CONSEIL SUPÉRIEUR DU NOTARIAT

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

Politique de Certification Pour les Certificats de classe 0 et 4 émis par l'autorité de certification Notaires

PC Notaires

Référence du document : OBJ/PC/ACN/000101
Statut du document : Standard
Version : 01.08
Date : 16/03/2015

PUBLIÉ

Historique du document

16/03/2015

Version : 1.08, Standard

Intégration de l'AC REALTS

27/01/2015

Version : 1.07, Standard

Mention de l'OCSP

12/03/2013

Version : 1.06, Standard

Remplacement d'APPLI.NOT par REAL.NOT

11/08/2010

Version : 1.05, Standard

Ajout des adresses des points de distribution internet des CRL et ARL ;
Complément du paragraphe 5.9.9, concernant le délai de rétablissement du système de vérification de l'état des certificats en cas de défaillance ;
Ajout du paragraphe 6.7.5 concernant la compromission d'un algorithme ou d'un paramètre.

07/12/2009

Version : 1.04, Standard

Mise à jour suite à la migration de l'IGC sur Opentrust-PKI

30/05/2007

Version : 01.03, Préliminaire

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

Modifications mineures

26/03/2007

Version : 01.02, Draft

Mise à jour suite aux revues et commentaires suivants :
- Revue formelle du 23 mars 2007 au CSN
- Commentaires transmis par REAL.NOT semaine 11

05/03/2007

Version : 01.01, Draft

Création du document

Table des matières

1. Documents associés

1.1. Documents applicables

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

[A2] AFNOR AC Z74-400. Exigences concernant la politique mise en œuvre par les autorités de certification délivrant des certificats qualifiés

[A3] ISO/IEC 9594. Distinguished name

[A4] Infrastructure de Certification Notariale. Description des certificats et des CRL

1.2. Documents de référence

[R1] Analyse de risques sur l'infrastructure de gestion de clés d'REAL.NOT

[R2] Plan de reprise d'activité

2. Introduction

2.1. 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 1.3. La présente politique de certification définit les exigences relatives à l'AC Notaires.

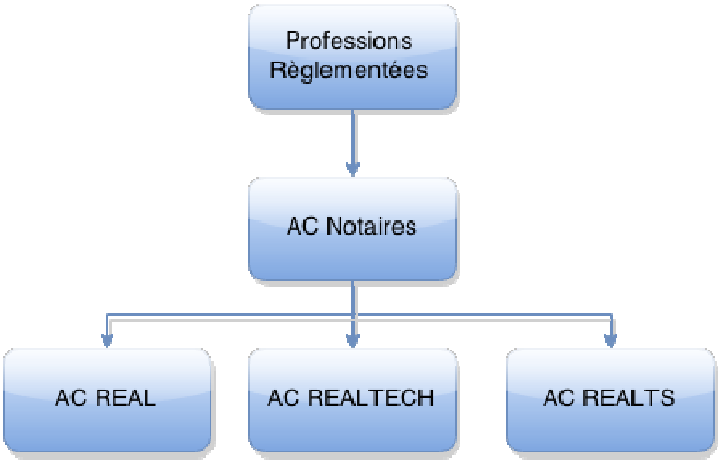
Sa structure est conforme au RFC 3647, [A1].

2.2. Identification du document

Le numéro d'OID du présent document est 1.2.250.1.78.1.1.3.1.1.5

2.3. Entités intervenant dans l'IGC

Les certificats des Notaires et de leurs collaborateurs sont générés par la composante dite AC-REAL, dont les certificats de signature sont eux même générés par la composante AC Notaires. Cette dernière composante est rattachée à l'AC Racine dédiée aux professions réglementées. L'ensemble constitue une hiérarchie de certification présentée dans le schéma ci-dessous. La présente politique de certification définit les exigences relatives à l'AC Notaires.
L'AC Notaires gère des certificats de classe 4 pour la signature des clés publiques de l'AC REAL.
Les certificats techniques (classe 0) sont émis par l'AC REALTECH.
Les certificats d'horodatage (classe 0) sont émis par l'AC REALTS



Le prestataire de service de certification électronique (PSCE) est le Conseil Supérieur du Notariat. Le CSN est également l'autorité de certification (AC) au sens de la norme AFNOR AC Z74-400 [A2], autorité à laquelle les utilisateurs des services de certification accordent leur confiance pour la création et l'émission des certificats.

Le CSN a recourt à REAL.NOT en tant qu'Opérateur de Service de Certification (OSC), pour opérer les fonctions de gestion des certificats.

2.3.1. Autorités de certification

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

2.3.2. Opérateur de Service de Certification

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

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

2.3.3. Autorité d'enregistrement

Sans objet.

2.3.4. Mandataires de certification

Sans objet

2.3.5. Porteurs de certificats

Il n'y a pas véritablement de porteurs pour l'AC REAL et pour les AC REALTECH et REALTS, au sens où les bi clés sont générés et stockés sur le HSM, et ne sont pas directement détenus par un titulaire.

