n° ME/AMSN/20230928-295/NP

INFRASTRUCTURE DE CONFIANCE NATIONALE
Politique de Certification
AC RACINE

Version	Date	Description	Auteurs	Société
0.1	03/07/2019	Version initiale	SR	SEALWeb
0.2	30/10/2019	Ajout de l'OID, nommage de l'AC	SR	SEALWeb
0.3	03/02/2020	Prise en compte des éléments de la cérémonie des clés	SR	SEALWeb
0.4	18/02/2020	Relecture et corrections	GM	AMSN
0.5	27/02/2020	Relecture et corrections	FG	AMSN
0.6	06/03/2020	Prise en compte des commentaires et réponses aux questions	SR	SEALWeb
0.61	10/03/2020	Relecture et compléments	FC	Certinomis
0.7	18/03/2020	Relecture et compléments	FG	AMSN
0.8	03/04/2020	Compléments, suppression de commentaires validés	SR	SEALWeb
0.9	08/04/2020	Relecture, validation	FG - GM - FC - SR	AMSN - SEALWeb - Certinomis
0.91	08/04/2020	Compléments, suppression de commentaires validés	SR	SEALWeb
0.92	09/04/2020	Relecture, validation	FG	AMSN
0.9.2.4	18/05/2020	Relecture et validation	DR - FF - FG - GM	AMSN
0.9.2.5	20/05/2020	Corrections	FG	AMSN
0.9.3	25/11/2020	Relecture, commentaires et mise à jour	FG - GM	AMSN
0.9.4	26/11/2020	Réponses aux commentaires Certinomis/Docaposte	SR	SEALWeb
0.9.4.1	01/12/2020	Mises à jour	HA - GM	DITN - AMSN
0.9.5	19/04/2021	Mises à jour	FG - GM	AMSN
1.0	04/11/2021	Validation	FG	AMSN
1.01	28/09/2023	Modification de la durée de conservation des réponses/requêtes OCSP et du formalisme du document	FG - TH	AMSN

État du document - Classification	Référence
En cours - Publique	2.16.492.1.1.1.1.1.1

Ce document comporte 45 pages.

24, rue du Gabian
98000 MONACO
Tél. : (+377) 98 98 24 93
amsn@gouv.mc

Sommaire

1 INTRODUCTION

1.1 PRESENTATION GENERALE

Au sein de la Principauté de Monaco, l'Agence Monégasque de Sécurité Numérique (AMSN) est responsable de la chaîne de certification de l'État Monégasque. Dans ce cadre, elle génère et opère l'Autorité de Certification Racine, source initiale de l'ensemble de la chaîne de certification.

Les certificats finaux mis en œuvre par le gouvernement monégasque sont générés par différentes Autorités de Certification opérationnelles, dépendant de l'Autorité de Certification « AC RACINE PRINCIPAUTÉ DE MONACO ». L'ensemble constitue une hiérarchie de certification.

Techniquement, l'AMSN recourt à une Infrastructure de Gestion des Clés (IGC) :

- hors-ligne pour la gestion de la clé de l'AC Racine ;
- en ligne pour la gestion des clés des AC Opérationnelles.

La présente Politique de Certification (PC) définit les engagements que prend l'AMSN quant aux opérations de son AC Racine « AC RACINE PRINCIPAUTÉ DE MONACO ».

Lorsque cela n'est pas précisé, le terme « AC » désigne dans le présent document l'« AC RACINE PRINCIPAUTÉ DE MONACO ».

1.2 IDENTIFIANT DU DOCUMENT

La présente PC est identifiée par le numéro d'OID suivant : 2.16.492.1.1.1.1.1.1

1.3 ENTITES INTERVENANT DANS L'IGC

L'AC gère exclusivement des certificats à destination des autorités de certification opérationnelles.

1.3.1 *Autorité de certification*

L'entité en charge de l'AC est l'AMSN.

L'AC met en place un comité de suivi nommé « comité de suivi des services de confiance » (C2SC), sous la responsabilité 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 dont notamment la Déclaration des Pratiques de Certification (DPC).

Ce comité est constitué des parties prenantes suivantes :

- le responsable de l'AC ;
- les responsables de chacune des AC opérationnelles ;
- le Responsable de la Sécurité des Systèmes d'Information (RSSI) du Gouvernement ;
- le Responsable de la Sécurité des Systèmes d'Information (RSSI) de la Mairie ;
- le Responsable de la Sécurité des Systèmes d'Information (RSSI) de la DSP.

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 et de l'ensemble de l'infrastructure à clés publiques qu'elle a mise en place.

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

- la mise en application de la Politique de Certification ;
- l'enregistrement des rôles de confiance et des porteurs de secrets ;
- l'émission des certificats ;
- la gestion du cycle de vie des certificats ;
- l'exploitation de l'IGC propre à l'« AC RACINE PRINCIPAUTÉ DE MONACO » ;
- la publication de la Liste des Autorités Révoquées (LAR) et de la Liste des Certificats Révoqués (LCR) ;
- la journalisation et l'archivage des événements et informations relatifs au fonctionnement de l'IGC.

1.3.2 *Autorité d'enregistrement*

L'AC intègre sa propre composante AE.

