d'approbation du document
- Précision apportée sur les délais de publication LCR/OCSP
- Modification du délai de récupération d'archives

21/01/2021

Version 1.3, Standard

- §1.1 : Correction des écarts de l'audit eIDAS de janvier 2021. Rajout de la déclaration de conformité au niveau ETSI NCP+
- § 5.7.3 Ajout du délai de reprise effectif du service suite à compromission (14 jours)

29/09/2020

Version : 1.2, Standard

- §3 - Mise à jour du DN des certificats
- §3.2.3 Ajout de « La signature par le RC des CGU REALTS en cours d'application.
- §4.9.9 Précision : taux de disponibilité **annuelle** d'au moins 99,5 pour cent, et ont **une plage de service** 24h/24 et 7j/7
- §5.2.1.3 Remplacement de « un comité de pilotage » par « comité de suivi mensuel de sécurité CSN-ADSN »
- §5.2.1.3 précision : **désigné** par le président du CSN
- §6.2.1 et reste du document : Remplacement EAL4+ par :
  - Le module cryptographique de signature de l'AC est labellisé « Certificat Critères Communs », selon le Schéma de l'ANSSI et les profils de protection reconnus par l'ANSSI.
- §6.6.2 Remplacement de : « revue de processus » par « comité de suivi mensuel de sécurité CSN-ADSN »

16/05/2019

Version : 1.1, Standard

Prise en compte des nouvelles versions des normes ETSI publiées en avril 2018

- 319 401 (V2.2.1) : Electronic Signatures and Infrastructures (ESI) ; General Policy Requirements for Trust Service Providers.
- 319 411-1 (V1.2.2) : Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for Trust Service providers issuing certificates ; Part 1 : General requirements.
- 319 411-2 (V2.2.2) : Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for Trust Service providers issuing certificates ; Part2 : Requirements for trust service providers issuing EU qualified certificates.

- Meilleure prise en compte du RGPD
- Changement REAL.NOT en ADSN

11/08/2017

Version : 0.1, Standard

- Création du document
- Nouvelle chaîne d'AC avec mise en œuvre de l'AC REALTS issue de Notaires de France

Table des matières

1. Introduction

1.1. Présentation générale

Le Conseil Supérieur du Notariat s'est positionné comme prestataire de service de certification électronique à destination des Notaires de France, en offrant des services supports à la signature de manière à permettre aux Notaires d'élaborer des actes authentiques dématérialisés et plus généralement de sécuriser l'ensemble de leurs échanges.

Pour ce faire, une hiérarchie de certification a été mise en place, qui est présentée dans le paragraphe 2.3. La présente politique de certification définit les exigences relatives à l'AC REALTS pour le profil « Certificat d'Horodatage» conformément au profil décrit dans [A12] à des fins d'installation sur les unités d'horodatage du service d'horodatage du notariat. Les certificats émis sont alors utilisés pour signer des demandes de jetons d'horodatage faites par les applications du notariat.

Cette Autorité de Certification répond aux exigences des normes EN 319401 [A8], EN 319411 [A9] et [A10] et EN 319412 [A11] et [A12].

Sa structure est conforme au RFC 3647, [A1]. La couverture des exigences prises par l'AC dans le cadre de cette Politique de Certification permet d'être conforme au règlement eIDAS [A12].

La présente PC est conforme aux exigences définies par la politique ETSI de niveau NCP+ (0.0.2042.1.2).

1.2. Identification du document

Le numéro d'OID du présent document est 1.2.250.1.78.2.1.3.5.1.1.

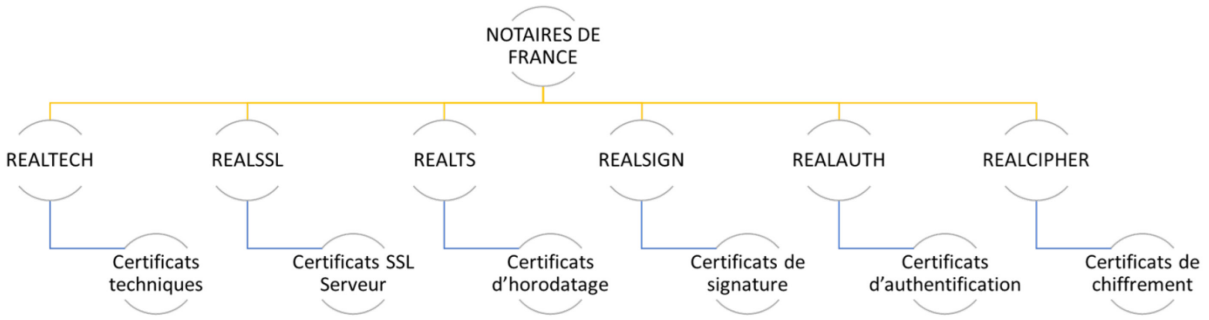
1.3. Entités intervenant dans l'IGC

L'AC REALTS émet des certificats techniques (classe 0) utilisés pour :

- Signer les demandes de certificats des unités d'horodatage du service d'horodatage du notariat;
- Signer les réponses OCSP;

Le premier profil est celui traité dans la présente PC. Il s'agit d'un profil de certificat contenant les extensions nécessaires à l'horodatage.

La hiérarchie d'Autorités de Certification mise en œuvre est la suivante :



Le prestataire de service de certification électronique (PSCE) est le Conseil Supérieur du Notariat. Le CSN est également l'autorité de certification (AC), autorité à laquelle les utilisateurs des services de certification accordent leur confiance pour la création et l'émission des certificats.

Le CSN a recourt à l'ADSN en tant qu'Opérateur de Service de Certification (OSC), pour opérer les fonctions de gestion des certificats.

1.3.1. Autorités de certification

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

L'AC est responsable des certificats signés en son nom et de l'ensemble de l'Infrastructure de Gestion des Clés publiques (IGC) qu'elle a mise en place.

En particulier, l'AC a la responsabilité des fonctions suivantes :
- Mise en application de la Politique de Certification ;
- Gestion des responsables de certificats;
- Gestion des certificats ;
- Publication de la Liste des Certificats Révoqués (LCR) et de la Liste des Autorités Révoquées (LAR) ;
- Journalisation et archivage des événements et informations relatives au fonctionnement de l'IGC.

L'AC assure ces fonctions en déléguant à ADSN les opérations de gestion des certificats des unités d'horodatage et les opérations de maintien en conditions opérationnelles des infrastructures techniques.
Dans tous les cas, l'AC en garde la responsabilité.

1.3.2. Opérateur de Service de Certification

L'opérateur de service de certification est ADSN. Il est en charge des :
- Fonction d'enregistrement
- Fonctions de génération des certificats
- Fonction de remise au responsable du certificat
- Fonction de publication
- Fonction de gestion des révocations
- Fonction d'information sur l'état des certificats

La fonction de génération des éléments secrets de l'unité d'horodatage qui doit recevoir le certificat est opérée par l'OSC directement, durant une cérémonie des clés.

1.3.3. Responsable de certificats (RC)

Le RC est identifié pour les certificats d'horodatage. Il n'y a pas de RC dans le cadre des certificats OCSP.

Le RC dédié aux unités d'horodatage du notariat est un personnel l'ADSN formellement identifié.

Le RC est une personne physique qui est responsable de l'utilisation du certificat et de la clé privée correspondant à ce certificat, pour le compte du CSN qui est identifié dans ce certificat. Le RC a un lien hiérarchique avec l'ADSN Il s'agit nécessairement d'un personnel interne.

Le RC respecte les conditions qui lui incombent définies dans la présente PC. Il est à noter que le certificat étant attaché au service d'horodatage et non au RC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.