2.3.6. Utilisateurs de certificats

Les utilisateurs de certificats sont :

- Les HSM de l'AC REAL
- Les HSM de l'AC REALTECH et de l'AC REALTS.

2.4. Usage des certificats

2.4.1. Domaines d'utilisation applicables

La présente politique de certification traite des bi clés et certificats de classe 4 (AC REAL, AC REALTECH et AC REALTS).
Les certificats de classe 4 sont utilisés pour la signature des certificats et des CRL gérés par les AC REAL, REALTECH et REALTS.
La politique traite également des certificats de classe 1 pour la signature des réponses OCSP.

2.4.2. Domaines d'utilisation interdits

Les certificats de classe 4 ne peuvent pas être utilisés en dehors de la signature des certificats et des CRL de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS.

2.5. Gestion de la PC

2.5.1. Entité gérant la PC

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

2.5.2. Point de contact

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

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

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

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

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

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

3.1. Informations devant être publiées

Les informations publiées sont les suivantes :

- La présente politique de certification
- Le document présentant les profils des certificats et CRL
- La liste des certificats révoqués (CRL) pour les titulaires machines, et l'ARL pour les certificats utilisés par les AC REAL, REALTECH et REALTS.
- Les certificats de l'AC Notaires en cours de validité, ainsi que les certificats en cours de validité de l'AC profession réglementée (hiérarchie à laquelle est rattachée l'AC Notaires)
- Les informations permettant aux utilisateurs de s'assurer de l'origine et de l'état des certificats de l'AC profession réglementée (certificats auto signés)

3.2. Entités chargées de la mise à disposition des informations

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

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

Les politiques de certification doivent être remises à jour et publiées tous les deux ans.
Les certificats d'AC sont diffusés ou mis en ligne préalablement à toute diffusion de certificats, ARL ou CRL, dans un délai de 24 heures.
La fréquence de publication des CRL et ARL doit être compatible avec un délai maximal de 24 heures entre la prise en compte d'une demande de révocation et sa publication. Les CRL et ARL sont publiées toutes les 24h au moins.

3.3. 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, CRL et ARL sont accessibles en lecture de manière internationale à toute personne souhaitant en prendre connaissance sur le site www.preuve-electronique.org.

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

4. Identification et authentification

4.1. Nommage

4.1.1. Types de noms

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

4.1.2. Nécessité d'utilisation de noms explicites

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

4.1.3. Anonymisation ou pseudonymisation des porteurs

Sans objet

4.1.4. Règles d'interprétation des différentes formes de noms

Les règles d'interprétation sont définies dans le document [A4].

4.1.5. Unicité des noms

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

4.1.6. Identification, authentification et rôle des marques déposées

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

4.2. Validation initiale de l'identité

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

4.2.1. Méthode pour prouver la possession de la clé privée

La génération des bi clés est effectuée en central par l'AC Notaires

4.2.2. Validation de l'identité d'un porteur AC REAL

La validation de l'identité d'un porteur AC REAL est effectuée lors de la cérémonie des clés et décrite dans le document de cérémonie des clés.

4.2.3. Informations non vérifiées du porteur

Sans objet

4.2.4. Validation de l'autorité du demandeur

En ce qui concerne le demandeur opérant pour l'AC REAL, il ne peut s'agir que de la personne autorisée à effectuer cette demande ou de son mandataire. Cela doit être validé lors de la cérémonie des clés.

En ce qui concerne l'AC REALTECH et l'AC REALTS, l'administrateur de la PKI est autorisé à effectuer les demandes de certificats lors d'une cérémonie particulière.

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

En ce qui concerne le demandeur opérant pour l'AC REAL ou de son mandataire, un contrôle doit être effectué, et la demande approuvée lors de la cérémonie des clés.
En ce qui concerne l'AC REALTECH et l'AC REALTS, l'administrateur de la PKI est autorisé à valider les demandes de certificats lors d'une cérémonie particulière.

4.2.6. Critères d'interopérabilité

Sans objet

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

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

4.3.1. Identification et validation pour un renouvellement courant

Dans le cas des certificats d'AC REAL, l'identification et validation pour un renouvellement courant sont effectuées lors de la cérémonie des clés.
En ce qui concerne l'AC REALTECH et l'AC REALTS, l'administrateur de la PKI est autorisé à valider les demandes de certificats lors d'une cérémonie particulière.

4.3.2. Identification et validation pour un renouvellement après révocation

En cas de renouvellement après révocation, l'AC REAL, l'AC REALTECH ou l'AC REALTS procède comme pour une demande initiale.

4.4. Identification et validation d'une demande de révocation

La demande de révocation de clé pour l'AC REAL, l'AC REALTECH ou l'AC REALTS ne peut émaner que d'une personne autorisée, et doit être validée formellement avant prise en compte.