Les AE assurent les fonctions suivantes :

- la réception des dossiers de demande de génération d'un certificat d'AC opérationnelle ;
- la réception des dossiers de demande de révocation d'un certificat d'AC opérationnelle ;
- la vérification de l'identité et de l'habilitation du responsable d'AC opérationnelle à demander la création du certificat correspondant ;
- le déclenchement de la génération des certificats dans le cadre d'une cérémonie des clés (AC Racine uniquement) ;
- le déclenchement de la génération programmée ou ponctuelle des LAR (AC Racine uniquement) ;
- le déclenchement des fonctions d'archivage des données d'enregistrement des demandes de certificats d'AC, des documents liés aux cérémonies des clés, et d'une manière plus générale, de tout document qui devrait être conservé pour assurer la traçabilité des actions en lien avec la chaîne d'AC.

1.3.3 *Porteurs de certificats*

Dans le cadre de cette PC, il n'y a pas de porteurs de certificats. Les certificats générés sont ceux des AC opérationnelles et sont rattachés à un responsable d'AC.

1.3.4 *Utilisateurs de certificats*

Les utilisateurs de certificats sont les collaborateurs, services, serveurs et applications qui souhaitent reconnaître les certificats émis par les AC opérationnelles rattachées à l'« AC RACINE PRINCIPAUTÉ DE MONACO ».

1.3.5 *Autres participants*

Sans objet.

1.4 USAGE DES CERTIFICATS

1.4.1 *Domaines d'utilisation applicables*

1.4.1.1 Bi-clés et certificats de l'« AC RACINE PRINCIPAUTÉ DE MONACO »

Les bi-clés et les certificats de l'« AC RACINE PRINCIPAUTÉ DE MONACO » sont utilisés exclusivement pour la signature :

- des demandes de certificats d'AC opérationnelles ;
- des LAR.

1.4.1.2 Bi-clés et certificats des AC opérationnelles

Les bi-clés et les certificats des AC opérationnelles sont utilisables exclusivement pour :

- signer des certificats finaux ;
- signer des LCR.

1.4.2 *Domaines d'utilisation interdits*

Tout autre usage que celui défini au paragraphe précédent est interdit.

1.5 GESTION DE LA PC

1.5.1 *Entité gérant la PC*

La PC est gérée par le C2SC.

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 :

Agence Monégasque de Sécurité Numérique (AMSN)

Adresse : 24, rue du gabian - 98000 Monaco

Ligne directe : (+377) 98.98.93.93

Fax : (+377) 99.90.33.49

Email : pex-amsn@gouv.mc

1.5.3 *Entité déterminant la conformité d'une DPC à 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 d'audits internes et du plan d'action décidé ou validé par le C2SC. Les services de confiance font l'objet d'une homologation de sécurité qui atteste que le responsable d'exploitation de l'IGC, également appelé autorité d'emploi, valide la mise en production de cette infrastructure en ayant connaissance des risques résiduels et en les acceptant.

1.6 DEFINITION 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
ACO	Autorité de Certification Opérationnelle
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
CEN	Comité Européen de Normalisation
DN	Distinguished Name (nom de l'autorité de certification émettrice)
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute (institut européen des normes de télécommunications)
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés
LAR	Liste des Autorités Révoquées
LCR	Liste des Certificats Révoqués
OCSP	Online Certificate Status Protocol (protocole de vérification de certificat en ligne)
OID	Object Identifier (identifiant universel d'un objet)
PASSI	Prestataire d'Audit en Sécurité des Systèmes d'Information
PC	Politique de Certification
PP	Profil de Protection
PSCo	Prestataire de Services de Confiance
RSA	Rivest Shamir Adleman
SSI	Sécurité des Systèmes d'Information

1.6.2 *Termes communs aux différentes PC et définitions*

Applications utilisatrices	Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat.
Authentification	Processus permettant de vérifier l'identité déclarée d'une personne ou de toute autre entité, ou de garantir l'origine de données reçues.
Bi clé	Une bi clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques.
Certificat	Donnée sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire. Cette attestation prend la forme d'une signature électronique réalisée par un prestataire de service de certification électronique (PSCE). Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci.
Certificat d'AC	Certificat d'une autorité de certification.
Chaîne de confiance	Ensemble des certificats nécessaires pour valider la généalogie d'un certificat d'un porteur de certificat. Dans une architecture horizontale simple, la chaîne se compose des certificats suivants : - celui de l'autorité de certification racine, base de la confiance de la chaîne de certification ; - celui de l'autorité de certification qui a émis le certificat ; - celui du porteur de certificat.
Hardware Security Module	Boîtier cryptographique matériel offrant un service de sécurité qui consiste à générer, stocker et protéger les clés cryptographiques notamment les clés publiques et privées des autorités de certification.
Infrastructure de gestion de clés	Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.
Liste de Certificats Révoqués (LCR)	Liste contenant les identifiants des certificats révoqués ou invalides.
Object Identifier	Identificateur numérique unique enregistré conformément à la norme d'enregistrement ISO (ISO/IEC 9834-1:2012) 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.
Promoteur d'application	Responsable d'un service de la sphère publique accessible par voie électronique.
Système d'information	Tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci.

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[1] (au sein de l'AMSN) est chargé de mettre à disposition l'information devant être publiée selon les formalités décrites dans la section §2.2 du présent document.