L'Autorité d'Horodatage du CSN prévoit en ce sens la procédure de transmission de la responsabilité de RC suivante : après avoir nommé le nouveau RC, l'AH convoque les deux RC et le transfert de responsabilité sur le certificat d'horodatage est formalisé dans un PV.

En tout état de cause, l'AC révoquera le certificat si aucun RC n'est nommé par l'Autorité d'horodatage.

1.3.4. Administrateur de l'IGC

Dans le cas de la délivrance des certificats, l'administrateur de l'IGC assure les phases techniques de saisie, de validation des demandes de génération et de révocation des certificats.

L'Administrateur de l'IGC est responsable de valider que la demande est conforme et que le nom demandé pour l'unité d'horodatage (champ CN du certificat) est libre et conforme au profil des certificats de l'AC REALTS [A4].

1.3.5. Utilisateurs de certificats

Les utilisateurs sont l'ensemble des tierces parties qui font confiance aux certificats émis par l'AC REALTS.

1.3.6. Porteurs de certificats

Il n'y a pas directement de porteurs de certificats dans le cadre de cette Politique de Certification. Il existe néanmoins une personne responsable de la gestion du cycle de vie des certificats, il s'agit du RC (voir 1.3.3).

1.4. Usage des certificats

1.4.1. Domaines d'utilisation applicables

1.4.1.1. Bi-clés et certificats du service d'horodatage

Les certificats de classe 0 émis par l'AC REALTS sont utilisables à des fins de signature de contremarque de temps pour les serveurs d'horodatage du CSN.

1.4.1.2. Bi-clés et certificats d'AC

Le certificat de l'AC REALTS est utilisé pour signer des certificats destinés aux unités d'horodatage du CSN.
L'AC émet également des certificats de signature de réponse OCSP.

Le certificat de l'AC REALTS est également utilisé pour signer les Listes de Certificats Révoqués correspondantes.

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

1.4.2. Domaines d'utilisation interdits

Les certificats de classe 0 ne peuvent pas être utilisés en dehors des usages définis dans le paragraphe 1.4.1.

1.5. Gestion de la PC

1.5.1. Entité gérant la PC

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

1.5.2. Point de contact

Responsable de la Sécurité des Systèmes d'Information (RSSI) du Conseil supérieur du notariat60 Boulevard de la Tour Maubourg
75007 Paris
Tél : 01 44 90 30 00
rssi.csn@notaires.fr

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

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

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

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

1.6. Définitions et acronymes

1.6.1. Acronymes

AC	**A**utorité de **C**ertification
AE	**A**utorité d'**E**nregistrement
AH	**A**utorité d'**H**orodatage
ANSSI	**A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation
C	**C**ountry (Pays)
CEN	**C**omité **E**uropéen de **N**ormalisation
CISSI	**C**ommission **I**nterministérielle pour la **S**écurité des **S**ystèmes d'**I**nformation
CN	**C**ommon **N**ame
CSN	**C**onseil **S**upérieur du **N**otariat
DN	**D**istinguished **N**ame
DPC	**D**éclaration de **P**ratiques de **C**ertification
DSA	**D**igital **S**ignature **A**lgorithm
EE	**E**ntité d'**E**nrôlement
ETSI	Institut européen des normes de télécommunication (**E**uropean **T**elecommunications **S**tandards **I**nstitute)
ICP	**I**nfrastructure à **C**lé **P**ublique
IGC	**I**nfrastructure de **G**estion de **C**lés
LAR	**L**iste des **A**utorités **R**évoquées
LCR	**L**iste des **C**ertificats **R**évoqués
O	**O**rganisation
OC	**O**pérateur de **C**ertification
OCSP	Protocole de vérification de certificat en ligne (**O**nline **C**ertificate **S**tatus **P**rotocol)
OID	Identifiant d'objet (**O**bject **ID**entifier)
OSC	**O**pérateur de **S**ervice de **C**ertification
PC	**P**olitique de **C**ertification
PP	**P**rofil de **P**rotection
PSCE	**P**restataire de **S**ervice de **C**ertification **E**lectronique

RC	**R**esponsable de **C**ertificat
RSA	Rivest Shamir Adelman
S/MIME	**S**ecure/**M**ultipurpose **I**nternet **M**ail **E**xtensions
SHA-256/512	**S**ecure **H**ash **A**lgorithm 256/512
SP	**S**ervice de **P**ublication
SSI	**S**écurité des **S**ystèmes d'**I**nformation
SSL	**S**ecure **S**ockets **L**ayer
TLS	**T**ransport **L**ayer **S**ecurity
URL	**U**niform **R**esource **L**ocator

1.6.2. Définitions

Applications utilisatrices
Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat.

Autorité de certification (AC)
Au sein d'un Prestataire de Service de Certification Electronique (PSCE), une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et le terme d'AC est le seul utilisé.

Autorité d'enregistrement
Cette fonction vérifie et valide les informations d'identification du futur porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du porteur lors du renouvellement du certificat de celui-ci.

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

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 (RSA ou DSA par exemple).

Certificat électronique
Document sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire (personne physique ou service applicatif). Cette attestation prend la forme d'une signature électronique réalisée par un prestataire de service de certification électronique (PSCE). Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Les usages des certificats électroniques régis par le présent document sont la signature électronique et l'horodatage.

Certificat d'AC

Certificat d'une autorité de certification.

Certification d'un prestataire de services de certification électronique
Acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) aux exigences de la PC pour un niveau de sécurité donné et correspondant au service visé par les certificats.

Chaîne de confiance
Ensemble des certificats nécessaires pour valider la généalogie d'un certificat final.
Dans l'architecture la plus simple, la chaîne se compose d'un Certificat d'Autorité de Certification et du certificat final.

Clé privée
Partie secrète d'une bi-clé détenue par son propriétaire. Cette partie de la clé ne doit pas être divulguée.

Clé publique
Partie publique d'une bi-clé mise à la disposition des tierces parties pour pouvoir valider l'utilisation d'un certificat.

Common Name (CN)
Identité réelle ou pseudonyme d'un Porteur, d'un Serveur ou d'une AC.

Composante
Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

Compromission
Divulgation, modification, substitution ou utilisation sans autorisation de données confidentielles (y compris les clés cryptographiques et d'autres paramètres de sécurité fondamentaux).

Déclaration des pratiques de certification (DPC)
Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Distinguished Name (DN)
Nom distinctif X.500 du Porteur, du Serveur ou de l'AC pour lequel le certificat est émis.

Fonction de génération des certificats
Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du porteur ou du responsable du certificat.

Fonction de gestion des révocations
Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction de publication

Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.

Fonction de remise au responsable
Cette fonction remet au responsable du certificat au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif du responsable, clé privée du responsable, codes d'activation,…).

Fonction d'information sur l'état des certificats
Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) ou selon un mode requête / réponse temps réel (OCSP).

HSM (Hardware Security Module)
Boîtier cryptographique matériel dans lequel sont stockées les clés publiques et privées des Autorités de Certification.

Infrastructure de Gestion de Clés (IGC)
Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Liste des Autorités Révoquées (LAR)
Liste contenant les identifiants des certificats d'autorités intermédiaires révoquées ou invalides.

Liste des Certificats Révoqués (LCR)
Liste contenant les identifiants des certificats révoqués ou invalides.

OID
Identificateur numérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.

Personne autorisée
Il s'agit d'une personne autre que le porteur et le mandataire de certification et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

Point de distribution de LCR
Adresse Internet de publication de la Liste des Certificats Révoqués mise à disposition par l'Autorité de Certification.

Politique de certification (PC)
Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs, les responsables de certificats et les utilisateurs de certificats.

Prestataire de services de certification électronique (PSCE)

Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

Produit de sécurité
Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Renouvellement d'un Certificat
Opération effectuée à la demande d'un Porteur ou d'un Responsable de Certificat ou en fin de période de validité d'un Certificat et qui consiste à générer un nouveau Certificat.