5. Exigences opérationnelles sur le cycle de vie des certificats

5.1. Demande de certificat

5.1.1. Origine d'une demande de certificat

Une demande de certificat de l'AC REAL émane de la personne autorisée par l'organisation, présente lors de la cérémonie.
Une demande de certificat de l'AC REALTECH ou de l'AC REALTS émane de l'administrateur de la PKI.

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

L'établissement d'une demande de certificat s'effectue selon une procédure de cérémonie de clés.

5.2. Traitement d'une demande de certificat

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

Pour les certificats de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS, le demandeur est identifié et la demande validée lors de la cérémonie des clés.

5.2.2. Acceptation ou rejet de la demande

Toutes les demandes de certificat d'AC REAL, d'AC REALTECH ou d'AC REALTS sont acceptées lors de la cérémonie de clés.

5.2.3. Durée d'établissement du certificat

Les certificats de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS sont générés et installés lors de la cérémonie.

5.3. Délivrance du certificat

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

La génération des bi clés de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS est consignée lors de la cérémonie des clés.

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

Le demandeur de certificat l'AC REAL, de l'AC REALTECH ou de l'AC REALTS est présent lors de la cérémonie des clés.

5.4. Acceptation du certificat

5.4.1. Démarche d'acceptation du certificat

En ce qui concerne l'AC REAL, le demandeur doit disposer d'un moyen au travers duquel il signifie son acceptation des éléments générés lors de la cérémonie des clés.

5.4.2. Publication du certificat

Les certificats de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS sont publiés sur l'intranet au travers de l'annuaire LDAP de publication des certificats, et sur l'Internet sur le site http://www.preuve-electronique.org.

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

Sans objet

5.5. Usage de la bi-clé et du certificat

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

L'utilisation des clés privées est limitée :

- A l'élaboration des certificats porteurs
- A la signature des CRL

Cet usage est indiqué explicitement dans les extensions des certificats [A4].

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

Pour les certificats de classe 4, l'utilisation de la clé publique et du certificat est limité au contrôle des certificats gérés par l'AC REAL, l'AC REALTECH ou l'AC REALTS, et à la validation des CRL.

5.6. 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 du bi-clé est autorisé.

5.6.1. Causes possibles de renouvellement d'un certificat

Sans objet

5.6.2. Origine d'une demande de renouvellement

Sans objet

5.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet

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

Sans objet

5.6.5. Démarche d'acceptation du nouveau certificat

Sans objet

5.6.6. Publication du nouveau certificat

Sans objet

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

Sans objet

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

5.7.1. Cause possible de changement de bi-clé

Les bi-clés de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS ont une durée de vie de 4 ans. La délivrance d'un nouveau certificat avant la fin de vie ne peut être que la conséquence d'une révocation, ou de la demande de renouvellement au bout de 2 ans pour garantir la continuité de service.

5.7.2. 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.

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

Identique à la demande initiale.

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

Identique à la demande initiale.

5.7.5. Démarche d'acceptation du nouveau certificat

Identique à la demande initiale.

5.7.6. Publication du nouveau certificat

Identique à la demande initiale.

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

Identique à la demande initiale.

5.8. Modification du certificat

Les modifications de certificats ne sont pas autorisées.

5.8.1. Cause possible de modification d'un certificat

Sans objet

5.8.2. Origine d'une demande de modification de certificat

Sans objet

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

Sans objet

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

Sans objet

5.8.5. Démarche d'acceptation du certificat modifié

Sans objet

5.8.6. Publication du certificat modifié

Sans objet

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

Sans objet

5.9. Révocation et Suspension des certificats

5.9.1. Causes possibles d'une révocation

5.9.1.1. Certificats de titulaires machines

Les causes de révocation sont les suivantes :

- Compromission, suspicion de compromission, perte ou vol de clé privée
- Cessation de l'activité de l'AC
- Décision suite à un échec de contrôle de conformité
- Révocation de l'AC Notaires

5.9.2. Origine d'une demande de révocation

Les personnes pouvant demander une révocation de certificat de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS sont le titulaire du certificat, ou le titulaire de l'AC Notaires (autorité du CSN).

5.9.3. Procédure de traitement d'une demande de révocation

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

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

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

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

Le délai maximum de traitement est de 24 heures.

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

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

5.9.7. Fréquence d'établissement des CRL et des ARL

Les CRL et ARL doivent être établies et publiées sur l'Intranet et sur l'Internet une fois par jour.

5.9.8. Délai maximum de publication d'une CRL ou d'une ARL

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

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

Les systèmes de révocation et de vérification doivent avoir un taux de disponibilité de 99,5 pour cent, et doit être disponible sous 24 heures.
En cas de défaillance du système, l'OSC s'engage à rétablir son fonctionnement sous 48h.

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

Cf. 5.9.6

5.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet

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

Cf. 5.9.4

5.9.13. Causes possibles d'une suspension

La suspension de certificat n'est pas prévue.