Les informations sont publiées sur l'URL suivante : https://icn.amsn.mc/icn

2.2 INFORMATIONS DEVANT ETRE MISES A DISPOSITION

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

- la présente PC ;
- les LAR ;
- le certificat auto-signé de l'AC en cours de validité.

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.

2.3 DELAIS ET FREQUENCES DE PUBLICATION

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

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

Les LAR de l'AC sont établies une fois par an en situation normale. Les 12 LAR de l'année (une par mois) sont alors pré-générées et la LAR du mois concerné est publiée en début de mois.

En cas de nécessité de révoquer un certificat d'AC opérationnelle, une nouvelle série de LAR est pré-générée et la LAR incluant le certificat nouvellement révoqué est immédiatement publiée. Les suivantes le sont sur le même rythme qu'en situation normale.

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 seules personnes autorisées de l'AC. L'accès au service de publication se fait de manière nominative et, dans la mesure du possible, avec une authentification à double facteur. Il est opéré par l'Opérateur Technique et le Gouvernement Princier.

[1] Renvoi vers document des rôles de confiance

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 conforme à la norme X501 et sous la forme d'une chaîne de type UTF8string.

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*

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

3.1.4 *Règles d'interprétation des différentes formes de noms*

Le nom de l'AC est défini par le C2SC.

3.1.5 *Unicité des noms*

Le C2SC assure l'unicité du DN demandé pour la création du certificat d'AC.

3.1.6 *Identification, authentification et rôle des marques déposées*

Le C2SC s'assure au moment de la validation de la demande de certificat d'AC que le nom distinctif utilisé est libre d'utilisation et que la dénomination demandée ne porte pas atteinte à des droits de propriété de tiers.

3.2 VALIDATION INITIALE DE L'IDENTITE

Le CS2SC :

- valide la demande de certificat d'AC lorsqu'il s'agit d'un certificat racine ;
- s'assure de la légitimité du demandeur lorsqu'il s'agit d'un certificat d'AC opérationnelle.

3.2.1 *Méthode pour prouver la possession de la clé privée*

Le certificat de l'« AC RACINE PRINCIPAUTÉ DE MONACO » est un certificat auto-signé. La demande est générée depuis les interfaces de l'IGC.

Le demandeur du certificat d'AC complète et signe un formulaire de demande de certificat d'AC opérationnelle faisant apparaître les informations nécessaires à l'établissement de ce certificat.

La clé privée de l'AC est directement générée dans le HSM rattaché à la racine de l'IGC. Ces opérations se font dans le cadre de la cérémonie des clés devant témoins.

3.2.2 *Validation de l'identité d'un organisme*

L'organisme porteur du certificat de l'AC racine est l'AMSN. Son identité est validée de fait par le Comité de Suivi des Services de Confiance (C2SC)[2] lors de l'analyse de la demande de certificat.

3.2.3 *Validation de l'identité d'un individu*

La validation de l'identité du demandeur est réalisée dans le cadre du C2SC.

3.2.4 *Informations non vérifiées du porteur*

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

3.2.5 *Validation de l'autorité du demandeur*

La présente version de la PC n'envisage que des émissions de certificats à des AC opérationnelles opérées par l'Opérateur Technique[2] sous la responsabilité de l'AMSN. Le C2SC s'assure de l'autorité du demandeur à demander un certificat pour une AC opérationnelle.

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. Le renouvellement se traduit alors par une nouvelle demande de certificat et bénéficie des mêmes procédures que pour une demande initiale (voir section 3.2 de la présente PC).

3.3.1 *Identification et validation pour un renouvellement courant*

La procédure est identique à une demande initiale.

3.3.2 *Identification et validation pour un renouvellement après révocation*

La procédure est identique à une demande initiale.

3.4 IDENTIFICATION D'UNE DEMANDE DE REVOCATION

La demande de révocation de clé pour une AC opérationnelle ne peut émaner que du responsable de l'AC opérationnelle ou du C2SC. Elle est validée formellement par le responsable du C2SC avant prise en compte.

Le certificat de l'« AC RACINE PRINCIPAUTÉ DE MONACO » étant un certificat auto-signé, il ne peut pas être révoqué.

En cas de compromission de la clé privée correspondant au certificat de l'AC, le C2SC réalisera l'ensemble des actions prévues en cas de compromission (voir 4.9).

[2] Spécifié dans le document relatif à la gestion des rôles.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 DEMANDE DE CERTIFICAT

4.1.1 *Origine d'une demande de certificat*

Le demandeur de certificat est le responsable de l'AC. Il réalise la demande directement en complétant et signant le formulaire de demande de certificat d'AC.

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

Après validation de la demande par le C2SC, il est planifié une cérémonie des clés au cours de laquelle seront générés les bi-clés et le certificat correspondant. Les opérations techniques de la cérémonie des clés se font dans une salle dont l'accès est contrôlé.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT DANS LE CADRE D'UNE NOUVELLE AC

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

Le C2SC reçoit une demande signée du responsable de l'AC.

4.2.2 *Acceptation ou rejet de la demande*

En cas de rejet de la demande, l'AC en informe le demandeur en lui apportant une justification.