Responsable Certificat
La personne physique responsable du certificat, notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le service ou le serveur identifié dans le certificat.

Révocation d'un Certificat
Opération dont le résultat est la suppression de la caution de l'AC sur un Certificat donné, avant la fin de sa période de validité exclusivement.
La demande peut être la conséquence de différents types d'événements tels que la compromission d'une bi-clé, le changement d'informations contenues dans un certificat, etc.
L'opération de révocation est considérée terminée quand le certificat mis en cause est publié dans la Liste des Certificats Révoqués. Le certificat est alors inutilisable.

Système d'information
Tout ensemble de moyen destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives elles-mêmes.

Utilisateur de certificat
Entité ou personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique ou une valeur d'authentification provenant d'un porteur de certificat ou chiffrer des données à destination d'un porteur de certificat.

Validation de certificat
Opération de contrôle du statut d'un Certificat ou d'une chaîne de certification.

Vérification de signature
Opération de contrôle d'une signature numérique.

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

2.1. Entités chargées de la mise à disposition des informations

L'AC est chargée de la mise à disposition de la politique de certification, de la déclaration des pratiques de certification et des conditions générales d'utilisation.

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

La plage d'accès à ce service est de 24h/24 et 7j/7.

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

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

2.2. Informations devant être publiées

Les informations publiées sont les suivantes :

- La présente politique de certification ainsi que la Politique de Certification de l'AC NOTAIRES DE FRANCE [R6]
- La déclaration de pratiques de l'AC REALTS
- Le document présentant les profils des certificats et CRL [R5]
- La liste des certificats révoqués (CRL) pour les pour les porteurs et l'AC , pendant une durée de 7 ans après la date de fin de validité de l'AC
- Les certificats de l'AC REALTS en cours de validité, ainsi que les certificats en cours de validité de l'AC NOTAIRES DE FRANCE (hiérarchie à laquelle est rattachée l'AC REALTS), pendant une durée de 7 ans après la date de fin de validité de l'AC
- Les informations permettant aux utilisateurs de s'assurer de l'origine et de l'état des certificats de l'AC NOTAIRES DE FRANCE (certificats auto signés)

Les documents PC, DPC et CGU sont publiés :

- au format PDF/A
- en français pour la DPC, français et anglais pour la PC et les CGU.

2.3. Délais et fréquences de publication

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

Les certificats d'AC sont diffusés ou mis en ligne préalablement à toute diffusion de certificats, au moment de la cérémonie des clés pour permettre de réaliser la signature des demandes de certificats pour les unités d'horodatage au plus tôt.

La fréquence de publication des LCR est compatible avec un délai maximal de 24 heures entre la prise en compte d'une demande de révocation et sa publication. Les LCR sont publiées toutes les 12h.

2.4. Contrôle d'accès aux informations publiées

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

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

3. Identification et authentification

3.1. Nommage

3.1.1. Types de noms

Les noms utilisés dans un certificat sont décrits selon la norme ISO/IEC 9594 (distinguished names), [A5], chaque titulaire ayant un nom distinct (DN).

3.1.2. Nécessité d'utilisation de noms explicites

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

Les informations portées dans le champ « Subject DN » du certificat sont décrites ci-dessous de manière explicite.
Le nom distinctif dans le cadre d'un certificat d'horodatage contient :

- le nom de l'unité d'horodatage sous la forme CN = [Organisme].[Bureau].UH[n].[date de génération de la bi-clé associée au certificat au format aaaammjjhhmmss] où :
    - [Organisme] correspond au nom de l'organisme détenteur du certificat (ADSN)
    - [Bureau] correspond au nom du bureau responsable du serveur (SDC)
    - [n] est un identifiant numérique de l'UH
    - L'identifiant unique contient la date et l'heure de la demande de génération de certificat auprès de l'AC REALTS.
- Le pays dans lequel est enregistrée l'AC (champ Country) ;
- La raison sociale de l'organisme, tel que figurant au K-Bis (attribut OrganizationName) pour le certificat de l'AC et le certificat de l'UH ;
- Le numéro SIREN du CSN (784350134) précédé de l'ICD 0002, pour remplir le champ OrganizationalUnit Name de l'organisme pour un certificat d'AC et le certificat d'UH.
- Le champ OrganizationIdentifier (2.5.4.97) renseigné comme spécifié dans la clause 5 de EN 319 412-1 [A11], avec le numéro de TVA intracommunautaire (VATFR-67784350134).

Les certificats décrits dans la présente Politique de Certification sont destinés exclusivement à un usage interne du CSN. Il n'est donc pas délivré de certificats de test pour des tierces parties. L'AC ne prévoit pas d'émettre des certificats de tests depuis les environnements de production.

3.1.3. Anonymisation ou pseudonymisation des porteurs

Les certificats objets de la présente PC ne peuvent en aucun cas être anonymes.
Les noms fournis pour l'établissement d'un certificat ne peuvent en aucun cas être des pseudonymes.

3.1.4. Règles d'interprétation des différentes formes de noms

Les règles d'interprétation sont définies dans le document [R6].

Les noms utilisés dans le champ CN (Common Name) des certificats contiennent un identifiant unique qui est établi manuellement lors de la génération du certificat.

Cet identifiant est basé sur un chiffre ainsi que la date et l'heure de génération de la demande.

3.1.5. Unicité des noms

La date de génération ainsi qu'un identifiant assure le caractère unique du CN du certificat d'horodatage.

3.1.6. Identification, authentification et rôle des marques déposées

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

3.2. Validation initiale de l'identité

La validation initiale de l'identité du RC est réalisée par l'huissier avant de débuter la cérémonie de clés. Le RC demande formellement l'autorisation de génération d'un certificat d'UH au CSN par mail. Le mail est annexé au constat de l'huissier.
Le RC est alors présent durant le processus de cérémonie des clés.

3.2.1. Méthode pour prouver la possession de la clé privée

L'AC REALTS reconnait un seul canal pour prouver la possession de la clé privée. Les clés sont générées directement sur l'équipement client.
La preuve de possession de la clé privée est traduite à travers un fichier de demande de certificat qui est transmis à l'AC pour pouvoir générer le certificat correspondant. Cette transmission se fait alors dans des conditions de sécurité optimales.

3.2.2. Validation de l'identité d'un organisme

Voir 3.2.3

3.2.3. Validation de l'identité d'un RC pour l'AC REALTS

3.2.3.1. Enregistrement d'un RC pour un certificat à émettre

La validation de l'identité d'un RC d'un certificat émis par l'AC REALTS est réalisée par l'huissier de justice avant de démarrer la cérémonie de clés.
Le RC doit constituer un dossier de demande contenant :

- Une demande de certificat envoyée par mail, datée de moins de 3 mois, validée par le responsable de l'AH Notaires et comportant le nom de l'unité d'horodatage pour laquelle le certificat doit être émis,

- Un mandat, daté de moins de 3 mois, désignant le futur RC comme étant habilité à être RC pour le service d'horodatage du notariat pour lequel le certificat doit être délivré. Ce mandat est signé par le responsable de l'entité du RC et co-signé, pour acceptation, par le futur RC,

- Un document officiel d'identité en cours de validité du futur RC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté lors de la cérémonie des clés.

- La signature par le RC des CGU REALTS en cours d'application.

L'OSC conserve une trace de la demande à travers un email identifiant l'objet de la demande, les informations à faire apparaître dans le certificat et le point de contact du RC (adresse email) à qui est rattaché le certificat une fois émis. Ces éléments sont joints en annexe du Procès-Verbal d'huissier de la cérémonie des clés.