5.9.14. Origine d'une demande de suspension

Sans objet

5.9.15. Procédure de traitement d'une demande de suspension

Sans objet

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

Sans objet

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

5.10.1. Caractéristiques opérationnelles

Les CRL et ARL sont au format v2, publiées :

- dans un annuaire LDAP v3 accessible au sein de la communauté notariale : ldap//annuaire.real.notaires.fr:389;
- sur le site interne www.preuve-electronique.org sous forme d'une liste :
  http://www.preuve-electronique.org/ListeRevocations/notaires.crl
  http://www.preuve-electronique.org/ListeRevocations/notaires.arl
  http://www.preuve-electronique.org/ListeRevocations/notaires2018.arl

http://www.preuve-electronique.org/ListeRevocations/notaires2020.arl
http://www.preuve-electronique.org/ListeRevocations/notaires2023.arl

5.10.2. Disponibilité de la fonction

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

5.10.3. Dispositifs optionnels

Sans objet

5.11. Séquestre de clé et recouvrement

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

5.11.1. Politique et pratiques de recouvrement par séquestre de clés

Sans objet

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

Sans objet

6. Mesures de sécurité non techniques

Les exigences présentées dans ce chapitre résultent de l'analyse de risques réalisée sur l'IGC [R1], et de la stratégie de gestion de risques définie par le comité de pilotage pour la composante OSC.

6.1. Mesures de sécurité physique

6.1.1. Situation géographique et construction des sites

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

6.1.2. Accès physique

L'accès physique aux fonctions de génération des certificats, génération des éléments secrets du porteur et de gestion des révocations, toutes fonctions opérées par l'OSC, doit être strictement limité aux seules personnes nominativement autorisées.
L'accès physique aux composantes de l'IGC supportant ces fonctions doit être limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique, permettant la séparation des rôles entre les différents intervenants.
La traçabilité des accès doit être assurée.
En dehors des heures ouvrables, des mesures de détection d'intrusion physique doivent être mises en œuvre.
Des mesures de sécurité physique sont également mises en place pour limiter les accès aux supports sensibles (supports de clés, dossier d'enregistrement, DPC, documents d'applications).

6.1.3. Alimentation électrique et climatisation

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

6.1.4. Exposition aux dégâts des eaux

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

6.1.5. Prévention et protection incendie

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

6.1.6. Conservation des supports

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

6.1.7. Mise hors service des supports

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

6.1.8. Sauvegarde hors site

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

6.2. Mesures de sécurité procédurales

6.2.1. Rôles de confiance

Les rôles de confiance suivant sont définis :

6.2.1.1. AC

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

6.2.1.2. AE

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

6.2.1.3. OSC

Un Comité de Pilotage est mis en place, chargé de l'application opérationnelle de la PC au travers de la mise en œuvre des mesures définies dans la DPC concernant particulièrement l'OSC. Le Comité de Pilotage fait réaliser les analyses de risques sur le périmètre dont il a la charge, décide de la stratégie de gestion des risques, valide et suit les plans d'actions correspondants. Il fait réaliser les audits internes sur sa composante, et suit la mise en place des mesures correctives nécessaires.
Le Responsable des Services Généraux est en charge de la définition, la mise en œuvre, la gestion et le suivi des mesures de sécurité physiques.
Le Responsable de l'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 systèmes, réseau et applications.
Le Responsable Qualité est chargé de la gestion du système de management de la sécurité. Il est également responsable des audits internes.

6.2.2. Nombre de personnes requises par tâche

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

6.2.3. Identification et authentification pour chaque rôle

Des mesures d'identification et d'authentification sont mises en place afin de supporter la mise en œuvre de la politique de contrôle d'accès et la traçabilité des opérations ; la politique de contrôle d'accès limite l'accès aux seules personnes autorisées conformément à leur besoin d'en connaître.
Les rôles attribués sont notifiés par écrit aux personnes concernées dans la description de poste.

6.2.4. Rôles exigeant une séparation des attributions

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

6.3. Mesures de sécurité vis à vis du personnel

6.3.1. Qualifications, compétences, et habilitations requises

Tout intervenant amené à occuper un rôle identifié comme sensible est soumis à une clause de confidentialité, gérée par l'employeur.
L'OSC s'assure que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles.
Le personnel d'encadrement possède l'expertise appropriée, et est familier des procédures de sécurité.
Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités (description de poste) et des procédures liées à la sécurité du système et au contrôle du personnel.

6.3.2. Procédures de vérification des antécédents

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

6.3.3. Exigences en matière de formation initiale

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

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

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants.
Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.

6.3.5. Fréquence et séquence de rotations entre différentes attributions

Sans objet

6.3.6. Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans la définition de poste ou la charte de sécurité du personnel pour les rôles sensibles tenus par le personnel de l'OSC et de l'AC.