4.2.3 *Durée d'établissement du certificat*

Le C2SC doit s'efforcer de traiter la demande de certificat dans un délai raisonnable. Même s'il n'y a aucune restriction concernant la durée maximale ou minimale de traitement, un délai maximum de 2 mois est établi entre la validation de la demande par le C2SC et la réalisation de la cérémonie des clés.

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 :

- génération des bi-clés directement sur les HSM associés à l'IGC (site nominal et site de secondaire) ;
- production de la CSR depuis les interfaces de l'IGC ;
- vérification technique de la CSR ;
- soumission de la CSR à l'AC et génération du certificat ;
- vérification du certificat.

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

Le demandeur de certificat est présent lors de la cérémonie des clés.

4.4 ACCEPTATION DU CERTIFICAT

4.4.1 *Démarche d'acceptation du certificat*

Le certificat produit est visualisé durant la cérémonie des clés par les participants. Le bon déroulement du script de cérémonie des clés et la signature du procès-verbal associé valent acceptation du certificat d'AC généré.

4.4.2 *Publication du certificat*

Le certificat fait l'objet d'une publication sur le site de publication (voir 2.2) avant toute utilisation en production de la clé privée associée.

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 RACINE PRINCIPAUTÉ DE MONACO »

La clé privée de l'« AC RACINE PRINCIPAUTÉ DE MONACO » est utilisée pour :

- signer son propre certificat d'AC (certificat auto-signé) ;
- signer les certificats des AC opérationnelles ;
- signer les LAR.

Ces usages sont explicitement définis dans les extensions des certificats.

4.5.1.2 Clé privée des AC opérationnelles

La clé privée d'une AC opérationnelle associée à un certificat émis par l'« AC RACINE PRINCIPAUTÉ DE MONACO » est destinée à :

- signer les certificats finaux des porteurs ;
- signer la LCR ;
- signer les certificats de répondeurs OCSP, le cas échéant.

Ces usages sont explicitement définis dans les extensions des certificats.

4.5.2 *Usage de la clé publique et du certificat*

4.5.2.1 Clé publique et certificat de l'« AC RACINE PRINCIPAUTÉ DE MONACO »

Le certificat de l'AC est utilisé pour :

- vérifier l'intégrité de la clé publique de l'AC (certificat auto-signé) ;
- vérifier l'origine et l'intégrité des certificats des AC opérationnelles ;
- vérifier l'origine et l'intégrité des LAR émises.

4.5.2.2 Certificats des AC opérationnelles

Les certificats de l'AC opérationnelle émis par l'« AC RACINE PRINCIPAUTÉ DE MONACO » sont destinés à :

- valider les certificats finaux des porteurs ;
- valider la LCR ;
- valider les certificats des répondeurs OCSP, le cas échéant.

4.6 RENOUVELLEMENT D'UN CERTIFICAT

Le renouvellement de certificat, au sens de la [RFC3647], 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 RACINE PRINCIPAUTÉ DE MONACO », seront renouvelés au minimum tous les 20 ans.

Les bi-clés, et les certificats correspondants des AC opérationnelles, seront renouvelés au minimum tous les 10 ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat (cf. chapitre 4.9).

4.7.2 *Origine d'une demande d'un nouveau certificat*

La demande d'un nouveau certificat est :

- à l'initiative du C2SC pour l'« AC RACINE PRINCIPAUTÉ DE MONACO »
- à l'initiative du responsable correspondant pour les AC opérationnelles.

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

La procédure est identique à la demande initiale. L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 3.3 ci-dessus. Pour les actions de l'AC, il faut se reporter au chapitre 4.3.1.

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

La procédure est identique à celle à suivre pour la demande initiale et décrite au chapitre 4.3.2.

4.7.5 *Démarche d'acceptation du nouveau certificat*

La procédure est identique à celle à suivre pour la demande initiale et décrite au chapitre 4.4.1.

4.7.6 *Publication du nouveau certificat*

La procédure est identique à celle à suivre pour la demande initiale et décrite au 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 celle à suivre pour la demande initiale et décrite au chapitre 4.4.3.

4.8 MODIFICATION DU CERTIFICAT

Pour modifier un certificat d'une AC opérationnelle, il faut le révoquer puis faire une nouvelle demande.

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*

Il peut exister plusieurs causes de révocation de certificat d'une AC opérationnelle :

- les informations de l'AC opérationnelle figurant dans son certificat ne sont plus correctes ;
- l'AC opérationnelle n'a pas respecté les modalités applicables d'utilisation du certificat ;
- l'AC opérationnelle n'a pas respecté ses obligations découlant de la présente PC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement de l'AC opérationnelle ;
- la clé privée de l'AC opérationnelle est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- le responsable de l'AC opérationnelle demande explicitement la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée et/ou de son support) ;
- cessation d'activité de l'AC opérationnelle ;
- cessation d'activité de l'« AC RACINE PRINCIPAUTÉ DE MONACO ».

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 d'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 d'AC opérationnelle ne peut émaner que :

- du responsable de l'AC opérationnelle ;
- du responsable du C2SC ;
- des autorités judiciaires via une décision de justice.

4.9.3 *Procédure de traitement d'une demande de révocation*

Une demande de révocation de certificat réceptionnée par l'AC doit au moins contenir les informations suivantes :

- le numéro de série du certificat à révoquer ;
- le nom associé au certificat à révoquer (DN complet) ;
- le nom et la qualité du demandeur de la révocation ;
- la cause de révocation.