3.2.3.2. Enregistrement d'un nouveau RC pour un certificat déjà émis

En cas de changement de RC, ADSN désignera sous la responsabilité du responsable de l'AH un nouveau RC. Ce dernier sera notifié formellement de cette responsabilité et constituera un dossier d'enregistrement contenant :

- Un mandat, daté de moins de 3 mois, désignant le futur RC comme étant habilité à être RC pour le service d'horodatage du notariat pour lequel le certificat doit être délivré. Ce mandat est signé par le responsable de l'entité du RC et co-signé, pour acceptation, par le futur RC,
- Un document officiel d'identité en cours de validité du futur RC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- L'adresse email du RC.

Ce dossier sera archivé par l'AC pour conservation des traces.

3.2.4. Informations non vérifiées du RC

Sans objet

3.2.5. Validation de l'autorité du demandeur

Le RC dispose d'un rôle de confiance et est engagé dans ce rôle. L'OSC s'assure pour le compte du CSN de la légitimité du RC.

3.2.6. Critères d'interopérabilité

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

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

Notamment, l'AC REALTS pourra attendre des AC demandant un accord de certification de respecter les formats des certificats suivant la norme [A11], [A12].

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

Un nouveau certificat ne peut pas être fourni au RC sans renouvellement de la bi-clé correspondante.
Le renouvellement se traduit alors par une nouvelle demande de certificat et bénéficie des mêmes procédures que pour une demande initiale (cérémonie de clés).

3.3.1. Identification et validation pour un renouvellement courant

Identique à une demande initiale.

3.3.2. Identification et validation pour un renouvellement après révocation

Identique à une demande initiale.

3.4. Identification et validation d'une demande de révocation

La demande de révocation d'un certificat peut émaner du RC ou bien d'une personne d'autorité au sein de l'organisation de l'AC.
Toute demande de révocation est traitée techniquement par l'administrateur de l'IGC.

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

La demande technique de certificat est faite à l'origine par l'administrateur de l'IGC au travers d'une demande interne tracée d'un RC identifié pour les certificats d'horodatage.

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

La demande de certificats est faite sous la forme d'une demande de certificat au format PKCS#10 intégrant la clé publique générée pour l'unité d'horodatage, qui sera signée par l'AC REALTS. Ce processus de génération technique est encadré dans une cérémonie des clés en présence notamment du RC et sous le contrôle d'un huissier.

4.2. Traitement d'une demande de certificat

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

La demande se fait sous la forme d'une requête au format PKCS#10 qui est opérée par l'administrateur de l'IGC au cours de la cérémonie de clés.
Le dossier de demande est vérifié par l'huissier de justice et le responsable de l'AH avant le traitement technique de la demande de certificat par l'administrateur de l'IGC.

4.2.2. Acceptation ou rejet de la demande

Toutes les demandes de certificat sont acceptées ou rejetées avant la signature de cette demande par l'AC REALTS.
Le rejet de la demande est notifié au RC correspondant. Le motif du rejet est alors précisé au RC.

4.2.3. Durée d'établissement du certificat

La durée d'établissement du certificat est de quelques minutes après la soumission du fichier à l'IGC par l'administrateur de l'IGC (réalisé au cours d'une même cérémonie des clés).

4.3. Délivrance du certificat

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

Le passage à l'état validé de la demande par l'administrateur de l'IGC dans le workflow de l'IGC déclenche le processus automatique de génération du certificat.

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

Le certificat est remis directement au RC identifié.

4.3.3. Durée de vie du certificat

Le certificat d'horodatage a une durée de vie de trois ans.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'OSC accompagne le RC après lui avoir délivré pour procéder aux étapes d'installation et de validation de ce certificat.
Si durant ces étapes, le certificat n'est pas conforme à la demande, il sera alors révoqué et une nouvelle demande devra être opérée à l'image de la demande initiale.

Dans le cas contraire, le certificat est réputé conforme par le RC qui complète et signe un PV d'installation de ce dernier. Ce PV est joint au constat de la cérémonie de clés rédigé par l'huissier.

4.4.2. Publication du certificat

Les certificats émis par l'AC REALTS sont publiés sur le site https://www.preuve-electronique.org.

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

Le RC et le responsable de l'AH constatent ensemble l'installation du certificat sur l'unité d'horodatage. Ceci fait partie du constat de la cérémonie de clés rédigé par l'huissier.

4.5. Usage de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat

La clé privée est utilisée pour signer des contremarques de temps dans le cadre de certificats d'horodatage.
Le certificat et la clé privée correspondante ne peuvent être utilisés que sur l'unité d'horodatage du notariat prévue à cet effet.
Ces usages sont explicitement définis dans les extensions des certificats (champ KeyUsage) [A4].

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

La clé publique et le certificat d'horodatage associé sont utilisés à des fins de validation des signatures des contremarques de temps délivrées par l'unité d'horodatage concernée.

4.6. Renouvellement d'un certificat

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

4.6.1. Causes possibles de renouvellement d'un certificat

Sans objet

4.6.2. Origine d'une demande de renouvellement

Sans objet

4.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet

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

Sans objet

4.6.5. Démarche d'acceptation du nouveau certificat

Sans objet

4.6.6. Publication du nouveau certificat

Sans objet

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

Sans objet

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

4.7.1. Cause possible de changement de bi-clé

Les bi-clés des certificats d'horodatage émis par l'AC REALTS ont une durée d'usage de 1 an. La délivrance d'un nouveau certificat avant la fin de vie ne peut être que la conséquence d'une révocation, ou de la demande de renouvellement au bout d'un an pour garantir la continuité de service.

4.7.2. Origine d'une demande de nouveau certificat

Dans tous les cas, la procédure de demande de nouveau certificat est identique à la procédure de demande initiale et une notification sera transmise au RC par mail pour faire état de l'expiration future de son certificat.

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

Identique à la demande initiale.

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

Identique à la demande initiale.

4.7.5. Démarche d'acceptation du nouveau certificat

Identique à la demande initiale.

4.7.6. Publication du nouveau certificat

Identique à la demande initiale.

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

Identique à la demande initiale.

4.8. Modification du certificat

Les modifications de certificats ne sont pas autorisées.

4.8.1. Cause possible de modification d'un certificat

Sans objet

4.8.2. Origine d'une demande de modification de certificat

Sans objet

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

Sans objet

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

Sans objet

4.8.5. Démarche d'acceptation du certificat modifié

Sans objet

4.8.6. Publication du certificat modifié

Sans objet

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

Sans objet

4.9. Révocation et Suspension des certificats

4.9.1. Causes possibles d'une révocation

4.9.1.1. Certificats d'horodatage

Les causes de révocation sont les suivantes :

- Compromission, suspicion de compromission, perte ou vol de clé privée ;
- Compromission ou suspicion de compromission, dépréciation d'un algorithme ;
- Fin programmée d'utilisation de l'algorithme de condensation mis en œuvre ;
- Le RC n'est plus identifiable ou l'administrateur de la IGC a pris la décision de révoquer son certificat ;
- Cessation de l'activité de l'AC ;
- Décision suite à un échec de contrôle de conformité remonté par l'audit interne ;
- Certificat n'étant plus en conformité avec la PC référencée
- Les algorithmes cryptographiques utilisés ne garantissent plus le lien entre le sujet et la clé publique.
- Révocation de l'AC REALTS.

4.9.1.2. Certificats d'AC

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

4.9.2. Origine d'une demande de révocation

4.9.2.1. Certificats électroniques d'horodatage

Les personnes qui peuvent demander la révocation d'un certificat d'horodatage sont les suivantes :

- Le RC ;
- le Président du CSN pour l'ensemble des certificats émis au nom de l'AC REALTS.

4.9.2.2. Certificats d'AC

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

4.9.3. Procédure de traitement d'une demande de révocation

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

4.9.3.1. Révocation d'un certificat électronique d'horodatage

La demande est transmise par mail par un RC formellement identifié aux exploitants techniques qui la prennent en compte.