6.3.7. Exigences vis à vis du personnel des prestataires externes

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

6.3.8. Documentation fournie au personnel

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

6.4. Procédures de constitution des données d'audit

6.4.1. Type d'événement à enregistrer

Il est nécessaire d'enregistrer les événements suivants :

- événements systèmes des différentes composantes de l'IGC (démarrage des serveurs, accès réseau, …) que ce soit sur le site actif ou le site de sauvegarde
- événements techniques des applications composant l'IGC, sur le site actif ou le site de sauvegarde

- événements fonctionnels des applications composant l'IGC (demande de certificats, validation, révocation, …) sur le site actif ou le site de sauvegarde
- opérations effectuées

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

6.4.2. Fréquence de traitement des journaux d'événements

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

6.4.3. Période de conservation des journaux d'événements

La période de conservation des journaux d'événement doit être :

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

6.4.4. Protection des journaux d'événements

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

6.4.5. Procédure de sauvegarde des journaux d'événements

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

6.4.6. Système de collecte des journaux d'événements

Un système de collecte des journaux d'événements doit être mis en place.

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

Sans objet

6.4.8. Evaluation des vulnérabilités

Le contrôle des journaux d'événement système et technique doit être continu et quotidien afin de permettre une anticipation des vulnérabilités, et des remontées d'alerte en cas de vulnérabilités.
Le contrôle des journaux des événements fonctionnels peut être réalisé à la demande en cas de litige, ou pour analyse de comportement de l'IGC.

6.5. Archivage des données

6.5.1. Types de données à archiver

Les données à archiver sont les suivantes :

- logiciels exécutables et fichiers de configuration
- PC et DPC
- Certificats, ARL et CRL publiés
- Formulaires d'enregistrement des titulaires
- Journaux d'événements

6.5.2. 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	10 ans
Configurations des logiciels	10 ans
Certificats de l'AC Notaires	10 ans
CRL & Certificats clients	10 ans
Evènements système	1 mois
Evènements techniques	1 an
Evènements fonctionnels	10 ans
Documentation	10 ans
Dossier d'enregistrement (demandes de certificats)	10 ans

6.5.3. Protection des archives

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

6.5.4. Procédure de sauvegarde des archives

Les archives sont sauvegardées de manière sécurisée, certaines en double enregistrement.

6.5.5. Exigences d'horodatage des données

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

6.5.6. Système de collecte des archives

Sans objet.

6.5.7. Procédure de récupération et de vérification des archives

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

6.6. Changement de clés d'AC

La durée de vie des clés d'AC Notaires est de 8 ans. La durée de vie des certificats est de 4 ans pour les certificats de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS.

6.7. Reprise suite à compromission et sinistre

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

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

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

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

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

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

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

La capacité de continuité de l'activité suite à un sinistre est également traitée dans le plan de reprise d'activité [R2].

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

Ce paragraphe traite de la compromission d'un algorithme ou d'un paramètre associé, tels que l'algorithme de condensat utilisé dans les certificats ou la longueur de la clé des certificats.

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

En cas d'information d'une compromission des éléments sus mentionnés, impactant les certificats des AC ou les certificats clients, l'AC et l'OSC déclenche une cellule de crise afin de déterminer les actions à mener pour rétablir le service au plus tôt ;

Par mesure de précaution, l'AC :

- demande à l'OSC l'arrêt immédiat des services de dématérialisation exploitant la clé REAL ;
- demande à l'OSC de diffuser immédiatement l'information à tous les mandataires et à tous les partenaires par mail.

6.8. Fin de vie de l'IGC

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

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

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

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

1. La clé privée d'émission des certificats ne sera transmise en aucun cas
2. Toutes mesures nécessaires seront prises pour la détruire ou la rendre inopérante
3. Le certificat d'AC sera révoqué
4. Tous les certificats émis encore en cours de validité seront révoqués
5. Tous les mandataires et porteurs de certificats révoqués ou à révoquer seront tenus informés.

7. Mesures de sécurité techniques

7.1. Génération et installation de bi clés

7.1.1. Génération de bi clé

7.1.1.1. Clés de l'AC Notaires

Les clés de l'AC Notaires sont générées lors de la cérémonie des clés, en présence du demandeur, de l'administrateur de l'AC profession réglementée et de l'AC Notaires, du tiers enregistrant la demande et du maître de cérémonie.

7.1.1.2. Clés de l'AC REAL

Les clés de l'AC REAL sont générées lors de la cérémonie des clés, en présence du demandeur, de l'administrateur de l'AC Notaires et de l'AC REAL, du tiers enregistrant la demande et du maître de cérémonie.

7.1.1.3. Clés de l'AC REALTECH et de l'AC REALTS

Les clés de l'AC REALTECH et de l'AC REALTS sont générées lors de la cérémonie des clés, en présence de l'administrateur de la PKI et du maître de cérémonie.

7.1.2. Transmission de la clé privée à son propriétaire

Sans objet

7.1.3. Transmission de clé publique à l'AC

Sans objet, les clés sont générées par l'AC.