La demande est faite à travers un formulaire prévu à cet effet pour ensuite être signée par le demandeur.

La demande est alors, dès réception, authentifiée et contrôlée par le C2SC. Le responsable du C2SC valide la demande et réunit le comité pour organiser au plus tôt une cérémonie des clés afin de traiter techniquement la demande de révocation.

4.9.4 *Délai accordé au porteur pour formuler la demande de révocation*

Dès que le responsable de l'ACO a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

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

L'ACR met tous les moyens en œuvre pour signer dans les meilleurs délais la révocation de l'ACO. Le délai maximum de traitement de la révocation est de 5 jours consécutifs après 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.

4.9.7 *Fréquence d'établissement des LAR*

Les LAR sont pré-générées tous les 12 mois. Elles sont publiées mensuellement le 1er jour du mois de leur validité. Elles ont une durée de validité de 45 jours.

4.9.8 *Délai maximum de publication des LAR*

Les LAR sont publiées le plus rapidement possible après la date d'établissement. Au maximum, le délai de publication sera de 10 jours.

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

Sans objet.

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

Sans objet.

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*

En cas de compromission de la clé privée de l'« AC RACINE PRINCIPAUTÉ DE MONACO » ou d'un certificat d'une AC opérationnelle, 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 et 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 RACINE PRINCIPAUTÉ DE MONACO » :
        - révoquer l'ensemble des certificats finaux émis par les AC opérationnelles ;
        - publier une nouvelle et dernière LCR pour chacune des AC opérationnelles ;
        - révoquer l'ensemble des certificats des AC opérationnelles ;
        - réémettre une dernière LAR faisant apparaître les numéros de série des certificats des AC opérationnelles ;
        - détruire toutes les anciennes LAR qui avaient été pré-générées ;
        - détruire les clés privées de l'« AC RACINE PRINCIPAUTÉ DE MONACO » et des AC opérationnelles.
    - Si la compromission concerne les clés d'une 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.

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). Ces informations permettent également de vérifier les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LAR ainsi que l'état du certificat de l'AC. Les LCR / LAR sont publiées à l'adresse spécifiée dans le 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 99,5%.

4.10.3 *Dispositifs optionnels*

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

4.11 FIN DE LA RELATION ENTRE UNE AC OPERATIONNELLE ET L'« AC RACINE PRINCIPAUTÉ DE MONACO »

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'« AC RACINE PRINCIPAUTÉ DE MONACO » et une AC opérationnelle avant la fin de validité du certificat de cette dernière, pour quelque raison que ce soit, le C2SC se réunit et statue sur l'une des deux dispositions suivantes :

- le certificat de l'AC opérationnelle et les certificats finaux émis par cette AC sont 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. Il ne sera par contre plus émis de certificats finaux via cette AC opérationnelle.

4.12 SEQUESTRE DE CLE ET RECOUVREMENT

Les clés privées des AC 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 MESURE 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 explosion, risque volcanique ou crue. Les environnements de l'IGC sont installés sur des sites sécurisés de production informatique, qui assurent notamment des protections contre les risques liés aux tremblements de terre.

L'hébergement de l'IGC est réparti entre trois sites dont un pour la racine, un principal et un secondaire dédié au secours et à la reprise d'activité localisé sur le territoire monégasque.

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. Les zones d'hébergement sont des zones protégées au sens de l'arrêté ministériel n°2016-723 du 12 décembre 2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié.

Les accès physiques à ces zones 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) sur le site d'hébergement de l'AC racine.

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*

Sans objet.

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 :

Rôles de confiance	AC racine (hors-ligne)	AC opérationnelle
Responsable d'AC	Responsable du C2SC	Responsable du service métier
Responsable d'AE	Responsable du C2SC (inclus dans le rôle de l'AC pour l'ACR)	Le responsable d'AE est en charge de mettre en œuvre les processus de gestion des certificats finaux et d'identification des porteurs de certificats conformément aux exigences définis par l'AC dans sa PC.
Administrateur système	Personne formellement identifiée au sein de l'AMSN en charge de réaliser les opérations d'administration de l'IGC et des clés d'AC	Opérateur technique du Prestataire en relation contractuelle avec l'AMSN. L'administrateur système est en charge de l'installation, du paramétrage, de la mise à niveau et de la correction d'un ou plusieurs sous-ensembles de l'IGC.
Exploitant / superviseur	Rôle non tenu dans le cadre de l'ACR	Opérateur technique du Prestataire en relation contractuelle avec l'AMSN. L'exploitant / superviseur est en charge du monitoring et des interventions de base tel un redémarrage.
Administrateur sécurité	Rôle non tenu dans le cadre de l'ACR	Opérateur technique du Prestataire 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 et piloter les audits techniques de sécurité.
Auditeur système	Rôle non tenu	Ce rôle est assuré par des personnes formellement identifiés au sein de l'AMSN pour l'ACR et des personnes du Prestataire en relation contractuelle avec l'AMSN pour les ACO. 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 plus des rôles de confiance opérationnels, l'AC identifie des porteurs de secrets qui disposent chacun d'une part des secrets des HSM mis en œuvre. Il existe deux types de secrets partagés :

	HSM racine	**HSMs de production**
Nombre de secret	1	1 secret par HSM hébergeant une ou plusieurs AC opérationnelles
Schéma de Shamir	Le secret est réparti avec un quorum de 3 parmi 5	Le secret est réparti avec un quorum de 3 parmi 5

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'AMSN pour des raisons de sécurité. Certains rôles de confiance sont occupés par plusieurs personnes pour que l'AMSN puisse assurer la continuité de ses services sans dégrader la sécurité des services offerts.