4.9.3.2. Certificats d'AC

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

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

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

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

4.9.5.1. Révocation d'un certificat électronique d'horodatage

Le délai maximum de traitement est de 24 heures.

4.9.5.2. Révocation d'un Certificat d'AC

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

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

L'utilisateur d'un certificat est tenu de vérifier l'état des certificats de la chaîne de confiance correspondante (AC NOTAIRES DE FRANCE, AC REALTS).
L'AC REALTS met à disposition des utilisateurs une LCR à jour, publiée sur le site www.preuve-electronique.org ainsi qu'un service OCSP associé.

4.9.7. Fréquence d'établissement des LCR

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

4.9.8. Délai maximum de publication d'une LCR

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

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

Les systèmes de révocation et de vérification ont un taux de disponibilité annuelle d'au moins 99,5 pour cent, et ont une plage de service 24h/24 et 7j/7. En cas de défaillance du système, l'OSC s'engage à rétablir le système sous 24h.

En cas de défaillance en période non ouvrée, la cellule de crise de l'OSC s'activera afin de garantir le rétablissement du système sous 48h.

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

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

Voir 4.9.6

4.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet.

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

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

4.9.13. Causes possibles d'une suspension

La suspension de certificat n'est pas prévue.

4.9.14. Origine d'une demande de suspension

Sans objet

4.9.15. Procédure de traitement d'une demande de suspension

Sans objet

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

Sans objet

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

4.10.1. Caractéristiques opérationnelles

Les LCR sont au format v2, publiées :

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

La LCR contient l'extension « ExpiredCertsOnCRL » et conserve les numéros de série de tous les certificats révoqués, même ceux qui ont expirés.

Un service OCSP conforme à la RFC 6277 et la RFC 2560 est aussi disponible à l'adresse : ocsp.preuve-electronique.org (cf 7).

Le service OCSP met en œuvre l'extension « archive cutoff », comme prévu par la RFC 6960, avec une date identique à la date de début de validité du certificat de l'AC et maintien disponible le statut de révocation du certificat après son expiration.

Si la requête OCSP contient une demande pour un numéro de série non émis par l'AC REALTS, alors le serveur OCSP mettra dans la réponse correspondante le statut « unknow » si l'AC REALTS est toujours valide, et « unauthorized » si cette dernière est expirée.
Le délai de publication de la LCR, de 60 minutes maximum, découle du délai de copie de la LCR de la PKI vers le CRLDP www.preuve-electronique.org. Le service OCSP est un service temps réel, mais qui nécessite une mise à jour opérationnelle de sa base de données de certificats pour prendre en compte le statut de révocation des certificats. En cas de contrôle de statut d'un certificat donnant une réponse différente, le statut du certificat donné par la LCR est à privilégier.

4.10.2. Disponibilité de la fonction

Les fonctions d'informations sur l'état des certificats sont disponibles sur la plage de service : 24 heures sur 24, 7 jours sur 7.

4.10.3. Dispositifs optionnels

Sans objet.

4.11. Fin d'abonnement

Dans le cadre de la présente PC il n'y a pas à proprement parlé d'abonné. Les seuls utilisateurs des certificats sont les unités d'horodatage mise en œuvre dans le service d'horodatage du CSN. En cas d'arrêt d'activité de l'AC ou des services d'horodatages, les certificats correspondants seront alors révoqués.

4.12. Séquestre de clé et recouvrement

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

4.12.1. Politique et pratiques de recouvrement par séquestre de clés

Sans objet

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

Sans objet

5. Mesures de sécurité non techniques

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

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

La localisation géographique des sites ne nécessite pas de mesures particulières face à des risques de type tremblement de terre, explosion, risque volcanique ou crue.

5.1.2. Accès physique

L'accès physique aux fonctions de génération des certificats, génération des éléments secrets du porteur et de gestion des révocations, toutes fonctions opérées par l'OSC, est strictement limité aux seules personnes nominativement autorisées.

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

La traçabilité des accès est assurée.

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

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

5.1.3. Alimentation électrique et climatisation

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

5.1.4. Exposition aux dégâts des eaux

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

5.1.5. Prévention et protection incendie

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

5.1.6. Conservation des supports

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

5.1.7. Mise hors service des supports

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

5.1.8. Sauvegarde hors site

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

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance

Les rôles de confiance suivant sont définis :

5.2.1.1. AC

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

5.2.1.2. AE

Le responsable de l'Autorité d'Enregistrement est le responsable d'application IGC.
Les opérations techniques d'enregistrement et de validation sont prises en charge par ADSN et plus directement par l'administrateur de l'IGC.
Deux rôles sont formalisés dans ce cadre et détenus par l'administrateur de l'IGC:

- L'officier d'enregistrement est en charge de vérifier les informations contenues dans la demande de certificat et de procéder à son approbation

- L'officier de révocation est en charge de traiter les demandes de révocation

5.2.1.3. OSC

Un comité de suivi mensuel de sécurité CSN-ADSN 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.

Les demandes de certificats d'horodatage sont validées au cours de cérémonie de clés qui réunissent :

- Le représentant de l'AC REALTS
- Le représentant de l'AH notaires
- Le responsable de certificat
- Le responsable de sécurité
- Le maître de cérémonie
- L'administrateur de l'IGC
- L'huissier de justice.

Le **Responsable de la sécurité** est en charge de l'implémentation des pratiques de sécurité. Ce rôle est porté par différentes personnes qui ont en charge la sécurité logique ou la sécurité physique. Le RSSI, responsable de la sécurité globale de l'OSC, est désigné par le président de l'ADSN.

L'administrateur système est en charge de l'installation, la configuration et la maintenance des systèmes de confiance de l'IGC.

L'opérateur système est en charge des actions quotidiennes sur l'IGC, notamment les sauvegardes et les restaurations.

L'Auditeur système dispose d'un rôle qui lui permet d'accéder aux traces systèmes des composantes de l'IGC et de les analyser.

Le Responsable d'application IGC est en charge de la définition, la mise en œuvre, la gestion et le suivi des mesures de sécurité logiques au niveau du réseau et de l'application. Pour ce faire, il s'appuie sur les administrateurs système.

L'Administrateur de l'IGC est un chargé d'applications de l'ADSN disposant du rôle de confiance **Administrateur Système**. Il saisit les demandes de certificat sur l'IGC et les valide au cours d'une cérémonie de clés. Il saisit également les demandes de révocation de certificats sous la supervision du responsable de la sécurité.

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

5.2.2. Nombre de personnes requises par tâche

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

5.2.3. Identification et authentification pour chaque rôle

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

Les rôles attribués sont notifiés par écrit aux personnes concernées dans la description de poste.

5.2.4. Rôles exigeant une séparation des attributions

Certains rôles de confiance sont dissociés et séparés de tout autre rôle de confiance. Une liste d'exclusion est maintenue dans [R3]. Une même personne ne peut disposer que d'un seul rôle de confiance.
Un rôle de confiance peut également être porteur d'une part de secret. Un porteur de secrets ne peut détenir qu'une seule part d'un même secret.

5.3. Mesures de sécurité vis à vis du personnel

5.3.1. Qualifications, compétences, et habilitations requises

Tout intervenant amené à occuper un rôle identifié comme sensible est soumis à une clause de confidentialité et de non conflit d'intérêts, gérée par ADSN. En outre les intervenants disposant d'un rôle de confiance attestent sur l'honneur n'avoir commis aucun délit en matière de cybercriminalité.
L'OSC s'assure que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles. Notamment les personnels de l'OSC suivent des formations au moins annuellement sur les menaces informatiques et les pratiques de sécurité du système d'information.

