

INFRASTRUCTURE DE CONFIANCE NATIONALE
Politique de Certification
AC TECHNIQUE

| Version | Date | Description | Auteurs | Société |
|---------|------------|---|---------|------------|
| 0.1 | 14/10/2019 | Version initiale | SR | SEALWeb |
| 0.9 | 16/11/2021 | Mises à jour | FG - SH | AMSN - DSN |
| 0.91 | 18/11/2021 | Mise en cohérence de la partie cachets | FG | AMSN |
| 0.92 | 21/11/2021 | Corrections mineures | FG | AMSN |
| 0.93 | 30/11/2021 | Relecture et commentaires | SR | SEALWeb |
| 0.94 | 01/12/2021 | Finalisation | FG | AMSN |
| 0.95 | 14/12/2021 | Ajout de la hiérarchie d'AC | FG | AMSN |
| 0.96 | 15/12/2021 | Ajout d'une extension | FG | AMSN |
| 1.0 | 14/02/2022 | Prise en compte des modifications post audit | FG | AMSN |
| 1.1 | 29/07/2022 | Modifications mineures | FG | AMSN |
| 1.11 | 28/09/2023 | Modifications (page de garde, disponibilité du service et durée de conservation des réponses/requêtes OCSP) | TH | AMSN |
| 1.2 | 16/02/2024 | Modifications de gabarit, hiérarchie d'AC, gestion d'incident critique et relecture | TH/FG | AMSN |

| État du document - Classification | Référence |
|-----------------------------------|----------------------|
| En cours - Publique | 2.16.492.1.1.1.1.6.1 |

Ce document comporte 60 pages.

Sommaire

| | | |
|----------|--|-----------|
| 1 | INTRODUCTION..... | 10 |
| 1.1 | Présentation générale | 10 |
| 1.2 | Identifiant du document | 11 |
| 1.3 | Entités intervenant dans l'IGC | 11 |
| 1.3.1 | Autorité de certification | 11 |
| 1.3.2 | Autorité d'Enregistrement (AE)..... | 12 |
| 1.3.3 | Porteur de certificat..... | 12 |
| 1.3.5 | Utilisateurs de certificats..... | 12 |
| 1.3.6 | Autres participants | 12 |
| 1.3.6.1 | Mandataire de certification | 12 |
| 1.3.6.2 | Souscripteur | 12 |
| 1.3.6.3 | Demandeur..... | 12 |
| 1.3.6.4 | Opérateur Technique..... | 13 |
| 1.4 | Usage des certificats..... | 13 |
| 1.4.1 | Domaines d'utilisation applicables | 13 |
| 1.4.1.1 | Bi-clés et certificats de l'AC TECHNIQUE | 13 |
| 1.4.1.2 | Bi-clés et certificats finaux | 13 |
| 1.4.2 | Domaines d'utilisation interdits | 13 |
| 1.5 | Gestion de la PC..... | 13 |
| 1.5.1 | Entité gérant la PC | 13 |
| 1.5.2 | Point de contact..... | 13 |
| 1.5.3 | Entité déterminant la conformité de la DPC avec la PC | 13 |
| 1.5.4 | Procédures d'approbation de la conformité | 14 |
| 1.6 | Définitions et acronymes | 14 |
| 1.6.1 | Abréviations..... | 14 |
| 1.6.2 | Termes communs aux différentes PC et autres documents..... | 15 |
| 2 | RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES..... | 17 |
| 2.1 | Entité chargée de la mise à disposition des informations..... | 17 |
| 2.2 | Informations devant être mises à disposition | 17 |
| 2.3 | Délais et fréquences de publication..... | 18 |
| 2.4 | Contrôle d'accès aux informations publiées | 18 |
| 3 | IDENTIFICATION ET AUTHENTIFICATION | 19 |
| 3.1 | Nommage..... | 19 |
| 3.1.1 | Types de noms | 19 |
| 3.1.2 | Nécessité d'utilisation de noms explicites | 19 |

Politique de Certification de l'AC TECHNIQUE

| | | |
|----------|--|-----------|
| 3.1.3 | Anonymisation ou pseudonymisation des Porteurs | 19 |
| 3.1.4 | Règles d'interprétation des différentes formes de noms | 19 |
| 3.1.5 | Unicité des noms..... | 19 |
| 3.1.6 | Identification, authentification et rôle des marques déposées..... | 19 |
| 3.2 | Validation initiale de l'identité | 20 |
| 3.2.1 | Méthode pour prouver la possession de la clé privée..... | 20 |
| 3.2.2 | Validation de l'identité d'un organisme..... | 20 |
| 3.2.3 | Validation de l'identité d'un individu..... | 20 |
| 3.2.3.1 | Enregistrement du Représentant légal..... | 20 |
| 3.2.3.2 | Enregistrement d'un RC [représentant de la personne morale] sans Mandataire de Certification | 20 |
| 3.2.3.3 | Enregistrement des Mandataires de Certification (MC)..... | 21 |
| 3.2.3.4 | Enregistrement d'un RC [représentant de la personne morale] via un MC | 21 |
| 3.2.4 | Informations non vérifiées du Porteur..... | 21 |
| 3.2.5 | Validation de l'autorité du demandeur..... | 21 |
| 3.2.6 | Certification croisée d'AC | 21 |
| 3.3 | Identification et validation d'une demande de renouvellement des clés..... | 22 |
| 3.3.1 | Identification et validation pour un renouvellement courant | 22 |
| 3.3.2 | Identification et validation pour un renouvellement après révocation | 22 |
| 3.4 | Identification d'une demande de révocation..... | 22 |
| 4 | EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS..... | 23 |
| 4.1 | Demande de certificat | 23 |
| 4.1.1 | Origine d'une demande de certificat..... | 23 |
| 4.1.2 | Processus et responsabilités pour l'établissement d'une demande de certificat..... | 23 |
| 4.1.3 | Processus et document de remise..... | 23 |
| 4.2 | Traitement d'une demande de certificat..... | 24 |
| 4.2.1 | Exécution des processus d'identification et de validation de la demande..... | 24 |
| 4.2.2 | Acceptation ou rejet de la demande | 24 |
| 4.2.3 | Durée d'établissement du certificat | 24 |
| 4.3 | Délivrance du certificat..... | 24 |
| 4.3.1 | Actions de l'AC concernant la délivrance du certificat | 24 |
| 4.3.2 | Notification par l'AC de la délivrance du certificat..... | 24 |
| 4.4 | Acceptation du certificat | 25 |
| 4.4.1 | Démarche d'acceptation du certificat | 25 |
| 4.4.2 | Publication du certificat | 25 |
| 4.4.3 | Notification par l'AC aux autres entités de la délivrance du certificat | 25 |
| 4.5 | Usage de la bi-clé et du certificat..... | 25 |
| 4.5.1 | Usage de la clé privée | 25 |
| 4.5.1.1 | Clé privée de l'AC TECHNIQUE..... | 25 |
| 4.5.1.2 | Clé privée des certificats finaux..... | 25 |
| 4.5.2 | Usage de la clé publique et du certificat | 25 |

Politique de Certification de l'AC TECHNIQUE

| | | |
|---------|--|----|
| 4.5.2.1 | Clé publique et certificat de l'AC TECHNIQUE..... | 25 |
| 4.5.2.2 | Clé publique des certificats finaux..... | 25 |
| 4.6 | Renouvellement d'un certificat..... | 26 |
| 4.6.1 | Causes possibles de renouvellement d'un certificat..... | 26 |
| 4.6.2 | Origine d'une demande de renouvellement..... | 26 |
| 4.6.3 | Procédure de traitement d'une demande de renouvellement..... | 26 |
| 4.6.4 | Notification au Porteur de l'établissement du nouveau certificat..... | 26 |
| 4.6.5 | Démarche d'acceptation du nouveau certificat..... | 26 |
| 4.6.6 | Publication du nouveau certificat..... | 26 |
| 4.6.7 | Notification par l'AC aux autres entités de la délivrance du nouveau certificat..... | 26 |
| 4.7 | Délivrance d'un nouveau certificat suite au changement de la bi-clé..... | 26 |
| 4.7.1 | Causes possibles de changement d'une bi-clé..... | 26 |
| 4.7.2 | Origine d'une demande d'un nouveau certificat..... | 26 |
| 4.7.3 | Procédure de traitement d'une demande d'un nouveau certificat..... | 27 |
| 4.7.4 | Notification au RC de l'établissement du nouveau certificat..... | 27 |
| 4.7.5 | Démarche d'acceptation du nouveau certificat..... | 27 |
| 4.7.6 | Publication du nouveau certificat..... | 27 |
| 4.7.7 | Notification par l'AC aux autres entités de la délivrance du nouveau certificat..... | 27 |
| 4.8 | Modification du certificat..... | 28 |
| 4.8.1 | Causes possibles de modification d'un certificat..... | 28 |
| 4.8.2 | Origine d'une demande de modification d'un certificat..... | 28 |
| 4.8.3 | Procédure de traitement d'une demande de modification d'un certificat..... | 28 |
| 4.8.4 | Notification au Porteur de l'établissement du certificat modifié..... | 28 |
| 4.8.5 | Démarche d'acceptation du certificat modifié..... | 28 |
| 4.8.6 | Publication du certificat modifié..... | 28 |
| 4.8.7 | Notification par l'AC aux autres entités de la délivrance du certificat modifié..... | 28 |
| 4.9 | Révocation et suspension des certificats..... | 28 |
| 4.9.1 | Causes possibles d'une révocation..... | 28 |
| 4.9.2 | Origine d'une demande de révocation..... | 29 |
| 4.9.3 | Procédure de traitement d'une demande de révocation..... | 29 |
| 4.9.3.1 | Procédure de révocation par le RC..... | 29 |
| 4.9.3.2 | Procédure de révocation par l'AE ou l'Officier de Sécurité de l'ICN..... | 30 |
| 4.9.3.3 | Procédure de révocation en l'absence du code de révocation..... | 30 |
| 4.9.4 | Délai accordé pour formuler la demande de révocation..... | 30 |
| 4.9.5 | Délai de traitement par l'AC d'une demande de révocation..... | 30 |
| 4.9.6 | Exigences de vérification de la révocation par les utilisateurs de certificats..... | 30 |
| 4.9.7 | Fréquence d'établissement des LCR..... | 30 |
| 4.9.8 | Délai maximum de publication des LCR..... | 31 |
| 4.9.9 | Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats..... | 31 |
| 4.9.10 | Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats..... | 31 |

Politique de Certification de l'AC TECHNIQUE

| | | |
|----------|---|-----------|
| 4.9.11 | Autres moyens disponibles d'information sur les révocations | 31 |
| 4.9.12 | Exigences spécifiques en cas de compromission de la clé privée ou de vulnérabilité zéro-jour..... | 31 |
| 4.9.13 | Causes possibles d'une suspension | 31 |
| 4.9.14 | Origine d'une demande de suspension..... | 31 |
| 4.9.15 | Procédure de traitement d'une demande de suspension | 32 |
| 4.9.16 | Limites de la période de suspension d'un certificat..... | 32 |
| 4.10 | Fonction d'information sur l'état des certificats | 32 |
| 4.10.1 | Caractéristiques opérationnelles | 32 |
| 4.10.2 | Disponibilité de la fonction..... | 32 |
| 4.10.3 | Dispositifs optionnels..... | 32 |
| 4.11 | Fin de la relation avec l'AC TECHNIQUE..... | 32 |
| 4.12 | Séquestre de clé et recouvrement | 32 |
| 4.12.1 | Politique et pratiques de recouvrement par séquestre des clés..... | 32 |
| 4.12.2 | Politique et pratiques de recouvrement par encapsulation des clés de session | 32 |
| 5 | MESURES DE SECURITE NON TECHNIQUES | 33 |
| 5.1 | Mesures de sécurité physique | 33 |
| 5.1.1 | Situation géographique et construction des sites | 33 |
| 5.1.2 | Accès physique | 33 |
| 5.1.3 | Alimentation électrique et climatisation | 33 |
| 5.1.4 | Vulnérabilité aux dégâts des eaux..... | 33 |
| 5.1.5 | Prévention et protection incendie..... | 33 |
| 5.1.6 | Conservation des supports | 33 |
| 5.1.7 | Mise hors service des supports..... | 33 |
| 5.1.8 | Sauvegardes hors site..... | 34 |
| 5.2 | Mesures de sécurité procédurales..... | 34 |
| 5.2.1 | Rôles de confiance | 34 |
| 5.2.2 | Nombre de personnes requises par tâche | 34 |
| 5.2.3 | Identification et authentification pour chaque rôle | 35 |
| 5.2.4 | Rôles exigeant une séparation des attributions | 35 |
| 5.3 | Mesures de sécurité vis-à-vis du personnel..... | 35 |
| 5.3.1 | Qualifications, compétences et habilitations requises..... | 35 |
| 5.3.2 | Procédures de vérification des antécédents..... | 35 |
| 5.3.3 | Exigences en matière de formation initiale | 35 |
| 5.3.4 | Exigences et fréquence en matière de formation continue..... | 36 |
| 5.3.5 | Fréquence et séquence de rotation entre différentes attributions | 36 |
| 5.3.6 | Sanctions en cas d'actions non autorisées..... | 36 |
| 5.3.7 | Exigences vis-à-vis du personnel des prestataires externes | 36 |
| 5.3.8 | Documentation fournie au personnel | 36 |
| 5.4 | Procédure de constitution des données d'audit | 36 |
| 5.4.1 | Types d'événements à enregistrer | 36 |