5.2.3 *Identification et authentification pour chaque rôle*

Chaque personne disposant d'un rôle de confiance est clairement identifiée par l'AMSN au travers d'un inventaire des rôles.

Chaque entité opérant une composante d'un service de l'AMSN 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 personnes font l'objet d'une traçabilité garantissant l'imputabilité des actions. Chaque attribution d'un rôle de confiance à une personne est notifiée et documentée par écrit.

Les rôles de confiance éventuellement assurés par l'opérateur technique de l'AMSN sont établis concrètement et acceptés formellement par les personnes ayant ces rôles.

5.2.4 *Rôles exigeant une séparation des attributions*

La présente politique autorise 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.

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 personnes opérant sur des postes sensibles correspondent à leurs compétences professionnelles.

Tous les rôles de confiance sont attribués en s'assurant que le niveau d'expertise de chaque personne désignée lui permet d'assurer pleinement les tâches associées au rôle qui lui est assigné.

Toute personne intervenant dans des rôles de confiance est de plus 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.

Dans le cas d'un fonctionnaire ou agent de l'État monégasque, un processus réglementaire est en place pour l'autoriser à pénétrer dans une zone protégée ; type de zone où sont notamment hébergés les services de l'AC.

Les autres intervenants doivent fournir chaque année à l'AMSN un extrait du bulletin n°3 de leur casier judiciaire.

5.3.3 *Exigences en matière de formation initiale*

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

Le Prestataire s'assure à cette fin que les personnes intervenant dans le fonctionnement d'une AC opérationnelle ont bien reçu une formation complète concernant les principes de fonctionnement et les mécanismes d'une AC.

Ainsi, chaque personne concernée suit un programme de formation pour accomplir correctement ses fonctions. Ce programme porte sur :

- les différentes applications et versions d'applications auxquelles il pourrait avoir accès dans le cadre de ses fonctions au sein du système de l'AC ;
- toutes les tâches qu'elle devra accomplir dans le cadre de l'IGC ;
- le matériel et les systèmes d'exploitation formant l'environnement opérationnel de l'AC ;
- le plan de secours de l'AC après un sinistre et les procédures de maintien des activités.

Avant l'entrée en fonction, il sera procédé à une familiarisation aux règles de sécurité en vigueur.

Des obligations identiques sont portées à la charge de l'AE et de son personnel.

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 leur mode de travail. 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 du 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.

L'AMSN transmet à l'ensemble des intervenants externes le Plan d'Assurance Sécurité (PAS), reprenant les règles de sécurité qui doivent être respectées dans le cadre de la mission qui leur est confiée. Ces règles de sécurité font l'objet d'une acceptation formelle par les différents intervenants.

5.3.8 *Documentation fournie au personnel*

Les règles de sécurité sont communiquées au personnel dès sa prise de fonction au regard du rôle qui lui est assigné. 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.

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

5.4 PROCEDURE DE CONSTITUTION DES DONNEES D'AUDIT

5.4.1 *Type 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 PKI.
  - l'activité des pare-feu et des systèmes de routage réseau ;
- Tous les événements relatifs à l'enregistrement des porteurs, en particulier :
  - réception d'une demande de certificat (initiale et renouvellement) ;
  - validation / rejet d'une demande de certificat ;
  - événements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction, ...) ;
  - génération des certificats des porteurs ;
  - publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
  - réception d'une demande de révocation ;
  - validation / rejet d'une demande de révocation ;
  - génération puis publication des LAR et LCR.

Pour l'« AC RACINE PRINCIPAUTÉ DE MONACO », étant opérée hors-ligne, les exigences sur l'activité des éléments réseau n'est applicable qu'à la fonction de publication.

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. Dans le contexte de l'ACR, cela revient à sauvegarder les traces des opérations de l'IGC et du HSM réalisées dans le cadre des cérémonies des clés. Ces éléments sont extraits des composants concernés à la fin de la cérémonie des clés et sont conservés dans un coffre.

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 opère une veille constante sur les vulnérabilités pouvant impacter ses produits.

Un processus interne définit les différents rôles applicables à chaque contact en matière de veille de gestion des vulnérabilités associées. 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.

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 (voir paragraphe 5.4.5).

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 ;
- 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) ;
- pour les AC opérationnelles les traces des opérations d'identification réalisées par les AE (justificatifs, vérification etc.)
- 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 (logiciel IGC et administration HSM) : version initiale de chacun des logiciels (celle mise en œuvre le jour de la cérémonie des clés initiale), la version n-1 et la version n ;
- configurations des logiciels : tous les fichiers de configuration associés aux versions archivées des logiciels ;
- certificats d'AC : 7 ans après la date d'expiration du certificat ;
- LCR et certificats clients : 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 (demandes de certificats) : durée de conservation identique à celle du certificat d'AC correspondant.

5.5.3 *Protection des archives*

Quel que soit leur support, les archives sont protégées en intégrité et ne sont accessibles qu'aux seules 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.