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

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

7.1.5. Tailles des clés

2048 bits pour la taille des clés AC

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

Cf. document profils [A4].

7.1.7. Objectifs d'usages de la clé

L'utilisation de la clé privée pour l'AC REAL, l'AC REALTECH ou l'AC REALTS et du certificat associé est limitée à la signature de certificats et de CRL, comme définie dans le document description des certificats et des CRL [A4].
La clé privée d'AC n'est utilisée que dans un environnement sécurisé.
L'utilisation des clés privées des titulaires machines est la sécurisation des flux et des données traitées, en support des fonctions d'authentification, de chiffrement et de signature de données.

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

7.2.1. Standards et mesures de sécurité pour les modules cryptographiques

7.2.1.1. Module cryptographique de l'AC Notaires

Le module cryptographique de l'AC pour la génération et la mise en œuvre des clés de signature doit répondre aux exigences énoncées par la réglementation.
Le module cryptographique de signature de certificat ne doit pas faire l'objet de manipulation non autorisée lors de son transport.
Le module cryptographique de signature de certificat et des informations de révocation ne fait pas l'objet de manipulation non autorisée lors de son stockage
Le module cryptographique de signature de certificat et des informations de révocation fonctionne correctement

7.2.1.2. Module cryptographique de l'AC REAL

Le module cryptographique de signature de l'AC REAL doit être évalué EAL 4+.

7.2.1.3. Module cryptographique des entités machines

Sans objet

7.2.2. Contrôle des clés privées par plusieurs personnes

Il doit y avoir un contrôle de la clé privée de l'AC Notaires par au moins deux personnes.
Il doit y avoir un contrôle de la clé privée de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS par au moins deux personnes.

7.2.3. Séquestre de la clé privée

Les clés privées de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS ne font pas l'objet de séquestre.

7.2.4. Copie de secours de la clé privée

Les clés privées de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS doivent faire l'objet de copie de secours.
Les clés privées de l'AC Notaires doivent faire l'objet de copie de secours.

7.2.5. Archivage de la clé privée

Les clés privées d'AC ne font pas l'objet d'un archivage.

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

7.2.6.1. Transfert de la clé privée de l'AC Notaires

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

7.2.6.2. Transfert de la clé privée de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS

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

7.2.7. Stockage de la clé privée dans le module cryptographique

7.2.7.1. Stockage de la clé privée de l'AC Notaires

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

7.2.7.2. Stockage de la clé privée de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS

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

7.2.8. Méthode d'activation de la clé privée

7.2.8.1. Activation de la clé privée de l'AC Notaires

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

7.2.8.2. Activation de la clé privée de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS

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

7.2.9. Méthode de désactivation de la clé privée

7.2.9.1. Désactivation de la clé privée de l'AC Notaires

La clé privée est désactivée à partir du module cryptographique.

7.2.9.2. Désactivation de la clé privée de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS

La clé privée est désactivée à partir du module cryptographique.

7.2.10. Méthode de destruction des clés privées

7.2.10.1. Destruction de la clé privée de l'AC Notaires

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

7.2.10.2. Destruction de la clé privée de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS

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

7.2.11. Niveau d'évaluation sécurité du module cryptographique

7.2.11.1. Module cryptographique de l'AC Notaires

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

7.2.11.2. Module cryptographique de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS

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

7.3. Autres aspects de la gestion des bi clés

7.3.1. Archivage des clés publiques

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

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

Les clés de signature et les certificats de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS ont une durée de vie de quatre ans
Les clés de signature et les certificats de l'AC Notaires ont une durée de vie de huit ans

7.4. Données d'activation

7.4.1. Génération et installation des données d'activation

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

Les éléments nécessaires à l'activation de la clé privée de l'AC Notaires doivent être générés de manière sécurisée, et uniquement accessibles à la personne autorisée à procéder à cette activation.

7.4.1.2. Génération et installation des données d'activation correspondant à la clé privée de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS

Les éléments nécessaires à l'activation de la clé privée de l'AC REAL, de l'AC REALTECH ou de l'AC REALTS doivent être générés de manière sécurisée, et uniquement accessibles à la personne autorisée à procéder à cette activation.

7.4.2. Protection des données d'activation

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

7.4.3. Autres aspects liés aux données d'activation

Sans objet.

7.5. Mesures de sécurité des systèmes informatiques

7.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

7.5.1.1. Identification et authentification

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

7.5.1.2. Contrôle d'accès

Les profils et droits d'accès aux équipements du PSCE doivent être définis et documentés, ainsi que les procédures d'enregistrement et de désenregistrement des utilisateurs.
Les systèmes [Applications et bases de données] doivent pouvoir distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. Il doit être possible de :

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

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

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

7.5.1.3. Administration et exploitation

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

7.5.1.4. Intégrité des composantes

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

7.5.1.5. Sécurité des flux

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

7.5.1.6. Journalisation et audit

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

7.5.1.7. Supervision et contrôle

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

7.5.1.8. Sensibilisation

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

7.5.2. Niveau d'évaluation sécurité des systèmes informatiques

7.6. Mesures de sécurité liées au développement des systèmes

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

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

7.6.1. Mesures liées à la gestion de la sécurité

L'IGC est suivie dans le cadre de la mise en place du système de management de la sécurité de l'OSC.
Le comité de pilotage gère la remontée d'information vers l'AC qui est averti de toute modification significative.
Les évolutions des composantes font l'objet d'une remise à jour des procédures opérationnelles.