Politique de Certification de l'AC TECHNIQUE

| | | |
|----------|---|-----------|
| 5.4.2 | Fréquence de traitement des journaux d'événements | 37 |
| 5.4.3 | Période de conservation des journaux d'événements | 37 |
| 5.4.4 | Protection des journaux d'événements | 37 |
| 5.4.5 | Procédure de sauvegarde des journaux d'événements..... | 37 |
| 5.4.6 | Système de collecte des journaux d'événements..... | 37 |
| 5.4.7 | Notification de l'enregistrement d'un événement au responsable de l'événement..... | 37 |
| 5.4.8 | Évaluation des vulnérabilités | 37 |
| 5.5 | Archivage des données..... | 38 |
| 5.5.1 | Types de données à archiver | 38 |
| 5.5.2 | Période de conservation des archives..... | 38 |
| 5.5.3 | Protection des archives | 38 |
| 5.5.4 | Procédure de sauvegarde des archives | 38 |
| 5.5.5 | Exigences d'horodatage des données..... | 38 |
| 5.5.6 | Système de collecte des archives | 38 |
| 5.5.7 | Procédures de récupération et de vérification des archives..... | 39 |
| 5.6 | Changement de clé d'AC | 39 |
| 5.7 | Reprise suite à la compromission et sinistre | 39 |
| 5.7.1 | Procédures de remontée et de traitement des incidents et des compromissions..... | 39 |
| 5.7.2 | Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) 39 | |
| 5.7.3 | Procédures de reprise en cas de compromission de la clé privée d'une composante..... | 40 |
| 5.7.4 | Capacités de continuité d'activité suite à un sinistre | 40 |
| 5.7.5 | Actions à mener en cas de compromission d'un algorithme ou d'un paramètre associé | 40 |
| 5.8 | Fin de vie de l'AC | 40 |
| 5.8.1 | Transfert ou cessation d'activité affectant l'AC | 41 |
| 5.8.2 | Cessation d'activité affectant l'AC | 41 |
| 6 | MESURES DE SECURITE TECHNIQUES..... | 42 |
| 6.1 | Génération et installation de bi-clés..... | 42 |
| 6.1.1 | Génération des bi-clés..... | 42 |
| 6.1.1.1 | Clé des AC opérationnelles..... | 42 |
| 6.1.1.2 | Clés des certificats d'horodatage | 42 |
| 6.1.2 | Transmission de la clé privée à son propriétaire | 42 |
| 6.1.3 | Transmission de la clé publique à l'AC..... | 42 |
| 6.1.4 | Transmission de la clé publique de l'AC aux utilisateurs de certificats..... | 42 |
| 6.1.5 | Tailles des clés..... | 43 |
| 6.1.6 | Vérification de la génération des paramètres des bi-clés et de leur qualité..... | 43 |
| 6.1.7 | Objectifs d'usage de la clé..... | 43 |
| 6.2 | Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques..... | 43 |
| 6.2.1 | Standards et mesures de sécurité pour les modules cryptographiques..... | 43 |
| 6.2.1.1 | Standards pour les modules cryptographiques..... | 43 |

Politique de Certification de l'AC TECHNIQUE

| | | |
|----------|--|-----------|
| 6.2.1.2 | Mesures de sécurité pour les supports cryptographiques des certificats finaux | 43 |
| 6.2.2 | Contrôle de la clé privée par plusieurs personnes | 43 |
| 6.2.3 | Séquestre de la clé privée..... | 43 |
| 6.2.4 | Copie de secours de la clé privée | 44 |
| 6.2.4.1 | Clé privée des AC opérationnelles..... | 44 |
| 6.2.4.2 | Clé privée des certificats finaux..... | 44 |
| 6.2.5 | Archivage de la clé privée..... | 44 |
| 6.2.6 | Transfert de la clé privée vers / depuis le module cryptographique..... | 44 |
| 6.2.7 | Stockage de la clé privée dans un module cryptographique | 44 |
| 6.2.8 | Méthode d'activation de la clé privée..... | 44 |
| 6.2.9 | Méthode de désactivation de la clé privée | 44 |
| 6.2.10 | Méthode de destruction des clés privées..... | 45 |
| 6.2.11 | Niveau de qualification du module cryptographique et des dispositifs de création de signature..... | 45 |
| 6.3 | Autres aspects de la gestion des bi-clés | 45 |
| 6.3.1 | Archivage des clés publiques..... | 45 |
| 6.3.2 | Durées de vie des bi-clés et des certificats..... | 45 |
| 6.3.2.1 | Durées de vie des bi-clés et des certificats des AC opérationnelles | 45 |
| 6.3.2.2 | Durées de vie des bi-clés et des certificats des certificats finaux | 45 |
| 6.4 | Données d'activation..... | 45 |
| 6.4.1 | Génération et installation des données d'activation..... | 45 |
| 6.4.2 | Protection des données d'activation | 45 |
| 6.4.3 | Autres aspects liés aux données d'activation..... | 45 |
| 6.5 | Mesures de sécurité des systèmes informatiques | 46 |
| 6.5.1 | Exigences de sécurité technique spécifiques aux systèmes informatiques..... | 46 |
| 6.5.1.1 | Identification et authentification | 46 |
| 6.5.1.2 | Contrôle d'accès | 46 |
| 6.5.1.3 | Administration et exploitation | 46 |
| 6.5.1.4 | Intégrité des composantes | 46 |
| 6.5.1.5 | Sécurité des flux | 46 |
| 6.5.1.6 | Journalisation et audit | 46 |
| 6.5.1.7 | Supervision et contrôle | 46 |
| 6.5.1.8 | Sensibilisation..... | 46 |
| 6.5.2 | Niveau de qualification des systèmes informatiques | 46 |
| 6.6 | Mesures de sécurité liées au développement des systèmes..... | 47 |
| 6.6.1 | Mesures liées à la gestion de la sécurité..... | 47 |
| 6.6.2 | Niveau d'évaluation sécurité du cycle de vie des systèmes..... | 47 |
| 6.7 | Mesures de sécurité réseau..... | 47 |
| 6.8 | Horodatage / Système de datation..... | 47 |
| 7 | PROFILS DE CERTIFICATS ET DES LCR..... | 48 |
| 7.1 | Profil des certificats | 48 |
| 7.1.1 | Certificats de l'AC TECHNIQUE | 48 |

Politique de Certification de l'AC TECHNIQUE

| | | |
|----------|--|-----------|
| 7.1.1.1 | Champs de base du certificat | 48 |
| 7.1.1.2 | Extensions du certificat..... | 49 |
| 7.1.2 | Certificats finaux d'horodatage (environnement HSM non QSCD) | 50 |
| 7.1.2.1 | Champs de base du certificat | 50 |
| 7.1.2.2 | Extensions du certificat..... | 51 |
| 7.2 | Liste des Certificats Révoqués | 52 |
| 7.2.1 | Champ de base | 52 |
| 7.2.2 | Extensions..... | 52 |
| 7.3 | OCSP..... | 53 |
| 7.3.1 | Champ de base | 53 |
| 7.3.2 | Extensions..... | 54 |
| 8 | AUDIT DE CONFORMITE ET AUTRES EVALUATIONS..... | 55 |
| 8.1 | Fréquences et / ou circonstances des évaluations..... | 55 |
| 8.2 | Identités / qualifications des évaluateurs..... | 55 |
| 8.3 | Relations entre évaluateurs et entités évaluées | 55 |
| 8.4 | Sujets couverts par les évaluations..... | 55 |
| 8.5 | Actions prises suite aux conclusions des évaluations | 55 |
| 9 | AUTRES PROBLEMATIQUES METIERS ET LEGALES | 56 |
| 9.1 | Tarif..... | 56 |
| 9.2 | Responsabilité financière | 56 |
| 9.2.1 | Couverture par les assurances | 56 |
| 9.2.2 | Autres ressources | 56 |
| 9.2.3 | Couverture et garantie concernant les entités utilisatrices | 56 |
| 9.3 | Confidentialité des données professionnelles | 56 |
| 9.3.1 | Périmètre des informations confidentielles..... | 56 |
| 9.3.2 | Informations hors du périmètre des informations confidentielles..... | 56 |
| 9.3.3 | Responsabilités en termes de protection des informations confidentielles | 56 |
| 9.4 | Protection des données personnelles..... | 57 |
| 9.4.1 | Politique de protection des données personnelles..... | 57 |
| 9.4.2 | Informations à caractère personnel | 57 |
| 9.4.3 | Responsabilité en termes de protection des données personnelles..... | 57 |
| 9.4.4 | Notification et consentement d'utilisation des données personnelles..... | 57 |
| 9.4.5 | Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives | 57 |
| 9.4.6 | Autres circonstances de divulgation d'informations personnelles..... | 57 |
| 9.5 | Droits sur la propriété intellectuelle et industrielle | 57 |
| 9.6 | Indépendance des parties et non-discrimination | 57 |
| 9.7 | Interprétations contractuelles et garanties..... | 58 |
| 9.7.1 | Autorités de Certification..... | 58 |
| 9.7.2 | Autorités d'enregistrement | 58 |
| 9.7.3 | Porteur de certificat..... | 58 |

Politique de Certification de l'AC TECHNIQUE

| | | |
|--------|---|----|
| 9.7.4 | Responsable de Certificat de personne morale | 58 |
| 9.7.5 | Utilisateurs de certificats..... | 58 |
| 9.7.6 | Autres participants | 58 |
| 9.8 | Limite de garantie | 58 |
| 9.9 | Limite de responsabilité | 59 |
| 9.10 | Indemnités | 59 |
| 9.11 | Durée et fin anticipée de validité de la PC | 59 |
| 9.11.1 | Durée de validité | 59 |
| 9.11.2 | Fin anticipée de validité | 59 |
| 9.11.3 | Effets de la fin de validité et clauses restant applicables | 59 |
| 9.12 | Amendements à la PC | 59 |
| 9.13 | Mécanisme et période d'information sur les amendements | 60 |
| 9.14 | Circonstances selon lesquelles l'OID doit être changé | 60 |
| 9.15 | Dispositions concernant la résolution de conflits | 60 |
| 9.16 | Juridictions compétentes | 60 |
| 9.17 | Disposition diverses | 60 |
| 9.17.1 | Accord global..... | 60 |
| 9.17.2 | Transfert d'activités | 60 |
| 9.17.3 | Conséquences d'une clause non valide..... | 60 |
| 9.17.4 | Application et renonciation..... | 60 |
| 9.17.5 | Force majeure | 60 |
| 9.17.6 | Autres dispositions..... | 60 |

Politique de Certification de l'AC TECHNIQUE

1 INTRODUCTION

1.1 PRESENTATION GENERALE

Au sein de la Principauté de Monaco, l'Agence Monégasque de Sécurité du Numérique (AMSN) est responsable de la chaîne de certification de l'État. Dans ce cadre, elle génère et opère les Autorités de Certification (AC) Opérationnelles pour le compte des Directions Métiers. Ces Autorités de Certification sont émises par une Autorité de Certification Racine dont les conditions de gestion sont définies dans la Politique de Certification associée [AMSN_PC_RACINE].

Les certificats finaux mis en œuvre par le Gouvernement monégasque sont générés par ces Autorités de Certification Opérationnelles également appelées Autorités de Certification Délégées (ACD). L'ensemble constitue une hiérarchie de certification.

Techniquement, l'AMSN recourt à une Infrastructure à Gestion de Clés (IGC) en ligne pour la gestion des clés des AC Opérationnelles.

Un responsable est désigné pour chaque Autorité de Certification.

La hiérarchie d'AC est la suivante :

- Racine : AC RACINE PRINCIPALTE DE MONACO
- ACD : AC MAIRIE, AC GOUVERNEMENT PRINCIER, AC ENTREPRISES, AC SERVICES ADMINISTRATIFS et AC TECHNIQUE.

Une AC SERVICES NUMERIQUES fait également partie de cette hiérarchie mais n'est pas présentée dans le tableau de synthèse suivant qui reprend également les types de certificat que chaque ACD est en capacité de produire.

| AC | Service | Niveau ETSI/eIDAS 319 411-1 & 319 411-2 | | OID | Service EKU | |
|---------------------------------|-------------------------------------|--|------------------|---------------------------|---------------------------|-------------------|
| AC RACINE PRINCIPALTE DE MONACO | Autorité Racine | | | 2.16.492.1.1.1.1.1.1 | | |
| AC MAIRIE | Signature | QCP-n-qscd | 0.4.0.194112.1.2 | 2.16.492.1.1.1.1.2.4.1.2 | Email protection | 1.3.6.1.5.5.7.3.4 |
| | Authentification | NCP+ | 0.4.0.2042.1.2 | 2.16.492.1.1.1.1.2.4.2.2 | TLS client authentication | 1.3.6.1.5.5.7.3.2 |
| | Signature (Mobile) | NCP | 0.4.0.2042.1.1 | 2.16.492.1.1.1.1.2.4.11.2 | Email protection | 1.3.6.1.5.5.7.3.4 |
| | Authentification (Mobile) | NCP | 0.4.0.2042.1.1 | 2.16.492.1.1.1.1.2.4.12.2 | TLS client authentication | 1.3.6.1.5.5.7.3.2 |
| AC GOUVERNEMENT PRINCIER | Signature | QCP-n-qscd | 0.4.0.194112.1.2 | 2.16.492.1.1.1.1.3.4.1.2 | Email protection | 1.3.6.1.5.5.7.3.4 |
| | Authentification | NCP+ | 0.4.0.2042.1.2 | 2.16.492.1.1.1.1.3.4.2.2 | TLS client authentication | 1.3.6.1.5.5.7.3.2 |
| | Signature (Mobile) | NCP | 0.4.0.2042.1.1 | 2.16.492.1.1.1.1.3.4.11.2 | Email protection | 1.3.6.1.5.5.7.3.4 |
| | Authentification (Mobile) | NCP | 0.4.0.2042.1.1 | 2.16.492.1.1.1.1.3.4.12.2 | TLS client authentication | 1.3.6.1.5.5.7.3.2 |
| AC ENTREPRISES | Signature | QCP-n-qscd | 0.4.0.194112.1.2 | 2.16.492.1.1.1.1.4.4.1.2 | Email protection | 1.3.6.1.5.5.7.3.4 |
| | Authentification | NCP+ | 0.4.0.2042.1.2 | 2.16.492.1.1.1.1.4.4.2.2 | TLS client authentication | 1.3.6.1.5.5.7.3.2 |
| | Cachets sur support carte à puce | QCP-I-qscd | 0.4.0.194112.1.3 | 2.16.492.1.1.1.1.4.4.5.2 | | |
| | Cachet serveur avec HSM non QSCD | QCP-I | 0.4.0.194112.1.1 | 2.16.492.1.1.1.1.4.4.6.2 | | |
| | Cachet serveur avec HSM QSCD | QCP-I-qscd | 0.4.0.194112.1.3 | 2.16.492.1.1.1.1.4.4.7.2 | | |
| | Cachets logiciels | LCP | 0.4.0.2042.1.3 | 2.16.492.1.1.1.1.4.4.8.2 | | |
| AC SERVICES ADMINISTRATIFS | Signature | QCP-n-qscd | 0.4.0.194112.1.2 | 2.16.492.1.1.1.1.5.4.1.2 | Email protection | 1.3.6.1.5.5.7.3.4 |
| | Authentification | NCP+ | 0.4.0.2042.1.2 | 2.16.492.1.1.1.1.5.4.2.2 | TLS client authentication | 1.3.6.1.5.5.7.3.2 |
| | Cachets sur support carte à puce | QCP-I-qscd | 0.4.0.194112.1.3 | 2.16.492.1.1.1.1.5.4.5.2 | | |
| | Cachet serveur avec HSM non QSCD | QCP-I | 0.4.0.194112.1.1 | 2.16.492.1.1.1.1.5.4.6.2 | | |
| | Cachet serveur avec HSM QSCD | QCP-I-qscd | 0.4.0.194112.1.3 | 2.16.492.1.1.1.1.5.4.7.2 | | |
| | Cachets logiciels | LCP | 0.4.0.2042.1.3 | 2.16.492.1.1.1.1.5.4.8.2 | | |
| AC TECHNIQUE | Cachet horodatage avec HSM non QSCD | QCP-I | 0.4.0.194112.1.1 | 2.16.492.1.1.1.1.6.4.10.2 | id-kp-timestamping | 1.3.6.1.5.5.7.3.8 |
| | Cachet horodatage avec HSM QSCD | QCP-I-qscd | 0.4.0.194112.1.3 | 2.16.492.1.1.1.1.6.4.13.2 | id-kp-timestamping | 1.3.6.1.5.5.7.3.8 |
| | Cachet horodatage logiciel | LCP | 0.4.0.2042.1.3 | 2.16.492.1.1.1.1.6.4.14.2 | id-kp-timestamping | 1.3.6.1.5.5.7.3.8 |
| | TSU | | | 2.16.492.1.1.1.1.6.11.2 | | |

La présente Politique de Certification (PC) définit les engagements que prend la DIRECTION DES SERVICES NUMÉRIQUES quant aux opérations de son ACD, appelée AC TECHNIQUE.