5.5.5 *Exigences d'horodatage des données*

L'ensemble des composants de l'IGC se synchronisent avec une source de temps de référence. Cette source de temps est elle-même synchronisée au moins une fois par jour avec UTC.

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 auprès du C2SC. Une restitution d'archives ne peut intervenir que dans le cadre d'une procédure judiciaire ou administrative.

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 opérée par l'Opérateur Technique et sur la base d'un processus permettant d'alerter le CERT-MC.

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 doit alors traiter l'anomalie. S'il estime que l'incident a un niveau de gravité important, il demande une révocation immédiate du certificat. Si celle-ci a lieu, il fait publier l'information de révocation du certificat sous le signe de l'urgence. Il le fait 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 fait publier l'information via l'ouverture d'un incident et notifie par courrier électronique l'ensemble des services utilisant les certificats émis par l'AC. Tous les certificats concernés sont alors révoqués suivant un planning établi le cas échéant.

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'AC. Les supports mémoire détenant ou ayant détenu des informations sensibles au sens de l'arrêté ministériel n° 2019-791 doivent être conservés par l'AMSN.

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

La compromission de la clé privée d'une composante et notamment lorsqu'il s'agit d'une clé d'ACR ou d'ACO est traitée par le C2SC dans le cadre d'une réunion de crise et conformément à la procédure de gestion des incidents de sécurité mis en place par l'AC. Le plan d'actions issu de cette réunion peut amener à arrêter définitivement l'activité de l'AC ou bien à refaire une nouvelle chaîne d'AC après révocation des certificats d'AC concerné.

En tout état de cause, en cas de suspicion de compromission ou de compromission avérée (source d'information interne ou externe à l'AC) de la clé privée d'une composante de l'ICN, la procédure prévoit notamment à partir de la réception du rapport d'incident de sécurité ad hoc :

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

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

Pour les autres sinistres affectant les activités de l'AC, un PRA est établi. Ce PRA est testé annuellement.

5.8 CESSATION D'ACTIVITE AFFECTANT L'AC

L'AC dispose d'un plan d'arrêt d'activité. L'AC 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.

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 de l'« AC RACINE PRINCIPAUTÉ DE MONACO »

Les clés de l'AC sont générées lors de la cérémonie des clés.

Cérémonie des clés

La cérémonie de génération des clés se déroule en présence d'un représentant du C2SC et suivant la procédure établie par le C2SC avec son Prestataire.

Module cryptographique

Voir chapitre 6.2.1.

6.1.1.2 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 établie par le C2SC avec son Prestataire.

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, en cours de validité y compris de manière dérogatoire.

6.1.2 *Transmission de la clé privée à son propriétaire*

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

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 garantissant que les données ne seront pas effacées durant le transport.

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

La clé publique d'AC est enveloppée dans un certificat racine auto signé. 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 de l'AC, ainsi que les informations correspondantes (certificat, empreinte numérique, PC et CGU correspondantes) pourront aisément être récupérées par les utilisateurs de certificats, via l'interface publique (voir 2.2).

6.1.5 *Tailles des clés*

Les clés d'AC ont les caractéristiques suivantes :

- algorithme utilisé : RSA ;
- taille des clés : 4096 bits.

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

L'équipement utilisé pour la génération des paramètres des bi-clés des AC est un module cryptographique configuré pour répondre au besoin. Les bi-clés ne peuvent être générées que sur un module cryptographique matériel qualifié.

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 LCR / LAR (cf. chapitre 1.4.1).

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 et fourni par la société ATOS/BULL.

Le boîtier racine est en version EL, ceux de production en version HR.

6.2.1.2 Mesures de sécurité pour les modules cryptographiques

L'AMSN s'assure de la sécurité physique et logicielle des modules cryptographiques utilisés en mettant en œuvre les versions qualifiées de ces équipements. En particulier, l'AMSN héberge ce matériel dans des zones d'accès contrôlées. Pour l'« AC RACINE PRINCIPAUTÉ DE MONACO », le module cryptographique est hors-ligne et n'est mis en œuvre que dans le cadre de cérémonies des clés.

L'AMSN s'assure de la sécurité des modules cryptographiques tout au long de leur cycle de vie, en particulier, lors de leur mise en place, de la cérémonie des clés et de leur utilisation jusqu'à leur fin de vie.

6.2.2 *Contrôle de la clé privée par plusieurs personnes*

Le contrôle de la clé privée de signature de l'AC est assuré par du personnel de confiance (porteurs de part de secret) et via un outil mettant en œuvre le partage des secrets.

Il y a N porteurs de part de secret pour chaque AC. Chacun se voit remettre ses parts sur des cartes à puce distinctes lors de la cérémonie des clés. Un quorum de porteurs parmi les N porteurs est nécessaire pour activer la clé privée de l'AC.

6.2.3 *Séquestre de la clé privée*

Aucune clé privée ne sera séquestrée.

6.2.4 *Copie de secours de la clé privée*

6.2.4.1 Clé privée de l'« AC RACINE PRINCIPAUTÉ DE MONACO »

La clé privée de l'AC n'étant pas en permanence activée au sein du module cryptographique, elle fait l'objet d'une copie de secours hors d'un module cryptographique.