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

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

5.3.2. Procédures de vérification des antécédents

Des procédures de vérification des antécédents sont mises en place pour les personnes appelées à occuper un rôle sensible.

5.3.3. Exigences en matière de formation initiale

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

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

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

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

5.3.5. Fréquence et séquence de rotations entre différentes attributions

Sans objet

5.3.6. Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans le règlement intérieur applicable pour les rôles sensibles tenus par le personnel de l'OSC et de l'AC.

5.3.7. Exigences vis à vis du personnel des prestataires externes

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

5.3.8. Documentation fournie au personnel

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

5.4. Procédures de constitution des données d'audit

5.4.1. Type d'événement à enregistrer

Il est nécessaire d'enregistrer les événements suivants :

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

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

5.4.2. Fréquence de traitement des journaux d'événements

Les journaux d'événements sont exploités :

- De manière quotidienne dans le cadre de processus automatisé de contrôle

- Systématiquement en cas de remontée d'événement anormal

5.4.3. Période de conservation des journaux d'événements

La période de conservation des journaux d'événement est :
- de un mois pour les événements systèmes
- de un an pour les événements techniques
- conforme aux obligations légales pour les événements fonctionnels

5.4.4. Protection des journaux d'événements

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

5.4.5. Procédure de sauvegarde des journaux d'événements

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

5.4.6. Système de collecte des journaux d'événements

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

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

Sans objet

5.4.8. Evaluation des vulnérabilités

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

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

Une revue mensuelle des événements anormaux est réalisée par l'AC à travers un comité de suivi sécurité.

5.5. Archivage des données

5.5.1. Types de données à archiver

Les données à archiver sont les suivantes :
- logiciels exécutables et fichiers de configuration
- PC et DPC et CGU
- Certificats et LCR publiés
- Dossiers d'enregistrement des RC
- Demande de génération des certificats d'horodatage
- Journaux d'événements

5.5.2. Période de conservation des archives

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

Type de données	Période de conservation
Logiciels	Version n – 1
Configurations des logiciels	Version n – 1
Certificats de l'AC REALTS	23 ans
LCR & Certificats clients	23 ans

Requêtes et réponses OCSP	23 ans
Evènements techniques	1 an
Evènements fonctionnels	23 ans
Documentation	10 ans
Dossier d'enregistrement (demandes de certificats)	23 ans
Formulaire d'enregistrement des RC	23 ans

5.5.3. Protection des archives

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

L'OSC met en œuvre les moyens nécessaires pour garantir la conservation des archives sur une période conforme aux exigences légales en matière de fourniture d'éléments de preuves. La durée de conservation et les moyens mis en œuvre sont décrits dans [R3].

5.5.4. Procédure de sauvegarde des archives

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

5.5.5. Exigences d'horodatage des données

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

5.5.6. Système de collecte des archives

Sans objet.

5.5.7. Procédure de récupération et de vérification des archives

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

5.6. Changement de clés d'AC

La durée de vie des clés d'AC REALTS est de 8 ans. La durée de vie des certificats est de 3 ans pour les certificats émis par l'AC REALTS. Les clés de l'AC REALTS devront être renouvelées au plus tard 4 ans moins 1 jour après la génération des clés de l'AC.

5.7. Reprise suite à compromission et sinistre

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

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

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

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

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

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

La compromission d'une clé d'AC entraîne immédiatement la révocation du certificat correspondant. Les cas de compromission des éléments secrets des autres composantes sont traités dans le plan de continuité d'activité.

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

L'AC et plus particulièrement l'OSC se tiennent continuellement informés des cas de compromission des éléments susmentionnés, par le biais d'organismes comme l'ANSSI.

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

Le délai de reprise effectif de l'activité en cas de compromission est de 14 jours.

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

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

5.8. Fin de vie de l'IGC

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

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

Dans le cas où ADSN cesserait son activité d'OSC à la demande du CSN, ADSN déroulera la procédure [R8] et maintiendra la disponibilité de la fonction de vérification de l'état des certificats d'horodatage.

Dans le cas où ADSN transférerait son activité d'OSC à une autre société, à la demande du CSN, l'archivage des journaux d'évènements tel que décrit dans le chapitre 5.4, ainsi que l'archivage des certificats et des informations relatives aux certificats mis en œuvre permettra de garantir un niveau de confiance constant. L'AC organisera alors la reprise des activités d'OSC par un nouvel opérateur [R9].

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

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

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

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

En cas de cessation d'activité de l'AC dans le cas d'un renouvellement de la chaîne d'AC ou dans une cessation totale, le CSN s'engage à gérer le maintien des statuts des certificats de la manière suivante :

- une dernière LCR dont la date d'expiration sera positionnée à la valeur 99991231235959Z
- une dernière réponse OCSP sera pré-générée pour chaque certificat émis et contenant une date de fin de validité positionnée à la valeur 99991231235959Z

Ces éléments sont publiés et disponibles 7 années après la date de fin de validité des AC associées.
Les réponses OCSP pré-générés sont activées pour répondre au plus tard avant la fin de validité du certificat de l'AC REALTS.

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

Dans le cadre de la présente PC, l'AE est assurée directement par l'AC.

6. Mesures de sécurité techniques

6.1. Génération et installation de bi clés

6.1.1. Génération de bi clé

6.1.1.1. Clés de l'AC REALTS

Voir PC AC NOTAIRES DE FRANCE [R6].
Les clés de l'AC REALTS sont générées lors de la cérémonie des clés.

6.1.1.2. Clés porteurs générées par l'AC

Sans objet

6.1.1.3. Clés porteurs générées par le porteur

Les clés sont générées directement sur le HSM de l'unité d'horodatage devant stocker le certificat.

6.1.2. Transmission de la clé privée à son propriétaire

Sans objet

6.1.3. Transmission de clé publique à l'AC

La paire de clé étant générée sur l'équipement devant héberger le certificat, la clé publique est transmise dans un fichier au format PKCS#10.

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

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

6.1.5. Tailles des clés

Les clés de l'AC REALTS ont une taille de 4096 bits.
Les clés des certificats finaux ont une taille de 2048 bits et 3072 bits pour les clés générées après le 01 janvier 2024.

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

Cf. document profils [R5].

6.1.7. Objectifs d'usages de la clé

L'utilisation de la clé privée d'AC et du certificat associé est limitée à la signature de certificats et de LCR, comme définie dans le document description des certificats et des LCR [R5].
La clé privée d'AC n'est utilisée que dans un environnement sécurisé.
Les clés privées des unités d'horodatage sont utilisées exclusivement à des fins de signature de demande de jetons d'horodatage pour les services d'horodatage du CSN.

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

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1. Module cryptographique de l'AC

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

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

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

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

Le module cryptographique de signature de l'AC est labellisé « Certificat Critères Communs », selon le Schéma de l'ANSSI et les profils de protection reconnus par l'ANSSI.

6.2.1.2. Modules cryptographiques des certificats d'horodatage

Les unités d'horodatage possèdent leur propre module cryptographique, identique à ceux de l'AC (labellisés « Certificat Critères Communs », selon le schéma de l'ANSSI et les profils de protection reconnus par l'ANSSI).

6.2.2. Contrôle des clés privées par plusieurs personnes

6.2.2.1. Module cryptographique de l'AC

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

6.2.3. Séquestre de la clé privée

Les clés privées de l'AC et des porteurs ne font pas l'objet de séquestre.
La clé privée des unités d'horodatage ne fait pas l'objet de séquestre.

6.2.4. Copie de secours de la clé privée

La clé privée de l'AC REALTS doit faire l'objet de copie de secours.
Les clés privées des certificats émis par l'AC REALTS ne font pas l'objet de copies de secours.