Lorsque cela n'est pas précisé, le terme « AC » désigne dans le présent document l'AC TECHNIQUE.

1.2 IDENTIFIANT DU DOCUMENT

La présente PC est identifiée par le numéro suivant : 2.16.492.1.1.1.1.6.1

1.3 ENTITES INTERVENANT DANS L'IGC

1.3.1 Autorité de certification

L'entité en charge de l'AC TECHNIQUE (AC) est la DIRECTION DES SERVICES NUMÉRIQUES.

Cette AC opérationnelle dépend de l'AC Racine qui relève de la responsabilité de l'AMSN.

Un comité de suivi nommé « comité de suivi des services de confiance » (C2SC) est mis en œuvre sous la responsabilité du Conseiller de Gouvernement-Ministre de l'Intérieur. Ce comité est le garant de l'application de la PC et de la bonne concordance avec les autres référentiels documentaires, la Déclaration des Pratiques de Certification (DPC) notamment.

Ce comité est constitué des parties prenantes suivantes :

- Le responsable de l'AC Racine ;
- Les responsables de chacune des ACD ;
- Le Responsable de la Sécurité des Systèmes d'Information du Gouvernement ;
- Le Responsable de la Sécurité des Systèmes d'Information de la Direction de la Sûreté Publique ;
- Le Responsable de la Sécurité des Systèmes d'Information de la Mairie ;
- L'Officier de Sécurité de l'ICN.

Le responsable de l'Opérateur Technique ou toutes personnes jugées utiles en lien avec l'ordre du jour d'une réunion du C2SC peuvent, le cas échéant, y être conviés.

L'AC est responsable des certificats signés en son nom.

En particulier, l'AC a la responsabilité des fonctions suivantes :

- Mise en application de la Politique de Certification ;
- Enregistrement des rôles de confiance ;
- Émission des Certificats ;
- Gestion du cycle de vie des Certificats ;
- Publication de la Liste des Certificats Révoqués (LCR) ;
- Journalisation et archivage des événements et informations relatives au fonctionnement de l'AC.

La responsabilité de l'enregistrement des porteurs de secrets de l'ICN incombe au responsable de l'AC Racine.

1.3.2 Autorité d'Enregistrement (AE)

La DIRECTION DES SERVICES NUMÉRIQUES (la Direction Métier) pour laquelle l'AC TECHNIQUE a été émise établit les processus de gestion des certificats finaux.

Pour cela, le rôle d'AE peut être délégué par l'AC. Dans ce cas, une convention, appelée « Convention AC-AE » est établie entre les parties. Dans le cas de la présente PC, tant que la fonction d'AE sera assurée par des personnes hiérarchiquement subordonnées à l'AC, aucune convention ne sera donc établie.

L'Autorité d'Enregistrement assure les fonctions suivantes :

- Réception des dossiers de demande de génération d'un certificat ;
- Réception des dossiers de demande de révocation d'un certificat ;
- Vérification de l'identité et de l'habilitation du futur Responsable de Certificat à demander la création du certificat correspondant ;
- Déclenchement de la génération des certificats ;
- Traitement de la révocation des certificats ;
- Déclenchement des fonctions d'archivage des données.

L'Autorité d'Enregistrement habilite formellement des personnes en son sein au rôle d'opérateurs d'enregistrement. Lorsque l'AC assure également les fonctions d'AE, cette habilitation est à réaliser par l'AC. Ces personnes sont en charge d'opérer les processus définis par l'Autorité d'Enregistrement dans le cadre, le cas échéant, de la convention établie avec l'Autorité de Certification.

1.3.3 Porteur de certificat

Sans objet.

L'AC TECHNIQUE ne délivrant que des certificats d'horodatage, il n'y a pas donc pas de Porteur de certificat au sens de la présente PC.

1.3.4 Responsable du Certificat de la personne morale

La notion de Responsable de Certificat ne s'applique qu'aux certificats finaux de personnes morales. Le Responsable du Certificat est la personne physique nommée et mandatée par le Responsable Légal de la personne morale pour gérer tout ou partie des certificats d'horodatage de cette dernière.

1.3.5 Utilisateurs de certificats

Les utilisateurs de certificats sont les collaborateurs, services, serveurs et applications qui font confiance aux certificats émis par l'AC.

1.3.6 Autres participants

1.3.6.1 Mandataire de certification

Le Mandataire de Certification (MC) est la personne physique nommée et mandatée par le Représentant légal pour gérer une flotte de certificats pour le compte de l'organisation qu'il représente. Il peut gérer à la fois les certificats pour des personnes physiques ou pour des personnes morales et peut donc être Responsable du Certificat.

1.3.6.2 Souscripteur

Le souscripteur est la personne physique ou morale qui paye ou adhère à un service de confiance proposé par l'AC.

1.3.6.3 Demandeur

Le demandeur est la personne physique qui effectue une demande auprès d'une Autorité d'Enregistrement pour obtenir un certificat d'horodatage.

1.3.6.4 Opérateur Technique

L'Opérateur Technique a la responsabilité du maintien en conditions opérationnelle et de sécurité des composants techniques permettant d'opérer l'AC. Cela inclut les fonctions de délivrance de certificats, de renouvellement et de révocation.

L'Opérateur Technique est lié contractuellement à l'AMSN.

1.4 USAGE DES CERTIFICATS

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats de l'AC TECHNIQUE

Les bi-clés et les certificats de l'AC TECHNIQUE sont utilisés exclusivement pour la signature :

- des demandes de certificats ;
- des LCR ;
- des réponses OCSP.

1.4.1.2 Bi-clés et certificats finaux

L'AC TECHNIQUE émet différents profils de certificats <PROFIL>, chacun identifié par un OID spécifique. Les usages sont explicites dans le gabarit du certificat.

Les profils définis sont les suivants :

- profil « Horodatage » ;
- Profil « OSCP ».

1.4.2 Domaines d'utilisation interdits

Tout autre usage que celui défini dans le paragraphe précédent est interdit.

1.5 GESTION DE LA PC

1.5.1 Entité gérant la PC

La PC est approuvée par le C2SC et mise en œuvre par l'AC.

1.5.2 Point de contact

Toute information concernant la présente PC ou la gestion de l'AC peut être demandée via le point de contact suivant :

- par courrier : DIRECTION DES SERVICES NUMÉRIQUES - 2 rue du Gabian - Immeuble "Les Industries" - BP 673 MC - 98014 MONACO CEDEX
- par courriel : identitenumérique@gouv.mc

1.5.3 Entité déterminant la conformité de la DPC avec la PC

La conformité de la DPC à la PC est validée par le C2SC.

1.5.4 Procédures d'approbation de la conformité

L'approbation de la conformité est prononcée par le responsable du C2SC sur la base de résultats de revues et d'audits internes et du plan d'actions décidé ou validé par le comité. Les services de confiance font l'objet d'une homologation de sécurité qui atteste que les instances dirigeantes valident la mise en production de l'infrastructure de gestion des clés en ayant connaissance des risques résiduels et en les acceptant.

L'AC TECHNIQUE mène l'homologation sur le périmètre qui la concerne.

1.6 DEFINITIONS ET ACRONYMES

Les acronymes utilisés dans la présente PC sont les suivants :

1.6.1 Abréviations

| | |
|---------------|--|
| AC | Autorité de Certification |
| ACD | Autorité de Certification Déléguée |
| AE | Autorité d'Enregistrement |
| AMSN | Agence Monégasque de Sécurité du Numérique |
| ANSSI | Agence Nationale de la Sécurité des Systèmes d'Information |
| C2SC | Comité de Suivi des Services de Confiance |
| CC | Critères Communs (norme ISO n°15408) |
| CEN | Comité Européen de Normalisation |
| CGU | Conditions Générales d'Utilisation |
| DN | Distinguished Name |
| DPC | Déclaration des Pratiques de Certification |
| DRHFFP | Direction des Ressources Humaines et de la Formation de la Fonction Publique |
| DSN | Direction des Services Numériques |
| DSP | Direction de la Sûreté Publique |
| EAL | Evaluation Assurance Level (niveau d'assurance de l'évaluation) |
| ETSI | European Telecommunications Standards Institute |
| FAQ | Foire Aux Questions |
| FIPS | Federal Information Processing Standards |
| HSM | Hardware Security Module |
| IGC | Infrastructure à Gestion de Clés |
| ICN | Infrastructure de Confiance Nationale |
| LAR | Liste des Autorités Révoquées |
| LCR | Liste des Certificats Révoqués |
| MC | Mandataire de Certification |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| OT | Opérateur Technique |
| PC | Politique de Certification |

| | |
|-------------|--|
| PSCo | Prestataire de Services de Confiance |
| QSCD | Qualified electronic Signature Creation Device (dispositif de création de signature qualifiée) |
| RC | Responsable du Certificat |
| RCI | Répertoire du Commerce et de l'Industrie |
| RSA | Rivest Shamir Adelman |

1.6.2 Termes communs aux différentes PC et autres documents

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.

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 - 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.

Cachet - Certificat de personne morale sous contrôle d'une personne physique. Il est mis en œuvre sur un serveur à partir d'une application.

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

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

Chaîne de confiance - Ensemble des Certificats nécessaires pour valider la généalogie d'un Certificat.

Dans le cas présent, la chaîne se compose du Certificat de l'Autorité de Certification Racine qui a émis le certificat de l'ACD, de celui de l'ACD qui a émis le certificat d'horodatage et de celui d'horodatage porté par le Responsable de Certificat.

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 ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Infrastructure de Confiance Nationale (ICN) - L'ICN est l'IGC mise en œuvre par l'AMSN pour le compte du Gouvernement princier. L'AC TECHNIQUE est une des autorités rattachées à l'ICN.

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

Mandataire de Certification (MC) - Personne physique ayant reçu mandat du Représentant légal pour gérer la flotte de certificats de l'entreprise (contrôle du dossier et de l'identité du futur titulaire).

Officier de sécurité de l'ICN - Personne qui a pour mission, sous les ordres de son autorité d'emploi, de fixer les règles et les consignes de sécurité à mettre en œuvre relatives aux personnes et aux informations ou supports protégés et d'en vérifier l'exécution. Dans le cadre de l'ICN, il s'agit du chef de ce projet au sein de l'AMSN.

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

Produit de sécurité - 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.

Représentant légal - Personne(s) légalement désignée(s) en vue de représenter et défendre les intérêts de l'entreprise. Le Représentant légal agit au nom et pour le compte de l'entreprise qu'il représente. Le

Politique de Certification de l'AC TECHNIQUE

Représentant légal est désigné dans les statuts de l'entreprise et son nom est renseigné dans le Répertoire du Commerce et de l'Industrie (RCI).

Responsable du Certificat (RC) - Personne physique qui porte le sujet du certificat.

Responsable du certificat de personne morale - indistinctement le Représentant légal ou un Mandataire de Certification de l'entreprise.

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

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1 ENTITE CHARGEE DE LA MISE A DISPOSITION DES INFORMATIONS

Le responsable de la publication est chargé de mettre à disposition les informations devant être publiées au nom de l'AC et décrites dans la section §2.2 du présent document. Dans le cas présent, cette responsabilité est répartie entre l'Opérateur Technique, l'AGENCE MONÉGASQUE DE SÉCURITÉ NUMÉRIQUE et la DIRECTION DES SERVICES NUMÉRIQUES suivant le périmètre précisé §2.2.

Les informations sont accessibles, en fonction des éléments à publier, aux URL suivantes :

- <https://icn.amsn.mc/icn/>
- <https://icn.monaco.fr/icn/>
- <http://technique-icn.gouv.mc/crl/>
- <http://technique-icn.monaco.fr/crl/>
- <http://technique-ocspicn.gouv.mc>
- <https://mconnect.gouv.mc/technique/>

Il est à noter que le téléchargement sur des liens http peut être identifié comme un comportement suspect sur certains navigateurs. Néanmoins, le téléchargement peut être confirmé par l'utilisateur, qui peut alternativement opter pour un lien https.

2.2 INFORMATIONS DEVANT ETRE MISES A DISPOSITION

Sur le périmètre du présent document, les informations publiées sont les suivantes :

| Nature de l'information | URL | Responsable |
|---|--|-------------|
| la présente PC | https://mconnect.gouv.mc/technique/ | DSN |
| les CGU | https://mconnect.gouv.mc/technique/ | DSN |
| la FAQ | https://mconnect.gouv.mc/technique/ | DSN |
| les éléments constitutifs du dossier d'enregistrement | https://mconnect.gouv.mc/technique/ | DSN |
| le certificat de l'AC | https://icn.amsn.mc/icn/ac-technique.crt | AMSN |
| le certificat de l'AC Racine | https://icn.amsn.mc/icn/acr.crt | AMSN |
| les LAR | http://icn.amsn.mc/icn/icn4096.crl http://icn.monaco.fr/icn/icn4096.crl | AMSN |
| les LCR | http://technique-icn.gouv.mc/crl/technique.crl http://technique-icn.monaco.fr/crl/technique.crl | AMSN |
| le service OCSP | http://technique-ocspicn.gouv.mc | AMSN |

La présente PC est publiée au format PDF/A. Les versions obsolètes des éléments définis ci-dessus restent publiées dans un espace dédié du site de publication. Chaque version de PC et de CGU est accompagnée de la date de publication et de son empreinte réalisée en SHA256.

2.3 DELAIS ET FREQUENCES DE PUBLICATION

Les politiques de certification sont remises à jour et publiées en cas de changement majeur et a minima tous les deux ans.

Les certificats de l'AC sont diffusés ou mis en ligne préalablement à toute diffusion de certificats finaux.

Les LAR sont établies tous les mois.

Les LCR de l'AC sont établies a minima toutes les 24h.

Une supervision est mise en place. Elle s'assure que la LCR publiée est non seulement en cours de validité mais qu'il s'agit bien de la dernière et que son contenu est intègre.

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

Les informations publiées sont mises à disposition en lecture à l'ensemble de la communauté des Utilisateurs.

Les ajouts, suppressions et modifications sont limités aux personnes autorisées de l'AC ou agissant pour son compte. L'accès au service de publication se fait, dans l'idéal, à l'aide d'un moyen d'authentification réunissant au moins 2 facteurs.

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) ; chaque titulaire ayant un nom distinct (DN).