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

Sans objet

7.7. Mesures de sécurité réseau

Les mesures mises en place répondent à l'analyse de risques effectues sur le système d'information [R1].
Les communications réseau véhiculant des informations confidentielles doivent faire l'objet de mesures de protection contre l'écoute des informations.
Des scans périodiques de détection de vulnérabilités sur les équipements du PSCE accessibles depuis l'Intranet ou l'Internet doivent être conduits.
Des passerelles de sécurité sont mises en place afin de protéger la composant locale du système d'information des accès non autorisés depuis l'Intranet et Internet.

7.8. Horodatage / système de datation

Cf. 6.5.5

8. Profils des certificats, OCSP et des CRL

Les profils des certificats et des CRL sont décrits dans un document propre, intitulé description des certificats et des CRL [A4].

8.1. Profils des certificats

8.1.1. Numéro de version

8.1.2. Extensions de certificat

8.1.3. OID des algorithmes

8.1.4. Forme des noms

8.1.5. Contrainte sur les noms

8.1.6. OID des PC

8.1.7. Utilisation de l'extension contraintes de politique

8.1.8. Sémantique et syntaxe des qualifiants de politique

8.1.9. Sémantiques de traitement des extensions critiques de la PC

8.2. Profil des listes de certificats révoqués

8.2.1. Numéro de version

8.2.2. Extensions de CRL et d'entrées de CRL

8.3. Profil OCSP

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

8.3.1. Numéro de version

La demande et la réponse OCSP sont en version 1.

8.3.2. Extensions OCSP

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

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

8.3.3.

9. Audit de conformité et autres évaluations

9.1. Fréquences et / ou circonstances des évaluations

Un contrôle de conformité à la PC lors de la mise en œuvre opérationnelle du système, et lors de toute modification significative est effectué
Dans tous les cas, un contrôle annuel est mis en place.

9.2. Identités : qualification des évaluateurs

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

9.3. Relations entre évaluateurs et entités évaluées

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

9.4. Périmètre des évaluations

Le contrôleur procède de manière régulière à des contrôles de conformité de la mise en œuvre :
- des politiques de certification
- des déclarations de pratique de certification
- des services mis en œuvre

9.5. Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC un avis qui peut être « réussite, échec, ou à confirmer ».
En cas d'échec, l'équipe d'audit remet des recommandations à l'AC ; le choix des mesures à appliquer appartient à l'AC.
En cas de résultat « à confirmer », l'équipe d'audit identifie les non conformités, et les hiérarchisent ; il appartient à l'AC de proposer un calendrier de résolution des non conformités ; un contrôle de vérification permettra de lever les non conformités identifiées.
En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC.

9.6. Communication des résultats

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

10. Autres problématiques métiers et légales

10.1. Tarifs

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

10.2. Responsabilité financière

10.2.1. Couverture par les assurances

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

10.2.2. Autres ressources

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

10.2.3. Couverture et garantie concernant les entités utilisatrices

Pas d'exigence spécifique.

10.3. Confidentialité des données professionnelles

10.3.1. Périmètre des informations confidentielles

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

En particulier, les informations suivantes sont traitées comme confidentielles :
- La DPC
- Les clés privées des titulaires machines et de l'AC Real
- Les données d'activation
- Les journaux d'événements
- Les causes de révocation des certificats

10.3.2. Informations hors du périmètre des informations confidentielles

Sans objet

10.3.3. Responsabilités en terme de protection des informations confidentielles

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

10.4. Protection des données personnelles

10.4.1. Politique de protection des données personnelles

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

10.4.2. Informations à caractère personnel

Sans objet

10.4.3. Informations à caractère non personnel

Pas d'exigence spécifique.

10.4.4. Responsabilité en terme de protection des données personnelles

Sans objet

10.4.5. Notification et consentement d'utilisation des données personnelles

Sans objet

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

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

10.4.7. Autres circonstances de divulgation d'informations personnelles

Pas d'exigence spécifique.

10.5. Droits sur la propriété intellectuelle et industrielle

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

10.6. Interprétations contractuelles et garanties

10.6.1. Autorités de certification

Le CSN est responsable :

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

Le CSN fait son affaire de toute conséquence dommageable résultant du non-respect du présent document par elle-même ou l'une des entités de l'IGC.
Sauf à démontrer qu'il n'a commis aucune faute intentionnelle ou de négligence, le CSN est responsable de tout préjudice causé à toute personne physique ou morale qu'y s'est fiée raisonnablement aux certificats délivrés dans chacun des cas suivants :
Les informations contenues dans le certificat ne correspondent pas aux informations fournies lors de l'enregistrement
La délivrance du certificat n'a pas donné lieu à vérification de possession de la clé privée correspondante par le porteur
L'AC ou l'OSC n'a pas fait procéder à l'enregistrement de la révocation d'un certificat, et publié cette information conformément à ses engagements.