6.2.5. Archivage de la clé privée

La clé privée de l'AC REALTS fait l'objet d'un archivage.
La clé privée des unités d'horodatage ne font pas l'objet d'archivage.

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

6.2.6.1. Transfert de la clé privée de l'AC

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

6.2.6.2. Transfert de la clé privée d'un certificat d'horodatage

Il n'y a pas de transfert de clé privée.

6.2.7. Stockage de la clé privée dans le module cryptographique

6.2.7.1. Stockage de la clé privée de l'AC

Le stockage de la clé privée de l'AC est réalisé par le module cryptographique dans les conditions de sécurité définies par le profil de protection support à la labellisation « Certificat Critères Communs », selon le schéma de l'ANSSI et les profils de protection reconnus par l'ANSSI.

6.2.7.2. Stockage de la clé privée d'un certificat d'horodatage

Le stockage de la clé privée d'un certificat d'horodatage est réalisé par le module cryptographique dans les conditions de sécurité définies par le profil de protection support à la labellisation « Certificat Critères Communs », selon le schéma de l'ANSSI et les profils de protection reconnus par l'ANSSI.

6.2.8. Méthode d'activation de la clé privée

6.2.8.1. Activation de la clé privée de l'AC

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

6.2.8.2. Activation de la clé privée d'un certificat d'horodatage

L'activation de la clé privée d'un certificat d'horodatage ne peut être effectuée que par les personnes autorisées, et nécessite la présence de deux personnes au moins.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Désactivation de la clé privée de l'AC

La clé privée est désactivée à partir du module cryptographique.

6.2.9.2. Désactivation de la clé privée d'un certificat d'horodatage

La désactivation de la clé privée d'une unité d'horodatage est liée à la désactivation du contexte d'horodatage configuré. Cette désactivation entraîne l'inutilisation ultérieure de la clé privée considérée.

6.2.10. Méthode de destruction des clés privées

6.2.10.1. Destruction de la clé privée de l'AC REALTS

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

6.2.10.2. Destruction de la clé privée d'un certificat d'horodatage

La clé privée est détruite à partir du module cryptographique conformément aux spécifications de l'éditeur de la solution HSM mise en œuvre.

6.2.11. Niveau d'évaluation sécurité du module cryptographique

6.2.11.1. Module cryptographique de l'AC

Les modules cryptographiques de l'AC ont fait l'objet d'une labellisation « Certificat Critères Communs », selon le Schéma de l'ANSSI et les profils de protection reconnus par l'ANSSI.

6.2.11.2. Module cryptographique d'un certificat d'horodatage

Les modules cryptographiques ont fait l'objet d'une labellisation « Certificat Critères Communs », selon le Schéma de l'ANSSI et les profils de protection reconnus par l'ANSSI.

6.3. Autres aspects de la gestion des bi clés

6.3.1. Archivage des clés publiques

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

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

Les clés de signature l'AC REALTS ont une durée de vie de huit ans et les certificats de huit ans.
Les clés de signature des certificats d'horodatage ont une durée d'utilisation de un an et les certificats ont une durée de vie de trois ans.

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

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

Voir PC NOTAIRES DE FRANCE [R6].

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

Sans objet.

6.4.2. Protection des données d'activation

Les données d'activation des clés d'AC ne sont délivrées qu'à la personne autorisée.

6.4.3. Autres aspects liés aux données d'activation

Sans objet.

6.5. Mesures de sécurité des systèmes informatiques

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

6.5.1.1. Identification et authentification

Les systèmes, applications et bases de données identifient et authentifient de façon unique les utilisateurs. Toute interaction entre le système et un utilisateur n'est possible qu'après une identification et une authentification réussies. Pour chaque interaction, le système peut établir l'identité de l'entité.

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

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

6.5.1.2. Contrôle d'accès

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

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

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

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

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

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

6.5.1.3. Administration et exploitation

L'utilisation de programmes utilitaires est restreinte et contrôlée.

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

Les conditions de mise en service (paramétrage initial de sécurité des serveurs) sont documentées. Les configurations mises en œuvre permettent de renforcer le niveau de sécurité des systèmes en appliquant des mesures de durcissement. Les mesures sont décrites dans la DPC [R3].

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

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

Les personnels concernés par ces procédures sont désignés formellement.

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

6.5.1.4. Intégrité des composantes

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

Les composantes du réseau local (OSC) sont maintenues dans un environnement physiquement sécurisé ; des vérifications périodiques de conformité de leur configuration sont effectuées.

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

6.5.1.5. Sécurité des flux

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

6.5.1.6. Journalisation et audit

Un suivi d'activité est possible au travers des journaux d'événements. Tous les événements liés à la sécurité des systèmes sont journalisés. Le détail des événements concernés sont décrits dans la DPC [R3].

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

6.5.1.7. Supervision et contrôle

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

6.5.1.8. Sensibilisation

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

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

6.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Sans objet.

6.6. Mesures de sécurité liées au développement des systèmes

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

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

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

6.6.1. Mesures liées à la gestion de la sécurité

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

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

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

Des comités de suivi sécurité mensuel CSN-ADSN permettent de s'assurer du maintien du niveau de sécurité et des améliorations à apporter.

6.7. Mesures de sécurité réseau

Les mesures mises en place répondent à l'analyse de risques effectuée sur le système d'information [R1].

Les communications réseau véhiculant des informations confidentielles font l'objet de mesures de protection contre l'écoute des informations. Les composants réseaux correspondants sont hébergés dans un environnement sûr.

Des scans périodiques de détection de vulnérabilités sur les équipements du PSCE accessibles depuis l'Intranet ou l'Internet sont conduits.

Des passerelles de sécurité sont mises en place afin de protéger la composant locale du système d'information des accès non autorisés depuis l'Intranet et Internet.

La redondance des accès sur les services du PSCE exposés sur Internet est assurée.

6.8. Horodatage / système de datation

Cf. 5.5.5.

7. Profils des certificats, OCSP et des CRL

Les profils des certificats et des LCR sont décrits dans un document propre, intitulé description des certificats et des LCR [A4].
Ce document est publié par ADSN sur son site et sur le site https://www.preuve-electronique.org.

7.1. Profils des certificats

7.1.1. Numéro de version

7.1.2. Extensions de certificat

7.1.3. OID des algorithmes

7.1.4. Forme des noms

7.1.5. Contrainte sur les noms

7.1.6. OID des PC

7.1.7. Utilisation de l'extension contraintes de politique

7.1.8. Sémantique et syntaxe des qualifiants de politique

7.1.9. Sémantiques de traitement des extensions critiques de la PC

7.2. Profil des listes de certificats révoqués

7.2.1. Numéro de version

7.2.2. Extensions de CRL et d'entrées de CRL

7.3. Profil OCSP

Le service OCSP est conforme à la RFC 6277 et la RFC 2560.
Le service est accessible aux serveurs du système d'informations de l'ADSN et sur Internet.

7.3.1. Numéro de version

La demande et la réponse OCSP sont en version 1.

7.3.2. Extensions OCSP

Demande OCSP :

- 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 ou SHA512 en fonction du contenu de la demande.