3.1.2 Nécessité d'utilisation de noms explicites

Les noms pour distinguer les titulaires sont explicites. Le nom distinctif est sous la forme d'une chaîne de type UTF8string de type nom X501.

Si un certificat de test doit être produit en environnement de production, le nom distinctif de ce dernier sera précédé de la chaîne de caractère « TEST ».

3.1.3 Anonymisation ou pseudonymisation des Porteurs

Sans objet ; la notion de Porteur ne s'appliquant pas dans le cadre de la présente PC.

3.1.4 Règles d'interprétation des différentes formes de noms

Tous les certificats émis identifient de manière explicite :

- l'émetteur du certificat, en identifiant clairement l'AC TECHNIQUE ;
- le nom du certificat d'horodatage sous la forme d'un nom d'application, d'un nom de service/direction/entité, etc. ;
- la raison sociale de l'organisme auquel appartient le certificat d'horodatage, tel que figurant au RCI (attribut OrganizationName) ;
- Le numéro de RCI dans le champ organizationIdentifiant sous la forme : NTRMC-<numéro de RCI>

Les informations portées sur le certificat d'horodatage sont vérifiées par l'Autorité d'Enregistrement soit sur présentation des justificatifs afférents, soit sur la base de données d'identification propres à l'État monégasque.

3.1.5 Unicité des noms

L'AE s'assure de l'unicité du couple organizationName, commonName par l'ajout d'un identifiant unique dans le commonName sous la forme d'un numéro de série construit sur le modèle suivant : millésime sur 2 digits suivi de TIMESTAMP suivi de 5 digits incrémentés de 1 à chaque fois en commençant par 00001. Exemple : SN=21TIMESTAMP00001.

3.1.6 Identification, authentification et rôle des marques déposées

Sans objet.

3.2 VALIDATION INITIALE DE L'IDENTITE

3.2.1 Méthode pour prouver la possession de la clé privée

Les fichiers de demande de certificat, contenant la clé publique à certifier, sont scellés à l'aide de la clé privée correspondante.

Le RC est, au même titre que le MC, la personne pouvant faire une demande de certificat. L'un comme l'autre sont identifiés initialement par l'AE.

Ils sont garants de la génération de la demande de certificat et habilités à soumettre cette demande auprès de l'ICN.

Les clés privées des certificats d'horodatage sont gérées et stockées dans des environnements qui sont sous la responsabilité du RC.

3.2.2 Validation de l'identité d'un organisme

Voir chapitre 3.2.3.

3.2.3 Validation de l'identité d'un individu

Dans le contexte de l'AC :

- le souscripteur est, d'une manière générale, le Mandataire de Certification (MC) ; ce dernier étant par défaut le Représentant légal. Il peut également être une autre personne physique légitimement mandatée par le Représentant légal ;
- le demandeur est soit le MC, soit le RC.

3.2.3.1 Enregistrement du Représentant légal

Lors du dépôt d'un dossier de demande, l'AE vérifie, le cas échéant, sur la base de données propres à l'État monégasque, notamment les ordonnances de nomination au journal de MONACO ou en se rapprochant de la DRHFFP, les mentions relatives au statut de Représentant légal.

Même si le Représentant légal est connu de l'AE, son identité est validée sur la base de la production d'une copie d'une pièce d'identité dans le dossier de demande accompagnée d'une présentation de l'original s'il est lui-même présent auprès de l'AE lors de la production des certificats.

3.2.3.2 Enregistrement d'un RC [représentant de la personne morale] sans Mandataire de Certification

Le RC peut être lui-même un Mandataire de Certification.

L'enregistrement d'un RC nécessite la prise d'un rendez-vous auprès d'un opérateur d'enregistrement de la DIRECTION DES SERVICES NUMÉRIQUES. Lors de ce rendez-vous, le futur RC présente les pièces suivantes :

- le mandat imprimé et co-signé par le Représentant légal et lui-même l'autorisant à demander un certificat d'horodatage pour le compte de l'organisme apparentant au Représentant légal ;
- le formulaire de demande de certificat imprimé et signé par le Représentant légal et lui-même ;
- un titre d'identité lui appartenant en cours de validité (Carte d'Identité, Passeport) ;
- une photocopie de son titre d'identité (Carte d'Identité, Passeport) ;
- une photocopie du titre d'identité du Représentant légal.

L'opérateur d'enregistrement vérifie alors les pièces et procède, le cas échéant, à la validation du rôle de RC.

L'ensemble des pièces du dossier d'enregistrement est enfin archivé.

3.2.3.3 Enregistrement des Mandataires de Certification (MC)

L'enregistrement d'un Mandataire de Certification nécessite la prise d'un rendez-vous auprès d'un opérateur d'enregistrement de la DIRECTION DES SERVICES NUMÉRIQUES. Lors de ce rendez-vous, le futur Mandataire présente les pièces suivantes :

- le mandat imprimé et co-signé par le Représentant légal et lui-même ;
- un titre d'identité lui appartenant en cours de validité (Carte d'Identité, Passeport) ;
- une photocopie de son titre d'identité (Carte d'Identité, Passeport) ;
- une photocopie du titre d'identité du Représentant légal.

L'opérateur d'enregistrement vérifie alors les pièces et procède, le cas échéant, à la validation du rôle de Mandataire.

L'ensemble des pièces du dossier d'enregistrement est enfin archivé.

3.2.3.4 Enregistrement d'un RC [représentant de la personne morale] via un MC

L'enregistrement d'un RC nécessite la prise d'un rendez-vous auprès d'un opérateur d'enregistrement de la DIRECTION DES SERVICES NUMÉRIQUES. Lors de ce rendez-vous, le Mandataire présente les pièces suivantes :

- le mandat imprimé et co-signé par le Représentant légal, le RC et lui-même autorisant le RC à demander un certificat d'horodatage au nom de l'organisme appartenant au Représentant légal ;
- le formulaire de demande de certificat imprimé et signé par le Représentant légal, le RC et lui-même ;
- un titre d'identité lui appartenant en cours de validité (Carte d'Identité, Passeport) ;
- une photocopie de son titre d'identité (Carte d'Identité, Passeport)
- une photocopie du titre d'identité (Carte d'Identité, Passeport) du Représentant légal ; la vérification de l'identité de ce dernier ayant, préalablement à la photocopie, été effectuée par le Mandataire.

L'opérateur d'enregistrement vérifie alors les pièces et procède, le cas échéant, à la validation du rôle de RC.

L'ensemble des pièces du dossier d'enregistrement est enfin archivé.

3.2.4 Informations non vérifiées du Porteur

Sans objet ; la notion de Porteur ne s'appliquant pas dans le cadre de la présente PC.

3.2.5 Validation de l'autorité du demandeur

L'AE et, par délégation, le Mandataire de Certification, s'assurent que le demandeur dispose des pouvoirs nécessaires pour effectuer cette demande. Cette vérification est effectuée sur la base des informations fournies dans la demande de certificat, et selon des règles spécifiques à la DIRECTION DES SERVICES NUMÉRIQUES, que l'AE fera valider par les responsables de l'Autorité de Certification, avant mise en application.

Pour l'AC TECHNIQUE, le demandeur est le Représentant légal, le Mandataire de Certification ou le Responsable de Certificat.

3.2.6 Certification croisée d'AC

Sans objet.

3.3 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES

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

3.3.1 Identification et validation pour un renouvellement courant

La procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial (voir paragraphe §3.2).

3.3.2 Identification et validation pour un renouvellement après révocation

Suite à la révocation d'un certificat, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial (voir paragraphe §3.2). Si la révocation fait suite à un problème technique lors du retrait du certificat ou avec le support cryptographique (cas de « révocation technique » dans un délai de moins de trois mois après la première demande, une nouvelle demande de certificat se basant sur le dossier d'enregistrement fourni pourra être effectuée. Au-delà, le processus est identique à celui du renouvellement intégrant la signature d'un formulaire daté et signé par le Responsable de Certificat et l'AE.

3.4 IDENTIFICATION D'UNE DEMANDE DE REVOCATION

Toute demande de révocation fait l'objet d'une authentification du demandeur et d'une vérification de sa légitimité pour la faire.

La demande de révocation d'un certificat émis par l'AC TECHNIQUE peut être effectuée par les acteurs suivants :

- le Responsable du Certificat de personne morale ou un Mandataire de Certification de l'organisme de rattachement du RC ;
- l'Autorité d'Enregistrement de l'AC TECHNIQUE ;
- le Représentant légal de l'organisme ;
- le Responsable du C2SC ;
- l'Officier de Sécurité de l'ICN ;
- le Responsable de l'AC.

Toute personne à l'origine d'une demande de révocation est authentifiée selon un processus propre à son statut :

- le RC à l'aide de son code de révocation fourni au moment de la demande de certificat, d'éléments présents dans le dossier d'enregistrement ;
- le Mandataire de Certification ou le Responsable du Certificat sur la base d'une signature manuscrite par comparaison avec la signature présente dans son dossier d'enregistrement ;
- l'Opérateur d'Enregistrement à l'aide de son certificat d'authentification ;
- le Représentant légal sur la base d'une signature manuscrite à l'aide d'un carton de signature ;
- le Responsable du C2SC par l'AE en face-à-face ou un courriel signé ;
- l'Officier de Sécurité de l'ICN à l'aide de son certificat de l'AC SERVICES ADMINISTRATIFS ou par l'AE, soit en face-à-face soit par l'intermédiaire d'un courriel signé ;
- le Responsable de l'AC par l'AE en face-à-face, par une signature manuscrite ou un courriel signé.

Le traitement des demandes de révocation est détaillé dans le paragraphe §4.9.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 DEMANDE DE CERTIFICAT

Le service d'enregistrement proposé par l'AC est disponible, sur rendez-vous, pendant les heures d'ouverture de la DIRECTION DES SERVICES NUMÉRIQUES.

4.1.1 Origine d'une demande de certificat

Une demande de certificat électronique doit avoir fait l'objet d'une vérification et d'une validation par l'AE, préalablement à sa délivrance.

Le processus de demande peut être dématérialisé et le certificat peut être demandé par :

- un RC directement, avec le consentement du Représentant légal de l'organisme ;
- un Mandataire de Certification, dûment mandaté pour cet organisme, dans le cas d'un consentement formel et préalable du futur RC ;
- le Représentant légal de l'organisme.

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

Les deux étapes de demande et de validation de l'identité du RC, objet du paragraphe §3.2.3.4, sont précisées dans ce paragraphe. La validation de la demande est décrite au paragraphe §4.2.1. Comme vu au paragraphe §3.2.3.4, la demande de certificat doit s'appuyer sur un dossier d'enregistrement, intégrant notamment un formulaire de demande comportant les informations suivantes :

- les coordonnées du RC :
 - nom, prénom ;
 - adresse électronique professionnelle ;
 - adresse postale.
- le nom du certificat d'horodatage qui sera positionné dans le certificat ;
- les CGUs ;
- la date et la signature (papier) du RC. Le dossier d'enregistrement doit être transmis à l'AE pour validation. Il peut être au format papier ou au format électronique. Le format électronique pourra résulter d'un scan des documents papier préalablement signés.

4.1.3 Processus et document de remise

À l'issue du processus de remise du certificat, l'opérateur d'enregistrement remet au RC, respectivement Représentant légal ou Mandataire de Certification un bordereau de remise comportant le code de révocation.

Le RC reçoit en parallèle par courriel le certificat au format p7b, PEM ou DER.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

L'identité du RC est vérifiée au travers de la vérification de documents officiels d'identité effectuée lors d'un face-à-face avec un Opérateur d'Enregistrement.

Le RC est en charge de soumettre, directement ou indirectement par l'intermédiaire du MC, sur les interfaces de l'AE la demande de certificat au format PKCS#10.

La demande est alors en attente de validation auprès d'un Opérateur d'Enregistrement.

Dans le processus de demande, chaque partie prenante au dossier (Représentant légal, Mandataire de Certification le cas échéant et Responsable de Certificat) doit répondre à 4 questions parmi les 7 proposées et l'Opérateur d'Enregistrement ne peut donner droit à la demande que si les réponses ont bien été fournies. Ces dernières n'ont d'autre utilité que d'authentifier le demandeur dans les cas où la révocation d'un certificat n'est rendue possible qu'à distance, par téléphone ; la vérification de l'identité du demandeur et donc de sa légitimité à demander la révocation d'un certificat se faisant par l'intermédiaire de ce jeu de questions/réponses.

Si aucun problème n'est détecté dans la demande, l'Opérateur d'Enregistrement saisit la demande dans ses interfaces.

4.2.2 Acceptation ou rejet de la demande

La demande se fait en présence du demandeur. Une fois saisie, elle fait l'objet d'un processus de validation par l'opérateur ayant effectué la saisie. Si la demande ne devait pas être validée, le RC serait informé des causes du rejet.

Si la demande est acceptée, le RC est informé de cet état et reçoit le certificat.

4.2.3 Durée d'établissement du certificat

Le certificat est généré quelques instants après la validation de la demande par l'Opérateur d'Enregistrement.

4.3 DELIVRANCE DU CERTIFICAT

4.3.1 Actions de l'AC concernant la délivrance du certificat

La validation de la demande déclenche l'opération technique de génération du certificat. Celle-ci contient les actions suivantes :

- signature par l'AC TECHNIQUE de la demande de certificat ;
- récupération par l'Opérateur d'Enregistrement du certificat généré ;
- transmission par courriel du certificat à l'adresse email du RC.

4.3.2 Notification par l'AC de la délivrance du certificat

À l'issue de la phase de validation par l'Opérateur d'Enregistrement, le courriel contenant le certificat récupéré est transmis au RC. Si ce dernier dispose des éléments lui permettant de consulter ses emails, il peut s'assurer de la réception du certificat en présence de l'Opérateur d'Enregistrement.

4.4 ACCEPTATION DU CERTIFICAT

4.4.1 Démarche d'acceptation du certificat

Le RC est amené à valider le contenu du certificat d'horodatage lors de sa mise en œuvre.

4.4.2 Publication du certificat

Les certificats finaux ne sont pas publiés.

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

Sans objet.

4.5 USAGE DE LA BI-CLE ET DU CERTIFICAT

4.5.1 Usage de la clé privée

4.5.1.1 Clé privée de l'AC TECHNIQUE

La clé privée de l'AC TECHNIQUE est utilisée pour :

- signer les certificats finaux ;
- signer les LCR ;
- signer les réponses OCSP.

Ces usages sont explicitement définis dans les extensions des certificats en positionnant les valeurs suivantes dans le champ « KeyUsage » :

- keyCertSign ;
- CRLSign ;
- digitalSignature.

4.5.1.2 Clé privée des certificats finaux

Les usages des certificats finaux sont explicitement définis dans le champ « KeyUsage » et dépendent du profil :

- certificat d'horodatage : digitalSignature ;
- certificat OSCP : digitalSignature.