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

10.6.2. Service d'enregistrement

Cf. ci-dessus

10.6.3. Porteurs de certificats

Sans objet

10.6.4. Utilisateurs de certificats

Sans objet

10.6.5. Autres participants

Pas d'exigence particulière

10.7. Limite de garantie

10.8. Limite de responsabilité

Le CSN ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation, des CRL et ARL ainsi que de tout autre équipement ou logiciel mis à disposition.
Le CSN décline en particulier sa responsabilité pour tout dommage résultant d'un emploi 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 porteur.
Le CSN ne pourra pas être tenu pour responsable de tout dommage résultant de réclamation par des tiers, de perte de clientèle, d'arrêt de travail ou de tout autre dommage, notamment indirects ou perte commerciale.

10.9. Indemnités

10.10. Durée et fin anticipée de validité de la PC

10.10.1. Durée de validité

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

10.10.2. Fin anticipée de validité

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

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

Sans objet

10.11. Notifications individuelles et communications entre les participants

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

10.12. Amendements à la PC

10.12.1. Procédures d'amendements

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

10.12.2. Mécanisme et période d'information sur les amendements

Pas d'exigence spécifique.

10.12.3. Circonstances selon lesquelles l'OID doit être changé

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

10.13. Dispositions concernant la résolution de conflits

Conformément aux textes législatifs et à la réglementation en vigueur, les certificats émis en vertu de la présente Politique Certification sont des certificats dont les conditions d'utilisation sont définies par la présente Politique Certification et par les conditions générales d'utilisation qui définissent les relations entre AC REAL et les notaires ainsi que leurs collaborateurs.

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

10.14. Juridictions compétentes

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

10.15. 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 REAL.

10.16. Dispositions diverses

10.16.1. Accord global

Pas d'exigence spécifique

10.16.2. Transfert d'activités

Cf. chapitre 5.8

10.16.3. Conséquences d'une clause non valide

Pas d'exigence spécifique

10.16.4. Application et renonciation

Pas d'exigence spécifique

10.16.5. Force majeure

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

10.17. Autres dispositions

Sans objet

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 CRL doit répondre aux exigences de sécurité suivantes :

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

11.2. Exigences sur la certification

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

12. Abréviations

AC	**A**utorité de **C**ertification
AEN	**A**utorité d'**E**nregistrement **N**ationale
AFNOR	**A**ssociation **F**rançaise de **N**ormalisation
CRL	Liste de révocation des certificats (**C**ertificate **R**evocation **L**ist)
CSN	**C**onseil **S**upérieur du **N**otariat
DPC	**D**éclaration de **P**ratiques de **C**ertification
ETSI	Institut européen des normes de télécommunication (**E**uropean **T**elecommunications **S**tandards **I**nstitute)
IGC	**I**nfrastructure de **G**estion de **C**lés
OID	Identifiant d'objet (**O**bject **ID**entifier)
OSC	**O**pérateur de **S**ervice de **C**ertification
PC	**P**olitique de **C**ertification
PRIS	**P**olitique de **R**éférencement **I**ntersectorielle de **S**écurité
PSCE	**P**restataire de **S**ervice de **C**ertification **E**lectronique

13. Glossaire

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

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

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

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

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

Déclaration des pratiques de certification

Déclaration des pratiques mises en œuvre par une autorité de certification pour émettre et gérer des certificats

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

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

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

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

Editions successives

Version / Edition	Date	Emetteur	Valideur	Approbateur
01.01	05/03/2007	JP Lacombe, Fidens	Comité stratégique TIC, RSSI venelles, Y. Thomassier, B. Duquesnoy	D. Lefèvre
01.02	26/03/2007	JP Lacombe, Fidens	Comité stratégique TIC, RSSI venelles, Y. Thomassier, B. Duquesnoy	D. Lefèvre
01.03	30/05/2007	JP Lacombe, Fidens	Comité stratégique TIC, RSSI venelles, Y. Thomassier, B. Duquesnoy	Membres du bureau CSN
1.04	07/12/2009	Y. Thomassier	Comité stratégique TIC	Membres du bureau CSN
1.05	11/08/2010	Y. Thomassier	Comité stratégique TIC	Membres du bureau CSN
1.06	12/03/2013	Y.Thomassier	D. Lefèvre	Membres du bureau CSN
1.07	27/01/2015	Y. Thomassier	D. Lefèvre	Membres du bureau CSN
1.08	16/03/2015	Y. Thomassier	D. Lefèvre	Membres du bureau CSN