Réponse OCSP :

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

8. Audit de conformité et autres évaluations

8.1. Fréquences et / ou circonstances des évaluations

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

8.2. Identités : qualification des évaluateurs

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

8.3. Relations entre évaluateurs et entités évaluées

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

8.4. Périmètre des évaluations

Le contrôleur procède de manière régulière à des contrôles de conformité de la mise en œuvre :

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

8.5. Actions prises suite aux conclusions des évaluations

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

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

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

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

8.6. Communication des résultats

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

9. Autres problématiques métiers et légales

9.1. Tarifs

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

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

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

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

9.2.2. Autres ressources

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

9.2.3. Couverture et garantie concernant les entités utilisatrices

Pas d'exigence spécifique.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Le CSN et l'OSC mettent en place un inventaire de tous les biens informationnels et procéder à une classification de manière à définir des exigences de protection en accord avec les besoins.
En particulier, les informations suivantes sont traitées comme confidentielles :
- Les clés privées de porteurs et d'AC
- Les données d'activation
- Les journaux d'événements
- Les dossiers d'enregistrement des RC

9.3.2. Informations hors du périmètre des informations confidentielles

Sans objet

9.3.3. Responsabilités en terme de protection des informations confidentielles

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

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

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

9.4.2. Informations à caractère personnel

Les données personnelles sont les données personnelles collectées concernant le RC (aucune donnée personnelle dans les certificats horodatage). Il s'agit du dossier RC d'engagement et de demande de délivrance / renouvellement / révocation des certificats (y compris copie des pièces d'identité et causes de révocation), et des données d'accès

physique (badge) aux locaux / DC d'hébergement des composants de la IGC / d'horodatage et enregistrements vidéos.

9.4.3. Informations à caractère non personnel

Pas d'exigence spécifique.

9.4.4. Responsabilité en terme de protection des données personnelles

Le CSN ou un tiers désigné par lui assure la confidentialité de tout Dossier Demandeur et éventuellement de certains événements conformément à ce qui est stipulé dans la présente PC. Le CSN s'engage à demander le respect de cette confidentialité auprès de toute entité intervenant pour lui ainsi qu'auprès de ses salariés.
Le CSN s'engage à prendre et à maintenir les mesures nécessaires pour assurer la sécurité et la confidentialité de tout dossier de demande et ce, conformément aux dispositions du Règlement (UE) 2016/679 du 27 avril 2016 [A6].
L'exécution et la gestion des Conditions Générales supposent la mise en œuvre d'un traitement de données à caractère personnel auquel le Titulaire consent et dont le CSN est le responsable. Conformément à la réglementation applicable en la matière, le Titulaire est informé que la communication de ses données est obligatoire et nécessaire pour prendre en compte sa demande de certificat, pour assurer sa gestion et son cycle de vie.
En vertu du Règlement (UE) 2016/679 du 27 avril 2016, le titulaire peut accéder aux données le concernant auprès :

- du Responsable de traitement, le Conseil Supérieur du Notariat, Autorité de certification, 60 boulevard de La Tour-Maubourg, 75007 PARIS – Tel : +33 1 44 90 30 00, mail : autorite-certification@notaires.fr
- ou du délégué à la protection des données du CSN, cil-csn@notaires.fr - 95 avenue des logissons, 13107 VENELLES Cedex.

Le cas échéant, le titulaire peut également demander la rectification ou l'effacement des données le concernant, obtenir la limitation du traitement de ces données ou s'y opposer pour motif légitime, hormis les cas où la réglementation ne permet pas l'exercice de ces droits.
Si le titulaire estime, après avoir contacté le Responsable de traitement ou le délégué à la protection des données, que ses droits ne sont pas respectés ou que le traitement n'est pas conforme aux règles sur la protection des données, il peut adresser une réclamation en ligne ou par voie postale auprès d'une autorité de contrôle.

9.4.5. Notification et consentement d'utilisation des données personnelles

Sans Objet

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

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

9.4.7. Autres circonstances de divulgation d'informations personnelles

Pas d'exigence spécifique.

9.5. Droits sur la propriété intellectuelle et industrielle

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

9.6. Interprétations contractuelles et garanties

9.6.1. Autorités de certification

Le CSN est responsable :

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

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

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

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

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

Enfin, le CSN engage sa responsabilité en cas de faute ou de négligence dans les précautions à prendre en termes de confidentialité des données personnelles qui lui sont confiées par les porteurs.

9.6.2. Service d'enregistrement

Cf. ci-dessus

9.6.3. RC

Les responsables de certificats délivrés pour les unités d'horodatage du CSN sont tenus de prendre connaissance, d'accepter la présente Politique de Certification.

9.6.4. Utilisateurs de certificats

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

- Que le numéro de série du certificat concerné n'était pas présent dans la LCR applicable

- Que le certificat utilisé était bien émis par la chaîne de certification applicable.

9.6.5. Autres participants

Pas d'exigence particulière

9.7. Limite de responsabilité

Le CSN décline en particulier sa responsabilité pour tout dommage résultant d'un emploi des bi-clés 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 les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le responsable du certificat.

9.8. Indemnités

Sans objet.

9.9. Durée et fin anticipée de validité de la PC

9.9.1. Durée de validité

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

9.9.2. Fin anticipée de validité

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

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

Sans objet

9.10. Notifications individuelles et communications entre les participants

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

9.11. Amendements à la PC

9.11.1. Procédures d'amendements

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

9.11.2. Mécanisme et période d'information sur les amendements

Pas d'exigence spécifique.

9.11.3. Circonstances selon lesquelles l'OID doit être changé

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

9.11.4. Informations aux utilisateurs

Toute nouvelle version de la présente Politique de Certification fera l'objet d'une information sur le site https://www.preuve-electronique.org à destination des porteurs et des applications utilisatrices.

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

9.12. Dispositions concernant la résolution de conflits

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

9.13. Juridictions compétentes

La présente Politique de Certification est soumise au droit français.

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

9.14. Conformité aux législations et réglementations

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

9.15. Dispositions diverses

9.15.1. Accord global

Pas d'exigence spécifique

9.15.2. Transfert d'activités

Cf. chapitre 5.8

9.15.3. Conséquences d'une clause non valide

Pas d'exigence spécifique

9.15.4. Application et renonciation

Pas d'exigence spécifique

9.15.5. Force majeure

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

9.16. Autres dispositions

Sans objet.

9.17. Conditions générales d'utilisation

Sans objet.

10. Documents associés

10.1. 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]	Règlement Européen eIDAS 910/2014
[A4]	Infrastructure de Certification Notariale. Description des certificats et des CRL
[A5]	ISO/IEC 9594. Distinguished name
[A6]	Règlement (UE) 2016/679 du 27 avril 2016
[A7]	LOI n° 2008-696 du 15 juillet 2008 relative aux archives
[A8]	EN 319401 « General Policy Requirements for Trust Service Providers »
[A9]	EN 319411-1 « General requirements »
[A10]	EN 319411-2 « Requirements for trust service »
[A11]	EN 319412-1 « Overview and common data structures »
[A12]	EN 319412-3 « Certificate profile for certificates issued to legal persons »

10.2. Documents de référence

[R1]	Analyse de risques
[R2]	Gestion de la continuité d'activité informatique
[R3]	Déclaration des Pratiques de Certification de l'AC REALTS
[R5]	Description des certificats et CRL de la chaine d'AC Notaires De France
[R6]	Politique de Certification de l'AC NOTAIRES DE FRANCE
[R8]	Cesser l'activité d'opérateur de service de confiance
[R9]	Transfert des activités OSC

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

11.1. Exigences sur les objectifs de sécurité

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

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

11.2. Exigences sur la certification

Le module est certifié conformément aux exigences ci-dessus, et avoir fait l'objet d'une labellisation « Certificat Critères Communs », selon le Schéma de l'ANSSI et les profils de protection reconnus par l'ANSSI.

12. Editions successives

Version / Edition	Date	Emetteur	Approbateur
0.1	11/08/2017	ADSN	Membres du bureau CSN
1.1	16/05/2019	ADSN	Membres du bureau CSN
1.2	29/09/2020	ADSN	Membres du bureau CSN
1.3	21/01/2021	ADSN	Membres du bureau CSN
1.4	18/10/2022	ADSN	Membres du bureau CSN
1.5	12/03/2024	ADSN	Membres du bureau CSN
1.6	11/02/2025	ADSN	Membres du bureau CSN