4.5.2 Usage de la clé publique et du certificat

4.5.2.1 Clé publique et certificat de l'AC TECHNIQUE

Les certificats de l'AC opérationnelle émis par l'AC TECHNIQUE sont destinés à :

- valider les certificats finaux ;
- valider la LCR ;
- valider les réponses OCSP, le cas échéant.

4.5.2.2 Clé publique des certificats finaux

L'utilisation du certificat et de la clé publique associée est limitée aux conditions d'usages définies dans la présente PC (voir § 1.4) et à l'usage prévu indiqué dans le certificat (attribut key usage et/ou extended key usage).

Le RC est tenu de vérifier la validité du certificat et la conformité de son utilisation.

4.6 RENOUELEMENT D'UN CERTIFICAT

Le renouvellement de certificat, au sens de la [RFC 3647], correspondant à la seule modification des dates de validité, n'est pas permis par la présente PC. Seule la délivrance d'un nouveau certificat suite au 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 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE AU CHANGEMENT DE LA BI-CLE

Conformément à la [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat lié à la génération d'une nouvelle bi-clé.

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques.

Les bi-clés et les certificats correspondants de l'AC TECHNIQUE sont renouvelés au minimum tous les 10 ans.

Les bi-clés et les certificats correspondants des certificats finaux sont renouvelés au minimum tous les 3 ans.

Dans certains cas, un certificat peut être renouvelé par anticipation : révocation du certificat, changement de paramètres cryptographiques, cessation d'activité de l'Autorité de Certification.

4.7.2 Origine d'une demande d'un nouveau certificat

La demande de certificat est toujours faite par le Mandataire de Certification ou le Responsable de Certificat de personne morale. Ce dernier se rapproche de la DIRECTION DES SERVICES NUMÉRIQUES pour connaître les modalités de dépôt de sa demande et notamment les éléments à fournir dans son dossier de demande.

Si la demande de nouveau certificat fait suite à une révocation, l'origine de la demande est le RC, le Représentant légal, le Responsable de Certificat de personne morale, le Mandataire de Certification ou l'Autorité d'Enregistrement.

Dans le cas d'une demande de nouveau certificat suite à une révocation, le processus est identique à la demande initiale.

Si la demande de nouveau certificat se fait dans le cadre d'une demande de renouvellement du certificat, l'origine de la demande est le Responsable de Certificat de personne morale.

Le RC peut anticiper la fin de vie de son (ses) certificat(s), préparer sa nouvelle demande selon le processus décrit au paragraphe §4.1 et solliciter un rendez-vous auprès de l'AE à l'adresse de courriel donnée au paragraphe §1.5.2.

S'il passe le délai d'expiration du certificat, il devra, quoi qu'il en soit, effectuer une nouvelle demande.

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

La procédure de traitement d'une demande de nouveau certificat est la suivante. Le Responsable du Certificat :

- reçoit les notifications de l'AE indiquant l'expiration proche des certificats ;
- se rapproche de la DIRECTION DES SERVICES NUMÉRIQUES pour s'assurer de l'évolution éventuelle des modalités de dépôt de sa demande et connaître notamment les éléments à fournir dans son dossier de demande ;
- sollicite un rendez-vous par courriel auprès de l'AE pour une remise en face-à-face du nouveau certificat ;
- l'AE se base sur le dossier d'enregistrement fourni pour l'identification et la validation de la demande de renouvellement.

4.7.4 Notification au RC de l'établissement du nouveau certificat

La procédure est identique à la demande initiale. Voir chapitre 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

La procédure est identique à la demande initiale. Voir chapitre 4.4.1.

4.7.6 Publication du nouveau certificat

La procédure est identique à la demande initiale. Voir chapitre 4.4.2.

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

La procédure est identique à la demande initiale. Voir chapitre 4.4.3.

4.8 MODIFICATION DU CERTIFICAT

Aucune modification ne peut être effectuée. Le certificat doit être révoqué et un nouveau doit être généré.

4.8.1 Causes possibles de modification d'un certificat

Sans objet.

4.8.2 Origine d'une demande de modification d'un certificat

Sans objet.

4.8.3 Procédure de traitement d'une demande de modification d'un 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 REVOCATION ET SUSPENSION DES CERTIFICATS

4.9.1 Causes possibles d'une révocation

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat objet de la présente PC :

- la clé privée du certificat est perdue, volée, inutilisable (dysfonctionnement du support), compromise ou suspectée de compromission (demande du Responsable de Certificat lui-même) ;
- les informations ou les attributs figurant dans le certificat ne sont plus valides ou plus en cohérence avec l'utilisation prévue du certificat, ceci avant l'expiration normale du certificat ;
- les algorithmes cryptographiques mis en œuvre sont obsolètes ;
- les algorithmes cryptographiques mis en œuvre ne sont plus considérés sûrs ;
- une vulnérabilité de type zéro-jour est découverte ;
- il a été démontré que le Responsable de Certificat n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le certificat d'AC est révoqué (ce qui entraîne la révocation des certificats signés par la clé privée correspondante) ;
- le RC ne satisfait plus aux conditions professionnelles requises (cessation d'activité, décès) ;
- le changement d'adresse de courriel du Responsable du Certificat dans le cas où cette adresse est renseignée dans le certificat ;

- le certificat de personne morale¹ n'est plus rattaché à un Responsable de Certificat (décès, départ, changement de fonction, etc.).

Les causes de révocation ne sont jamais publiées.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours de l'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

4.9.2 Origine d'une demande de révocation

Une demande de révocation de certificat ne peut émaner que :

- du Responsable de Certificat ;
- du Mandataire de Certification ;
- de l'Autorité d'Enregistrement ayant validé l'émission du certificat ;
- du Responsable du C2SC ;
- du Représentant légal ;
- de l'Officier de Sécurité de l'ICN ;
- du Responsable de l'AC.

Dans le cas où, au travers d'une décision de justice, une révocation est imposée par les autorités judiciaires, la demande de révocation ne peut émaner que de l'une des personnes susmentionnées.

4.9.3 Procédure de traitement d'une demande de révocation

Une demande de révocation de certificat est réceptionnée par l'AC à l'adresse :

service-horodatage@gouv.mc

Elle doit au moins contenir les informations suivantes :

- le nom associé au certificat à révoquer (a minima le CN accompagné, si nécessaire, du SN) ;
- le nom et la qualité du demandeur de la révocation ;
- la cause de révocation.

4.9.3.1 Procédure de révocation par le RC

Le processus de révocation par le RC est le suivant :

- le Responsable de Certificat contacte par e-mail la DIRECTION DES SERVICES NUMÉRIQUES ;
- l'opérateur AE contacte en retour le demandeur par téléphone dans les 24h ;
- le RC fournit son code de révocation ;
- l'opérateur AE se connecte à l'interface de gestion ;
- il s'authentifie à l'aide de son certificat ;
- il recherche le certificat d'horodatage à l'aide des informations communiquées ;
- il sélectionne le certificat à révoquer ainsi qu'un motif de révocation et envoie la demande de révocation ;
- l'AC procède à la révocation ;
- le numéro de série du certificat révoqué apparaîtra dans la prochaine LCR publiée ;
- le RC reçoit par courriel une notification de la révocation ;
- l'opération est enregistrée dans les journaux d'événements.

¹ Ce cas de figure se présente lorsque, pour une raison particulière, le Représentant légal de la personne morale n'a pas nommé de nouveau Responsable de Certificat en cas de changement.

4.9.3.2 Procédure de révocation par l'AE ou l'Officier de Sécurité de l'ICN

Le processus de révocation par l'AE ou l'Officier de Sécurité de l'ICN est le suivant :

- l'opérateur AE se connecte à l'interface de gestion ;
- il s'authentifie à l'aide de son certificat issu de l'AC SERVICES ADMINISTRATIFS ;
- il recherche le certificat d'horodatage à l'aide des informations communiquées ;
- il sélectionne le certificat à révoquer ainsi qu'un motif de révocation et envoie la demande de révocation ;
- l'AC procède à la révocation ;
- le numéro de série du certificat révoqué apparaîtra dans la prochaine LCR publiée ;
- le RC reçoit par courriel une notification de la révocation ;
- l'opération est enregistrée dans les journaux d'événements.

Le Responsable d'AC, respectivement le Responsable du C2SC ou une autorité judiciaire, peuvent saisir par courrier officiel l'Opérateur d'Enregistrement de l'AE, respectivement l'Officier de Sécurité de l'ICN, pour effectuer l'opération de révocation.

4.9.3.3 Procédure de révocation en l'absence du code de révocation

Le Responsable de Certificat peut avoir perdu son code de révocation. Le Représentant légal voire le Mandataire de Certification peuvent vouloir, pour des raisons légitimes, révoquer un certificat (licenciement, départ, départ en retraite, maladie, etc.).

Dans ce cas, le demandeur, qu'il soit le Responsable de Certificat de personne morale, le Représentant légal ou le Mandataire de Certification, contacte par e-mail la DIRECTION DES SERVICES NUMÉRIQUES. L'AE contacte en retour le demandeur par téléphone dans les 24h.

L'authentification de la personne par téléphone se fait par le biais des réponses aux 4 questions personnelles (parmi les 7) que le demandeur aura renseignées lors du dépôt de son dossier d'enregistrement.

4.9.4 Délai accordé pour formuler la demande de révocation

La demande de révocation doit être formulée dès connaissance de l'évènement correspondant.

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

La fonction de gestion des révocations est disponible 24 heures sur 24, 7 jours sur 7.

Les demandes de révocation sont, quant à elles, traitées dans les 24h suivant la réception de la demande.

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

L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état de la chaîne de certificats correspondante jusqu'au certificat de l'AC. Il pourra utiliser, à cette fin, le dernier statut de révocation publié.

Les utilisateurs des certificats doivent notamment vérifier la non-révocation des certificats sur lesquels ils vont baser leur confiance. Cette vérification se fait en consultant les LCR disponibles, ou en interrogeant le service en ligne d'état des certificats (OCSP) qui intègre une réponse « certificat révoqué » après la date de fin de vie du certificat. Les certificats révoqués restent présents dans la LCR même après leur date d'expiration d'origine.

4.9.7 Fréquence d'établissement des LCR

Le service d'état des certificats publie une mise à jour quotidienne des LCR. Chaque LCR contient la date et l'heure prévisionnelles de publication de la LCR suivante.

Par mesure de sécurité, les LCR ont une durée de validité de 5 jours.

4.9.8 Délai maximum de publication des LCR

Le délai maximum de publication d'une LCR après sa génération est de 30 minutes.

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

Un système de vérification en ligne (OCSP) est mis en œuvre et répond aux mêmes exigences de sécurité, notamment en termes de disponibilité, que le système de publication des LCR.

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 ou de vulnérabilité zéro-jour

En cas de compromission de la clé privée de l'AC TECHNIQUE, ou dans le cadre de la publication d'une vulnérabilité de type zéro-jour, le C2SC déclenche une réunion de crise et prend les mesures suivantes :

- diffusion auprès des parties prenantes et sur son site de publication de la compromission ;
- alerte sur le fait de ne plus faire confiance aux certificats de la chaîne d'AC concernée ;
- organisation d'une cérémonie des clés pour :
 - si la compromission concerne les clés de l'AC opérationnelle :
 - révoquer l'ensemble des certificats finaux émis par l'AC opérationnelle,
 - publier une nouvelle et dernière LCR pour cette AC opérationnelle,
 - révoquer le certificat de l'AC opérationnelle,
 - réémettre les LAR pré-générées,
 - détruire toutes les anciennes LAR qui avaient été pré-générées,
 - publier la nouvelle LAR en cours de validité,
 - détruire la clé privée de l'AC opérationnelle,
 - si la compromission concerne un certificat final :
 - révoquer le certificat concerné,
 - suivant les circonstances, une publication manuelle d'une nouvelle LCR pourra être déclenchée en faisant une demande auprès de l'Opérateur Technique,
 - analyse de la compromission,
 - si le Responsable de Certificat doit disposer d'un nouveau certificat, le processus initial de délivrance sera alors réalisé et il devra alors faire une nouvelle demande de certificat.

4.9.13 Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC.

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'ETAT DES CERTIFICATS

4.10.1 Caractéristiques opérationnelles

L'AMSN fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR comme des LAR et l'état du certificat de l'AC. Les LCR et les LAR sont publiées à l'adresse spécifiée au chapitre 2.2, et à l'adresse contenue dans les certificats émis

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24h, 7j/7j. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4h et un taux de disponibilité annuel de 99,95%.

4.10.3 Dispositifs optionnels

La présente PC ne formule pas d'exigence spécifique sur le sujet.

4.11 FIN DE LA RELATION AVEC L'AC TECHNIQUE

En cas de fin de relation contractuelle / hiérarchique / réglementaire avec l'AC TECHNIQUE avant la fin de validité du certificat, pour une raison ou pour une autre, le C2SC se réunit et statue sur une des deux possibilités suivantes :

- le certificat de l'AC opérationnelle et les certificats finaux émis par cette AC doivent obligatoirement être révoqués. Une dernière LCR est alors produite pour cette AC opérationnelle et de nouvelles LAR seront pré-générées incluant le numéro de série de cette AC opérationnelle ;
- l'AC opérationnelle n'est pas révoquée, et son certificat reste valide jusqu'à sa fin de vie. Le service est alors transféré.

4.12 SEQUESTRE DE CLE ET RECOUVREMENT

Les clés privées des AC ne sont pas séquestrées. Les clés privées des certificats finaux ne sont pas séquestrées.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

5 MESURES DE SECURITE NON TECHNIQUES

5.1 MESURES DE SECURITE 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. Les environnements de l'AMSN sont installés sur des sites sécurisés de production informatique.

L'hébergement de l'IGC est réparti entre deux sites dont un principal et un secondaire dédié au secours et à la reprise d'activité localisé sur le territoire monégasque. Il n'existe pas de risque géographique particulier pour le site principal ni pour le site de secours, ces derniers ne sont pas situés à proximité d'un quelconque site à risque ni en zone inondable. La gestion de ce type de risque est contractuellement sous la responsabilité du bailleur.

5.1.2 Accès physique

Les salles d'hébergement bénéficient d'un niveau de sécurité physique double. L'accès physique au site se fait nécessairement avec l'accompagnement d'une personne autorisée de l'AMSN.

Les accès physiques aux zones d'hébergement de l'IGC font l'objet de journalisation et de vidéo-surveillance : le périmètre de sécurité défini autour des machines hébergeant les composantes de l'IGC n'est accessible qu'aux personnes disposant d'un rôle de confiance.

En dehors des heures ouvrables, la mise en œuvre de moyens de détection d'intrusion physique et logique renforce la sécurité de l'IGC.

5.1.3 Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre 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 Vulnérabilité aux dégâts des eaux

La définition du périmètre de sécurité prend en considération les risques inhérents aux dégâts des eaux. Des moyens de protection sont mis en œuvre pour parer les risques résiduels (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, pour un même niveau de sensibilité.

5.1.8 Sauvegardes hors site

Des sauvegardes externalisées sont mises en œuvre et organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conformément aux engagements de la présente PC notamment en matière de disponibilité et de protection en confidentialité et en intégrité des informations sauvegardées. Les supports de sauvegarde font l'objet d'une mise sous coffre hors site plusieurs fois par an.

5.2 MESURES DE SECURITE PROCEDURALES

5.2.1 Rôles de confiance

L'AMSN définit explicitement les rôles de confiance requis pour assurer le fonctionnement et la sécurité de ses services. Les définitions des rôles de confiance sont rendues disponibles à l'ensemble des personnels concernés.

L'AC définit les rôles de confiance suivants :

- Responsable d'AC :
 - Il s'agit du responsable de la Direction Métier en charge des services numériques pour le compte de l'État ;
- Administrateur IGC :
 - Ce rôle est délégué à une ou plusieurs personnes formellement identifiées chez l'Opérateur Technique en relation contractuelle avec l'AMSN. L'administrateur IGC est en charge de gérer l'IGC pour le compte de l'Administration ;
- Administrateur système :
 - Ce rôle est délégué à une ou plusieurs personnes formellement identifiées chez l'Opérateur Technique en relation contractuelle avec l'AMSN ;
- Administrateur sécurité :
 - Ce rôle est délégué à une ou plusieurs personnes formellement identifiées chez l'Opérateur Technique en relation contractuelle avec l'AMSN. L'administrateur sécurité est en charge d'assurer le maintien de l'IGC en condition de sécurité. Il doit appliquer les correctifs nécessaires, piloter les audits techniques de sécurité ;
- Exploitant / superviseur :
 - Ce rôle est délégué à une ou plusieurs personnes formellement identifiées chez l'Opérateur Technique en relation contractuelle avec l'AMSN. L'exploitant / superviseur est en charge d'assurer le maintien des fonctions de l'IGC en condition opérationnelle ;
- Auditeur système :
 - Ce rôle est partagé entre des personnels formellement identifiés au sein du Gouvernement Princier et des personnels chez l'Opérateur Technique en relation contractuelle avec l'Administration. Le rôle de l'auditeur système est de pouvoir accéder aux configurations et aux traces des composants de l'IGC en lecture seulement pour détecter des incidents de sécurité ou des vulnérabilités.

En sus de ces rôles de confiance opérationnels, l'AC identifie les porteurs de secrets qui disposent d'une part des secrets de l'AC répartis selon l'algorithme de SHAMIR avec un quorum de 3 parmi 5. La répartition des secrets et de leurs porteurs de l'ICN ainsi que leur suivi sont confiés à l'AMSN.

5.2.2 Nombre de personnes requises par tâche

Selon le type d'opération effectuée, le nombre et les rôles des personnes devant être présentes, en tant qu'acteurs ou témoins, peuvent varier. En effet, certaines tâches sensibles, telles que la génération du certificat d'une AC, nécessitent plus d'une personne occupant un rôle de confiance au sein de l'ICN pour des raisons de sécurité. Certains rôles de confiance sont occupés par plusieurs personnes pour permettre à l'AMSN d'assurer la continuité des services de l'ICN sans dégrader la sécurité des services offerts.

5.2.3 Identification et authentification pour chaque rôle

Chaque personnel en rôle de confiance est clairement identifié par l'AC au travers d'un inventaire des rôles.

Chaque entité opérant une composante d'un service de confiance vérifie, pour chacun de ses composants, l'identité et les autorisations de tout membre du personnel ainsi que d'éventuelles personnes extérieures intervenant sur les tâches sensibles.

Avant d'utiliser une application critique contribuant à un service de confiance, tout personnel est obligatoirement identifié et authentifié au préalable. Toutes les opérations réalisées sur les systèmes par les personnels font l'objet d'une traçabilité garantissant l'imputabilité des actions. Chaque attribution d'un rôle de confiance à un membre du personnel est notifiée et documentée par écrit.

Les rôles de confiance assurés par l'Opérateur Technique sont établis concrètement et acceptés formellement par les personnes ayant ces rôles. L'Opérateur Technique tient à jour l'inventaire et le produit à l'Administration sur simple demande dans les 48h suivant la demande en jours ouvrés.

5.2.4 Rôles exigeant une séparation des attributions

Il est autorisé par la présente politique que plusieurs rôles soient opérés par une même personne. Cependant, pour des raisons de sécurité, certains rôles ne peuvent pas être opérés par la même personne. De façon générale, les rôles et responsabilités sont attribués sur le principe du moindre privilège afin de limiter le risque de conflit d'intérêts et limiter les opportunités de réalisation d'actions non autorisées ou de mauvaise utilisation des biens mis en œuvre par le service de confiance.

Le rôle d'auditeur système ne peut pas être cumulé.

Le rôle d'« exploitant / superviseur » peut être cumulé avec celui d'« Administrateur système ».

5.3 MESURES DE SECURITE VIS-A-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. Les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles. Le personnel d'encadrement possède l'expertise appropriée, et est familier des procédures de sécurité. Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités (description de poste), et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 Procédures de vérification des antécédents

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

L'AC peut demander à cet effet la production d'une copie du bulletin n°3 de leur casier judiciaire. Ces vérifications sont effectuées préalablement à l'affectation à un rôle de confiance et revues au minimum tous les 3 ans.

5.3.3 Exigences en matière de formation initiale

Le personnel est formé en tant que de besoin aux logiciels, matériels et procédures de fonctionnement de l'IGC.

5.3.4 Exigences et fréquence en matière de formation continue

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 rotation 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 la définition de poste ou la charte de sécurité du personnel pour les rôles sensibles tenus par le personnel 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.

Chaque prestataire transmet à l'ensemble de ses sous-traitants les règles de sécurité qui doivent être respectées dans le cadre de la mission qui leur est sous-traitée. Ces règles de sécurité font l'objet d'une acceptation formelle par les différents sous-traitants.

5.3.8 Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de leur prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans l'IGC disposent des procédures correspondantes. Les porteurs de rôles, appelés également rôles de confiance, signent dès leur prise de fonction une attestation dans laquelle ils reconnaissent avoir obtenu la formation nécessaire à la conduite de leur rôle.

Cette règle s'applique à l'ensemble des personnes intervenant sur l'IGC.

5.4 PROCEDURE DE CONSTITUTION DES DONNEES D'AUDIT

5.4.1 Types d'événements à enregistrer

L'AC collecte les éléments suivants :

- tous les événements relatifs à la sécurité, en particulier :
 - les changements de politique de sécurité des systèmes ;
 - les démarrages et arrêts des systèmes ;
 - les pannes matérielles et logicielles ;
 - les tentatives d'accès au système IGC.
 - l'activité des pare-feu et des systèmes de routage réseau ;
- tous les événements relatifs à l'enregistrement des demandes, en particulier :
 - la réception d'une demande de certificat (initiale et renouvellement) ;
 - la validation / le rejet d'une demande de certificat ;
 - les événements liés aux clés de signature et aux certificats d'AC (génération [cérémonie des clés], sauvegarde / récupération, révocation, renouvellement, destruction, etc.) ;
 - la génération des certificats ;
 - la publication et la mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
 - la réception d'une demande de révocation ;
 - la validation / le rejet d'une demande de révocation ;
 - la génération puis la publication des LAR et LCR.

5.4.2 Fréquence de traitement des journaux d'événements

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

5.4.3 Période de conservation des journaux d'événements

La période de conservation des journaux d'événement est :

- d'un mois pour les événements systèmes ;
- d'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'AC. Ils ne sont pas modifiables. 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 journaux font l'objet de sauvegardes régulières.

5.4.6 Système de collecte des journaux d'événements

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

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

Sans objet.

5.4.8 Évaluation des vulnérabilités

L'AMSN et l'Opérateur Technique opèrent une veille constante sur les vulnérabilités pouvant impacter les produits mis en œuvre dans le cadre de l'ICN.

Cette veille concerne les vulnérabilités applicatives, les vulnérabilités liées à l'IGC mais également les vulnérabilités pouvant impacter les équipements de sécurité mis en œuvre ou encore les logiciels utilisés par chaque collaborateur. Les algorithmes utilisés dans le cadre de l'ICN font notamment partie de la veille opérée.

Des tests d'intrusion sont conduits régulièrement pour l'ensemble des produits de l'IGC par un auditeur externe selon une méthodologie rigoureuse. Ces tests, menés sur un environnement de pré-production sont dits « applicatifs » mais concernent également la partie infrastructure.

5.5 ARCHIVAGE DES DONNEES

Des dispositions en matière d'archivage sont mises en place par l'AC. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

5.5.1 Types de données à archiver

Les données à archiver sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC et DPC publiques, le cas échéant ;
- les versions confidentielles des DPC ;
- les certificats émis ;
- les LAR et LCR émises ou publiées ;
- les différents engagements signés par l'AMSN (contrat avec l'Opérateur Technique par exemple) ;
- les journaux d'évènements des différentes entités de l'IGC (voir 5.4).

5.5.2 Période de conservation des archives

Les durées de conservation suivantes sont respectées :

| | |
|------------------------------|--|
| logiciels | version en cours et version précédente |
| configurations des logiciels | version en cours et version précédente |
| certificats d'AC | 7 ans après la date d'expiration du certificat |
| LCR | 7 ans après la date d'expiration du certificat |
| certificats finaux | 7 ans après la date d'expiration du certificat |
| requêtes et réponses OCSP | Aucune donnée conservée |
| événements techniques | 1 an |
| événements fonctionnels | durée de conservation identique à celle du certificat d'AC correspondant |
| documentation | 10 ans après la fin de vie de la version concernée |
| dossier d'enregistrement | 10 ans après le dépôt |

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.

5.5.4 Procédure de sauvegarde des archives

Les archives sont sauvegardées de manière sécurisée, et accessibles uniquement aux seules personnes autorisées. L'archivage des dossiers d'enregistrement est à la charge de l'AC. Le reste relève du périmètre de responsabilité de l'AMSN et la DSN, chacune en ce qui la concerne.

5.5.5 Exigences d'horodatage des données

L'ensemble des composants de l'IGC sont synchronisés à une source de temps de référence. Cette source de temps est synchronisée avec UTC au moins une fois par jour.

5.5.6 Système de collecte des archives

Sans objet.

5.5.7 Procédures de récupération et de vérification des archives

Les archives peuvent être restituées sur demande motivée à l'AC.

5.6 CHANGEMENT DE CLE D'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité du certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.

Au regard de la date de fin de validité de ce certificat, son renouvellement sera demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée sera utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 REPRISE SUITE A LA COMPROMISSION ET SINISTRE

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

Des procédures (sensibilisation, formation des personnels notamment) et des moyens de remontée et de traitement des incidents (analyse des différents journaux d'événements notamment) sont mis en œuvre. En particulier, les anomalies sont remontées automatiquement à une cellule de veille.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de l'IGC.

Le responsable du C2SC doit en être informé immédiatement. Il devra alors traiter l'anomalie. S'il estime que l'incident a un niveau de gravité important, il demandera une révocation immédiate du certificat. Si celle-ci a lieu, il fera publier l'information de révocation du certificat dans la plus grande urgence, voire immédiatement. Il le fera via l'ouverture d'un incident de priorité maximale et via une notification par courrier électronique à l'ensemble des services utilisant les certificats émis par l'AC.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors le responsable du C2SC fera publier l'information via l'ouverture d'un incident et notifiera par courrier électronique l'ensemble des services utilisant les certificats émis par l'AC. Tous les certificats concernés seront alors révoqués suivant un planning établi le cas échéant.

Par ailleurs, l'AC notifiera la personne morale à laquelle un service de confiance a été fourni, sans retard excessif, dès lors qu'une violation de la sécurité ou une perte d'intégrité est susceptible de lui porter atteinte.

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

Si le matériel de l'AC est endommagé ou hors service alors que les clés de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des services de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC.

En cas de destruction du matériel, l'Opérateur Technique remplace le matériel défectueux et transmet une copie du procès-verbal de destruction à l'AMSN.

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

La procédure prévoit notamment à partir de la réception du rapport de suspicion de compromission ou de compromission (source d'information interne ou externe à l'AC) :

- prise en compte du rapport,
- réunion du C2SC et information des intéressés (internes à l'AC),
- identification de la procédure à appliquer,
- mise en œuvre de la procédure à appliquer,
- information des tiers intéressés.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Le PRA est testé annuellement.

5.7.5 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'Officier de Sécurité de l'ICN se tiennent continuellement informés des cas de compromission des éléments susmentionnés.

En cas de prise de connaissance d'une compromission d'un algorithme ou d'un paramètre associé, impactant les certificats des AC ou les certificats clients, l'AC et l'Officier de Sécurité de l'ICN informent le C2SC qui déclenche une cellule de crise afin de déterminer les actions à mener pour rétablir le service au plus vite.

Par mesure de précaution, l'Officier de Sécurité de l'ICN demande :

- aux différents responsables d'AC d'imposer à leur(s) AE l'arrêt immédiat du service de délivrance des certificats et ce, jusqu'à nouvel ordre émanant du C2SC ;
- au responsable de l'AC et au Directeur des Services Numériques d'informer au travers de leurs portails respectifs les utilisateurs disposant de certificat(s) émis par l'AC.

5.8 FIN DE VIE DE L'AC

L'AC dispose d'un plan d'arrêt d'activité. Elle s'engage à maintenir publiés, directement par ses propres moyens ou via une prestation externalisée, les éléments relatifs au service de publication indiqué au paragraphe §2.2.

L'AC peut être amenée à cesser son activité ou à la transférer en tout ou partie à un autre prestataire de service de confiance pour diverses raisons. Elle prend alors toutes dispositions pour couvrir les coûts lui permettant de respecter ses engagements.

Le transfert d'activité est défini comme la fin d'activité de l'AC sans pour autant qu'il n'y ait d'incidence sur la validité des certificats émis antérieurement et sur la reprise de l'activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité de l'AC avec une incidence sur la validité des certificats émis antérieurement.

L'AC assure ses fonctions directement ou en les déléguant en tout ou partie à travers, par exemple, de la sous-traitance. Dans tous les cas, elle en conserve la responsabilité vis-à-vis de ses parties prenantes (utilisateurs, porteurs, etc.). Dans le cadre de la fin de vie de l'AC, le responsable de l'AC met fin à toute autorisation de ses sous-traitants en lien avec l'émission des services de confiance, d'agir pour son compte.

5.8.1 Transfert ou cessation d'activité affectant l'AC

Afin d'assurer un niveau de confiance constant pendant et après un transfert ou une cessation, l'AC :

- met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment des informations relatives aux certificats),
- assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC,
- communique à l'Officier de Sécurité de l'ICN 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,
- présente 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 la PC,
- communique à l'AMSN les modalités des changements survenus,
- en mesure l'impact et fait l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, en termes de communication, etc.),
- présente un plan d'action destiné, dans le meilleur des cas à supprimer, sinon réduire, le risque pour les applications et la gêne pour les porteurs et, d'une manière plus générale, les utilisateurs de certificats,
- tient informée l'AMSN de tout obstacle rencontré ou délai supplémentaire nécessaire dans le déroulement du processus.

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou, d'une manière plus générale, des utilisateurs de certificats, l'AC les en avise aussitôt que possible et, a minima, à travers le portail **M CONNECT** dans le délai d'1 (un) mois avant le transfert ou la cessation d'activité.

5.8.2 Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de sorte que les obligations visées paragraphe 5.8.1, à l'exception de la dernière, soient à exécuter par l'AC ou l'entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR voire des LAR conformément aux engagements pris dans sa PC.

L'AC stipule dans ses pratiques les dispositions prises en cas de cessation de service. Elles incluent :

- la notification des entités affectées,
- le transfert de ses obligations à d'autres parties,
- la gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC :

- s'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats,
- prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante,
- révoque son certificat,
- révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité,
- informe tous les porteurs des certificats révoqués ou à révoquer,
- une dernière CRL est émise avec une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« 99991231235959Z »).

6 MESURES DE SECURITE TECHNIQUES

6.1 GENERATION ET INSTALLATION DE BI-CLES

6.1.1 Génération des bi-clés

6.1.1.1 Clé des AC opérationnelles

Cérémonie des clés

La cérémonie de génération des clés se déroule en présence d'un représentant du C2SC et suivant la procédure du maître de cérémonie.

Module cryptographique

Les clés associées aux certificats émis par l'AC sont obligatoirement générées et utilisées dans un module cryptographique ayant fait l'objet d'une qualification par l'ANSSI.

6.1.1.2 Clés des certificats d'horodatage

La clé privée doit être stockée sur un environnement cryptographique matériel de niveau CC EAL4+ ou FIPS 140-2 level 3.

6.1.2 Transmission de la clé privée à son propriétaire

Les clés privées d'AC sont directement générées dans le module cryptographique correspondant.

Dans le cas des certificats d'horodatage, la clé privée est générée dans l'environnement cryptographique matériel.

6.1.3 Transmission de la clé publique à l'AC

La clé publique d'une AC opérationnelle est transmise dans le cadre d'une cérémonie des clés via un support amovible transporté de manière sécurisée.

Dans le cas d'un certificat d'horodatage, soit la clé publique est :

- transmise à l'AC via un canal sécurisé sous la forme d'une demande technique de certificat (CSR). Cette demande est signée par la clé privée du certificat ;
- générée en central par l'Opérateur Technique et n'est donc pas transmise.

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

La clé publique d'une AC est enveloppée dans un certificat. Sa diffusion s'accompagne de l'empreinte numérique du certificat ainsi que d'une déclaration précisant qu'il s'agit bien d'une clé publique de l'AC. La clé publique d'une AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) pourront aisément être récupérées par les utilisateurs de certificats, via le site de publication (voir 2.2).

La clé publique d'un certificat final n'est pas diffusée aux applications utilisatrices.

6.1.5 Tailles des clés

Les clés d'AC ont les caractéristiques suivantes :

- algorithme utilisé : RSA
- taille minimale des clefs : 4096 bits

Les clés des certificats finaux ont les caractéristiques suivantes :

- algorithme utilisé : RSA
- taille minimale des clefs : 2048 bits

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

L'équipement de génération de bi-clés utilisé pour la génération des paramètres des bi-clés des AC est un module cryptographique configuré pour répondre à ces exigences. Les bi-clés ne peuvent être générées que sur un module conforme à cette exigence, ou d'un niveau cryptographique et sécuritaire supérieur.

6.1.7 Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de réponse OCSP et de LCR (voir chapitre 1.4.1).

L'utilisation d'une clé privée de certificat final et du certificat associé est limité aux usages définis au chapitre 1.4.1 et reste sous la responsabilité du RC. Il lui appartient donc de s'assurer que le certificat dont il dispose est bien utilisé dans les conditions d'usage prévues.

6.2 MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Standards pour les modules cryptographiques

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique sécurisé.

Il s'agit d'un module cryptographique Proteccio qualifié par l'ANSSI fourni par la société ATOS/BULL. Il s'agit d'un modèle HR.

6.2.1.2 Mesures de sécurité pour les supports cryptographiques des certificats finaux

Voir chapitre §6.1.1.2.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance (porteurs de secrets) et via un outil mettant en œuvre le partage des secrets. Il y a n porteurs de secrets pour chaque AC, qui se voient remettre ces secrets sur carte à puce lors de la cérémonie des clés. Un quorum de porteurs parmi les n porteurs est nécessaire pour activer la clé privée de l'AC.

Les clés privées des certificats d'horodatage sont sous le contrôle des Responsables de Certificat.

6.2.3 Séquestre de la clé privée

Sans objet.

6.2.4 Copie de secours de la clé privée

6.2.4.1 Clé privée des AC opérationnelles

Les clés privées des AC opérationnelles sont dupliquées sur le HSM présent sur le second site d'hébergement. Cette duplication se fait via une copie de secours qui est réalisée sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement utilisé offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuie sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique. Le contrôle des opérations de chiffrement / déchiffrement est conforme aux exigences du chapitre 6.2.2.

6.2.4.2 Clé privée des certificats finaux

Les clés privées des certificats finaux ne font pas l'objet d'une copie de secours.

6.2.5 Archivage de la clé privée

Sans objet.

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

Le transfert vers ou depuis le module cryptographique ne se fait que pour la génération des copies de sauvegardes. Ceci se fait sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

Les clés privées des certificats finaux stockées dans des environnements cryptographiques ne sont pas exportables.

6.2.7 Stockage de la clé privée dans un module cryptographique

Le stockage des clés privées d'AC est réalisé dans un module cryptographique répondant aux exigences du chapitre 6.2.1.

Le stockage des clés privées des certificats finaux est réalisé dans un module cryptographique répondant aux exigences du chapitre 6.2.1.

6.2.8 Méthode d'activation de la clé privée

L'activation des clés privées d'AC se fait dans un module cryptographique et est contrôlée via des données d'activation (voir chapitre 6.4).

Pour les clés sur des environnements HSM, plusieurs modes d'activation sont envisageables :

- un identifiant d'API partagé entre le HSM et l'application métier ;
- la fourniture d'une clé d'activation au moment du chargement de la clé dans le HSM et détenue par le Responsable de Certificat.

6.2.9 Méthode de désactivation de la clé privée

La clé privée d'une AC est désactivée après chaque opération cryptographique par arrêt électrique du module cryptographique.

Dans le cas de la clé privée correspondant à un certificat d'horodatage, s'agissant d'un environnement HSM, la clé privée est désactivée par arrêt électrique du boîtier.

6.2.10 Méthode de destruction des clés privées

La destruction définitive d'une clé privée d'AC ou d'une clé privée générée sur un boîtier HSM est réalisée par :

- la destruction de l'instance de la clé sur le module cryptographique, et
- la destruction des moyens de restauration de la clé privée :
 - la destruction de toutes les copies de secours de la clé privée, ou
 - la destruction des moyens d'activation de la clé privée.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de création de signature

Les modules cryptographiques répondent aux exigences du chapitre 6.2.1.

6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1 Archivage des clés publiques

Les clés publiques des AC ainsi que les clés publiques incluses dans les certificats émis sont archivées pour la période indiquée en 5.5.2.

6.3.2 Durées de vie des bi-clés et des certificats

6.3.2.1 Durées de vie des bi-clés et des certificats des AC opérationnelles

Les clés des AC opérationnelles et les certificats associés ont une durée de vie maximale de 10 ans.

6.3.2.2 Durées de vie des bi-clés et des certificats des certificats finaux

Les clés privées des certificats finaux ont une durée d'utilisation limitée à un an alors que les certificats associés ont une durée de vie maximale de 3 ans. L'objectif est de laisser deux ans pour valider les jetons d'horodatage et permettre ainsi de construire des formats de signature étendus.

6.4 DONNEES D'ACTIVATION

6.4.1 Génération et installation des données d'activation

Les éléments nécessaires à l'activation des clés privées des AC opérationnelles, sont générées de manière sécurisée, et uniquement accessibles aux seules personnes autorisées à procéder à cette activation.

Ces éléments sont générés dans le cadre de cérémonies des clés et remis à des porteurs de secrets.

Les données d'activation des clés privées des certificats d'horodatage sont personnalisées par le RC lui-même au moment de la génération du bi-clé sur l'environnement cryptographique.

6.4.2 Protection des données d'activation

Les parts de secrets des clés d'AC sont remises sur une carte à puce qui fait l'objet d'une mise sous enveloppe sécurisée.

Le RC a la responsabilité d'assurer la confidentialité des données d'activation du certificat d'horodatage.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 MESURES DE SECURITE DES SYSTEMES 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 réussie. Pour chaque interaction, le système établit l'identité de l'entité. Les informations d'authentification sont stockées de façon telle qu'elles sont seulement accessibles par des utilisateurs autorisés.

6.5.1.2 Contrôle d'accès

Les systèmes ne sont accessibles qu'aux personnes autorisées.

6.5.1.3 Administration et exploitation

L'utilisation de programmes utilitaires est restreinte et contrôlée. Les procédures opérationnelles d'administration et d'exploitation de l'AC sont documentées, suivies et régulièrement mises à jour. Les conditions de mise en service (paramétrage initial de sécurité des serveurs) sont documentées. Les conditions de fin de vie (destruction et mise au rebut) des équipements sont documentées afin de garantir la non-divulgaration des informations sensibles qu'ils peuvent détenir. L'ensemble des matériels sensibles de l'IGC font l'objet de procédure de maintenance afin de garantir la disponibilité des fonctions et des informations. 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 de l'IGC afin de fournir une protection contre les logiciels malveillants. Les composantes du réseau local sont maintenues dans un environnement physiquement sécurisé ; des vérifications périodiques de conformité de leur configuration sont effectuées.

6.5.1.5 Sécurité des flux

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

6.5.1.7 Supervision et contrôle

Une surveillance est mise en place afin de détecter, d'enregistrer et de réagir 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 personnes ayant un rôle de confiance au sein de l'IGC sont mises en œuvre.

6.5.2 Niveau de qualification des systèmes informatiques

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC est documentée. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau sont documentées et contrôlées.

6.6 MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES

6.6.1 Mesures liées à la gestion de la sécurité

Tous les développements réalisés par l'Opérateur Technique et impactant l'IGC sont documentés et réalisés de manière à en assurer la qualité. Les objectifs de sécurité sont définis lors des phases de spécification et de conception. Les systèmes et les produits utilisés sont fiables et sont protégés contre toute modification.

De plus, l'Opérateur Technique opère un cloisonnement entre les environnements de pré-production et de production. Ceci permet d'assurer une mise en production de qualité.

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

Toute évolution significative d'un système d'une composante de l'IGC est testée et validée avant déploiement. Ces opérations sont réalisées par du personnel de confiance.

6.7 MESURES DE SECURITE RESEAU

Pour les AC opérationnelles, des cloisonnements réseaux sont mis en œuvre pour assurer une séparation des flux, notamment les flux d'administration.

6.8 HORODATAGE / SYSTEME DE DATATION

Les AC opérationnelles sont synchronisées suivant les modalités évoquées au paragraphe 5.5.5.

7 PROFILS DE CERTIFICATS ET DES LCR

7.1 PROFIL DES CERTIFICATS

7.1.1 Certificats de l'AC TECHNIQUE

7.1.1.1 Champs de base du certificat

Le tableau suivant présente les champs de base :

| Champ | Valeur |
|--------------------------------|--|
| Version | 2 (pour version 3) |
| SerialNumber | 53:A6:8B:60:33:3E:81:A0:b9:AB:59:C5:B1:01:96:59 |
| Signature | Sha256WithRSAEncryption |
| Issuer | <ul style="list-style-type: none"> • CN=AC RACINE PRINCIPALTE DE MONACO • OU=0206 20A00001 • orgID=NTRMC-20A00001 • O=AMSN • C=MC |
| Subject | <ul style="list-style-type: none"> • CN=AC TECHNIQUE • OU=0206 20A00001 • orgID=NTRMC-20A00001 • O=AMSN • C=MC |
| Validity | <ul style="list-style-type: none"> • notBefore: Date de création • notAfter: notBefore + 10 ans |
| Subject Public Key Info | RSA 4096 bits |

Politique de Certification de l'AC TECHNIQUE

7.1.1.2 Extensions du certificat

Le tableau suivant présente les extensions :

| Champ | OID | Criticité | Valeur |
|---------------------------------------|-------------------|-----------|---|
| Authority Key Identifier | 2.5.29.35 | Non | 97:B0:7D:B6:FE:4B:A9:55:30:CF:EB:3B:87:7E:0E:66:3A:9C:3D:E9 |
| Subject Key Identifier | 2.5.29.14 | Non | 51:62:BB:6E:3A:B8:97:63:0A:50:38:46:BC:0B:45:D3:6D:8B:F0:9F |
| Key Usage | 2.5.29.15 | Oui | keyCertSign, CRLSign, digitalSignature |
| Basic Constraints | 2.5.29.19 | Oui | <ul style="list-style-type: none"> • CA:true • Maximum Path Length : absent |
| X509v3 Certificate Policies | 2.5.29.32 | Non | Policy: 2.16.492.1.1.1.1.6.1 |
| X509v3 CRL Distribution Points | 2.5.29.31 | Non | Full Name: <ul style="list-style-type: none"> • URI:http://icn.amsn.mc/icn/icn4096.crl • URI:http://icn.monaco.fr/icn/icn4096.crl |
| Authority Information Access | 1.3.6.1.5.5.7.1.1 | Non | CA Issuers - URI:https://icn.amsn.mc/icn/acr.crt |

7.1.2 Certificats finaux d'horodatage (environnement HSM non QSCD)

7.1.2.1 Champs de base du certificat

Le tableau suivant présente les champs de base :

| Champ | Valeur |
|--------------------------------|--|
| Version | 2 (pour version 3) |
| SerialNumber | Généré automatiquement |
| Signature | Sha256WithRSAEncryption |
| Issuer | <ul style="list-style-type: none"> • CN=AC TECHNIQUE • OU=0206 20A00001 • orgID=NTRMC-20A00001 • O=AMSN • C=MC |
| Subject | <ul style="list-style-type: none"> • serialNumber=<identifiant unique du certificat d'horodatage> • CN=HORODATAGE-MONACO <YY>TIMESTAMP-NNN² • Locality=MONACO <optionnel> • State=MONACO <optionnel> • OU=0206 21A00312 • orgID=NTRMC-21A00312 • O=DIRECTION DES SERVICES NUMERIQUES • C=MC |
| Validity | <ul style="list-style-type: none"> • notBefore: Date de création • notAfter: notBefore + 3 ans |
| Subject Public Key Info | RSA 2048 bits |

² Le CN doit être unique pour identifier de manière non équivoque chaque UH. Il porte à cette fin un compteur incrémental qui certifie cette unicité et débutant à 001.

Politique de Certification de l'AC TECHNIQUE

7.1.2.2 Extensions du certificat

Le tableau suivant présente les extensions :

| Champ | OID | Criticité | Valeur |
|---------------------------------------|-------------------|-----------|---|
| Authority Key Identifier | 2.5.29.35 | Non | 51:62:BB:6E:3A:B8:97:63:0A:50:38:46:BC:0B:45:D3:6D:8B:F0:9F |
| Subject Key Identifier | 2.5.29.14 | Non | [RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le certificat |
| Key Usage | 2.5.29.15 | Oui | Authentication : digitalSignature |
| Extended Key Usage | 2.5.29.37 | Oui | id-kp-timestamping |
| Basic Constraints | 2.5.29.19 | Non | <ul style="list-style-type: none"> • CA: false • Maximum Path Length : absent |
| X509v3 Certificate Policies | 2.5.29.32 | Non | Policy: 0.4.0.194112.1.1 qcpLegal Policy: 2.16.492.1.1.1.6.1 <ul style="list-style-type: none"> • CPS: https://mconnect.gouv.mc/technique Policy: 2.16.492.1.1.1.6.4.10.n ³ où n est le numéro de version |
| X509v3 CRL Distribution Points | 2.5.29.31 | Non | Full Name: <ul style="list-style-type: none"> • http://technique-icn.gouv.mc/crl/technique.crl • http://technique-icn.monaco.fr/crl/technique.crl |
| Subject Alternative Name | 2.5.29.17 | Non | [RFC822]=<optionnel><courriel du Responsable du certificat ou adresse générique de l'entité> |
| Authority Information Access | 1.3.6.1.5.5.7.1.1 | Non | CA Issuers - URI: https://icn.amsn.mc/icn/ac-technique.crt OCSP Issuers - URI: http://technique-oscpi.cn.gouv.mc |
| Private Key Usage Period | 2.5.29.16 | Non | id-ce-privateKeyUsagePeriod = 1 an |
| QCStatement | 1.3.6.1.5.5.7.1.3 | Non | id-etsi-qcs-QcCompliance id-etsi-qct-eseal QcEuPDS= https://mconnect.gouv.mc/technique |

³ Dans le cas de la présente PC, n=2.

7.2 LISTE DES CERTIFICATS REVOQUES

7.2.1 Champ de base

| Champ | Valeur |
|----------------------|---|
| Version | 1 (pour version 2) |
| Signature | SHA256WithRSA |
| Issuer | <ul style="list-style-type: none"> • CN=AC TECHNIQUE • OU=0206 20A00001 • orgID=NTRMC-20A00001 • O=AMSN • C=MC |
| Validity | 5 jours |
| Revoked Certificates | <ul style="list-style-type: none"> • Serial Number • Revocation Date |

7.2.2 Extensions

| Champ | Criticité | Valeur |
|--------------------------|-----------|---|
| Authority Key Identifier | non | 51:62:BB:6E:3A:B8:97:63:0A:50:38:46:BC:0B:45:D3:6D:8B:F0:9F |
| CRL Number | non | Défini par l'outil |
| ExpiredCertsOnCRL | non | True |

7.3 OCSP

7.3.1 Champ de base

| Champ | Valeur |
|--------------------------------|---|
| Version | 2 (pour version 3) |
| SerialNumber | Généré automatiquement |
| Signature | Sha256WithRSAEncryption |
| Issuer | <ul style="list-style-type: none"> • CN=AC TECHNIQUE • OU=0206 20A00001 • orgID=NTRMC-20A00001 • O=AMSN • C=MC |
| Subject | <ul style="list-style-type: none"> • CN=FQDN du serveur OSCP • OU=0206 20A00001 • orgID= NTRMC-20A00001 • O= AMSN • C=MC |
| Validity | <ul style="list-style-type: none"> • notBefore: Date de création • notAfter: notBefore + 3 ans |
| Subject Public Key Info | RSA 2048 bits |

7.3.2 Extensions

| Champ | OID | Criticité | Valeur |
|---------------------------------------|----------------------|-----------|---|
| Authority Key Identifier | 2.5.29.35 | Non | 51:62:BB:6E:3A:B8:97:63:0A:50:38:46:BC:0B:45:D3:6D:8B:F0:9F |
| Subject Key Identifier | 2.5.29.14 | Non | [RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat |
| Key Usage | 2.5.29.15 | Oui | Authentification : digitalSignature |
| Extended Key Usage | 2.5.29.37 | Non | id-kp-OCSPSigning |
| Basic Constraint | 2.5.29.19 | Non | <ul style="list-style-type: none"> • CA:false • Maximum Path Length : absent |
| X509v3 Certificate Policies | 2.5.29.32 | Non | Policy: 2.16.492.1.1.1.1.6.1 <ul style="list-style-type: none"> • CPS: https://mconnect.gouv.mc/technique Policy: 2.16.492.1.1.1.1.6.4.15.n ⁴ où n est le numéro de version |
| X509v3 CRL Distribution Points | 2.5.29.31 | Non | Full Name: <ul style="list-style-type: none"> • http://technique-icn.gouv.mc/crl/technique.crl • http://technique-icn.monaco.fr/crl/technique.crl |
| Subject Alternative Name | 2.5.29.17 | Non | [RFC822]=<optionnel><courriel du Responsable du certificat ocsps> |
| Authority Information Access | 1.3.6.1.5.5.7.1.1 | Non | CA Issuers - URI: https://icn.amsn.mc/icn/ac-technique.crt |
| ArchiveCutOff | 1.3.6.1.5.5.7.48.1.6 | Non | Date de début de validité du certificat d'AC |

⁴ Dans le cas de la présente PC, n=2.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Le présent chapitre ne concerne que les audits et évaluations de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

D'autres audits externes pourront être réalisés, notamment pour obtenir des certifications de conformité aux normes ETSI ou des qualifications de service de confiance dans le cadre du Référentiel Général de Sécurité de la Principauté annexé à l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance.

8.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Suite à toute modification significative d'une composante de l'IGC, l'AC procède à une analyse de sécurité et fait évoluer en conséquence, le cas échéant, les mesures techniques et organisationnelles permettant de maintenir ou d'améliorer le niveau de sécurité attendu.

L'AC procède également régulièrement à un contrôle de conformité de l'IGC, en tout ou partie. La fréquence de ce contrôle est réalisée a minima tous les 2 ans.

8.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

L'AC choisit et assigne une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité contrôlée.

8.3 RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'IGC, et être dûment autorisée à pratiquer les contrôles visés.

8.4 SUJETS COUVERTS PAR LES EVALUATIONS

Les audits de sécurité portent sur tout ou partie de l'IGC et visent à vérifier le respect des engagements et pratiques définies dans la présente PC et dans la DPC associée.

8.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

À l'issue d'un audit de sécurité, l'équipe d'audit rend à l'AC, un avis parmi les suivants :

- « réussite »,
- « échec »,
- « à confirmer ».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- en cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du Certificat de la composante, la révocation de l'ensemble des Certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes ;
- en cas de résultat « à confirmer », l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus ;
- en cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et de la DPC.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 TARIF

Le service de publication est gratuit au même titre que l'accès à l'information nécessaire à la constitution d'une demande de certificat ou à son utilisation.

En revanche, le tarif des certificats, en fonction de leur nature, est fixé par arrêté ministériel consultable en ligne sur le Journal de Monaco.

9.2 RESPONSABILITE FINANCIERE

9.2.1 Couverture par les assurances

Pour faire face à ses obligations, l'AC a souscrit une police d'assurance pour couvrir, éventuellement financièrement, ses responsabilités liées à ses opérations et/ou activités.

9.2.2 Autres ressources

Sans objet.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Pas d'exigences spécifiques.

9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1 Périmètre des informations confidentielles

Sur le périmètre de la présente PC, les informations suivantes sont considérées comme confidentielles :

- la partie non publique de la DPC, le cas échéant ;
- les clés privées de l'AC ;
- les données d'activation associées aux clés privées d'AC ;
- tous les secrets de l'IGC ;
- les journaux d'événements des composantes de l'IGC ;
- les formulaires de demande de génération et de révocation d'AC ;
- les causes de révocation.

9.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3 Responsabilités en termes de protection des informations confidentielles

De manière générale, les informations confidentielles ne sont accessibles qu'aux personnes concernées par de telles informations ou qui ont l'obligation de conserver et/ou traiter de telles informations. L'AC s'engage à traiter les informations confidentielles recueillies dans le respect des lois et règlements en vigueur.

9.4 PROTECTION DES DONNEES 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.

9.4.2 Informations à caractère personnel

Les informations à caractère personnel sont les informations nominatives du Mandataire de Certification, du Responsable de Certificat de personne morale, du Représentant légal enregistrées au sein du dossier d'enregistrement. Il s'agit notamment des informations nom / prénom / courriel / numéro de téléphone / numéro de série, / etc., ainsi que des motifs de révocation.

9.4.3 Responsabilité en termes de protection des données personnelles

Toute collecte de données à caractère personnel par l'AC est réalisée dans le strict respect de la législation et de la réglementation en vigueur.

9.4.4 Notification et consentement d'utilisation des données personnelles

Le RC est averti que la signature des Conditions Générales d'Utilisation emporte son consentement à l'utilisation de ses données personnelles.

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

Les enregistrements peuvent être mis à disposition aux autorités en cas de réquisition judiciaire.

9.4.6 Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

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

9.6 INDEPENDANCE DES PARTIES ET NON-DISCRIMINATION

L'organisation mise en place par l'AC est dédiée à ses activités et garantit l'étanchéité des rôles. Elle permet de préserver l'impartialité des opérations de génération et de révocation de certificats. Elle assure que les activités de confiance fournies sont pratiquées de façon équivalente pour l'ensemble des bénéficiaires ayant accepté les conditions générales d'utilisation du service et respectant les obligations qui leur incombent.

Dans toute la mesure du possible, l'AC met en œuvre des approches appropriées pour rendre son service accessible à toute personne y compris en situation de handicap, en prenant en compte au cas par cas les spécificités de chaque demandeur.

D'une manière générale, les services fournis par l'AC tels que, notamment, la génération de certificats, la gestion des révocations et le statut des certificats sont exercés de façon indépendante et ne sont donc soumis à aucune pression éventuelle.

9.7 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Les obligations communes aux composantes de l'IGC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (voir chapitre 7.3),
- respecter les accords ou contrats qui les lient entre elles,
- documenter leurs procédures internes de fonctionnement, mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.7.1 Autorités de Certification

Le C2SC est notamment responsable de :

- la validation et de la publication de la PC,
- la validation de la DPC, et de sa conformité à la PC,
- 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.

La DIRECTION DES SERVICES NUMÉRIQUES, en tant qu'AC, est responsable, sauf à démontrer qu'il n'a été commis aucune faute intentionnelle ou de négligence, des préjudices causés aux utilisateurs, si :

- les informations contenues dans le certificat ne correspondent pas aux informations d'enregistrement,
- l'AC n'a pas fait procéder à l'enregistrement de la révocation d'un certificat, et n'a pas publié cette information conformément à ses engagements.

9.7.2 Autorités d'enregistrement

Voir §1.3.2.

9.7.3 Porteur de certificat

Voir §1.3.3.

9.7.4 Responsable de Certificat de personne morale

Voir §1.3.5.3.

9.7.5 Utilisateurs de certificats

Voir §1.3.4.

9.7.6 Autres participants

Voir §1.3.5.1.

9.8 LIMITE DE GARANTIE

Sans objet.

9.9 LIMITE DE RESPONSABILITE

D'une manière générale, la responsabilité de l'AC Opérationnelle ne peut être engagée si elle respecte les dispositions prévues par la présente politique.

De fait, toute condition supplémentaire non portée dans ce document ne pourra être valablement considérée comme une obligation de l'AC.

Ainsi, l'AC Opérationnelle décline toute responsabilité :

- à l'égard d'une utilisation non autorisée ou non conforme des données d'authentification, des certificats, des LAR/LCR, ainsi que de tout autre équipement ou logiciel mis à disposition ;
- 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 ;
- conséquences des retards ou des pertes que pourraient subir dans leur transmission tout élément à destination de l'AC ou de l'une de ses composantes ; et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'article 1003 du Code civil.

En particulier, les dommages directs et indirects et notamment les pertes d'exploitation, dus à la révocation d'un certificat par l'AC, à un retard dans le renouvellement d'un certificat non imputable à l'AC, à un délai de traitement respectant les engagements décrits dans les présentes conditions, ne sauraient être retenus contre l'AC.

9.10 INDEMNITES

Sans objet.

9.11 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.11.1 Durée de validité

La PC doit rester en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.11.2 Fin anticipée de validité

Cette PC reste en application jusqu'à la publication d'une nouvelle version.

9.11.3 Effets de la fin de validité et clauses restant applicables

Sans objet.

9.12 AMENDEMENTS A LA PC

L'AC procède à toute modification des spécifications stipulées dans la PC et la DPC et/ou des composantes de l'AC qui lui apparaissent nécessaires pour l'amélioration de la qualité des services de Certification et de la sécurité des processus. L'AC procède également à toute modification des spécifications stipulées dans la PC et la DPC et/ou des composantes de l'AC qui est rendue nécessaire par une législation, réglementation en vigueur ou par les résultats des contrôles. Le responsable de l'AC est responsable de la procédure d'amendement de la PC.

Une revue de la PC est réalisée tous les ans dans le cadre de la préparation des audits bisannuels qui lorsqu'ils ne sont pas internes sont de renouvellement de qualification.

9.13 MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS

Toutes les composantes et acteurs de l'IGC sont tenus informés des amendements effectués sur la PC, et des impacts pour eux.

9.14 CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE

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

9.15 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

Une procédure de conciliation à l'amiable pour la résolution des conflits est mise en place. Elle doit nécessairement précéder toute action devant une juridiction. Le point de contact vers lequel se retourner est, le cas échéant, celui décrit dans le certificat final dans le champ Issuer Alternative Name. À défaut, il s'agit de celui énoncé au paragraphe 1.5.2.

9.16 JURIDICTIONS COMPETENTES

Toute contestation et tout litige pouvant naître à l'occasion de l'exécution de la présente PC seront du ressort exclusif des cours et des tribunaux monégasques avec seule application de la loi monégasque.

9.17 DISPOSITION DIVERSES

9.17.1 Accord global

Sans objet.

9.17.2 Transfert d'activités

Sans objet.

9.17.3 Conséquences d'une clause non valide

Sans objet.

9.17.4 Application et renonciation

Sans objet.

9.17.5 Force majeure

Sont considérés comme relevant de la force majeure, tous les cas habituellement retenus par les cours et tribunaux monégasques notamment lors de la survenance d'un événement imprévisible, irrésistible ou insurmontable.

En cas de force majeure, l'AC, ne pouvant en tout ou partie exécuter les obligations mises à sa charge, n'est cependant pas tenue d'en informer les Responsables de Certificat.

9.17.6 Autres dispositions

Sans objet.