Cette copie 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 s'appuie notamment 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 la clé privée d'AC ne soit à aucun moment en clair en dehors du module cryptographique.

Il est établi deux copies de secours. Ces copies sont stockées sur des supports de nature différente et sont conservées dans des coffres-forts hébergés sur des sites géographiquement différents. Le contrôle des opérations de chiffrement / déchiffrement est conforme aux exigences du chapitre 6.2.2.

6.2.4.2 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 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 s'appuie notamment 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.

6.2.5 *Archivage de la clé privée*

Sans objet.

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

Le transfert vers / 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.

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.

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 (cf. chapitre 6.4).

Pour l'« AC RACINE PRINCIPAUTÉ DE MONACO », la clé privée étant désactivée après chaque opération cryptographique (voir 6.2.9), un quorum de porteurs de secrets devra être présent afin de réaliser l'activation de la clé avant chaque opération.

6.2.9 *Méthode de désactivation de la clé privée*

La clé privée de l'« AC RACINE PRINCIPAUTÉ DE MONACO » est désactivée après chaque opération cryptographique par redémarrage du module cryptographique. La saisie des données d'activation sont alors nécessaires pour réactiver la clé de l'ACR.

6.2.10 *Méthode de destruction des clés privées*

La destruction définitive d'une clé privée d'AC 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 au paragraphe 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 de l'« AC RACINE PRINCIPAUTÉ DE MONACO »

La clé de l'« AC RACINE PRINCIPAUTÉ DE MONACO » et le certificat associé ont une durée de vie de 30 ans.

6.3.2.2 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.

6.4 DONNEES D'ACTIVATION

6.4.1 *Génération et installation des données d'activation*

Les éléments nécessaires à l'activation de la clé privée de l'« AC RACINE PRINCIPAUTÉ DE MONACO », et des clés privées des AC opérationnelles sont générés de manière sécurisée, et ne sont accessibles qu'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.

6.4.2 *Protection des données d'activation*

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

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 des composantes de l'IGC identifient et authentifient de façon unique leurs utilisateurs. Toute interaction entre une composante et un utilisateur n'est possible qu'après une identification et une authentification réussies. Pour chaque interaction, la composante établit l'identité de l'entité. Les informations d'authentification sont stockées de telle façon qu'elles sont seulement accessibles par des utilisateurs autorisés.

6.5.1.2 Contrôle d'accès

Les composantes de l'IGC ne sont accessibles qu'aux seules 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 rebus) des équipements sont documentées afin de garantir la non-divulgation des informations sensibles qu'ils peuvent détenir. L'ensemble des matériels sensibles de l'IGC 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. Elles visent notamment à s'assurer du maintien de l'intégrité et de la confidentialité des données de l'IGC.

6.5.1.4 Intégrité des composants de l'IGC

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 usagers 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.

Les objectifs de sécurité sont définis lors des phases de spécification et de conception. Les systèmes et les produits utilisés sont fiables et protégés contre toute modification.

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 réalisés 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 l'« AC RACINE PRINCIPAUTÉ DE MONACO », l'AC étant hors ligne, il n'y a pas d'accès réseau en entrée ou en sortie.

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

6.8 HORODATAGE / SYSTEME DE DATATION

Pour l'« AC RACINE PRINCIPAUTÉ DE MONACO », l'AC étant hors ligne, l'horloge est synchronisée manuellement avant toute utilisation. Cette opération est faite pendant la cérémonie des clés.

Les AC opérationnelles, quant à elles, sont synchronisées suivant les modalités évoquées au paragraphe 5.5.5.

7 PROFILS DE CERTIFICATS ET DES LCR/LAR

7.1 PROFIL DES CERTIFICATS

7.1.1 *Certificats de l'« AC RACINE PRINCIPAUTÉ DE MONACO »*

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	Généré automatiquement lors de la cérémonie des clés
Signature	Sha256WithRSAEncryption
Issuer	• CN=AC RACINE PRINCIPAUTE DE MONACO • OU=0206 20A00001 • orgID=NTRMC-20A00001 • O=AMSN • C=MC
Subject	Identique à l'issuer (certificat auto-signé) • CN=AC RACINE PRINCIPAUTE DE MONACO • OU=0206 20A00001 • orgID=NTRMC-20A00001 • O=AMSN • C=MC
Validity	• notBefore: Date de création • notAfter: notBefore + 30 ans
Subject Public Key Info	RSA 4096 bits

7.1.1.2 Extensions du certificat

Le tableau suivant présente les extensions :

Champ	OID	Criticité	Valeur
authorityKeyIdentifier	2.5.29.35	Non	keyid: 97:B0:7D:B6:FE:4B:A9:55:30:CF:EB:3B:87:7E:0E:66:3A:9C:3D:E9
subjectKeyIdentifier	2.5.29.14	Non	97:B0:7D:B6:FE:4B:A9:55:30:CF:EB:3B:87:7E:0E:66:3A:9C:3D:E9
keyUsage	2.5.29.15	Oui	keyCertSign, CRLSign, digitalSignature
basicConstraints	2.5.29.19	Oui	• CA: true • Maximum Path Length : absent
authorityInfoAccess	1.3.6.1.5.5.7.1.1	Non	CA Issuers - URI:https://icn.amsn.mc/icn/acr.crt

7.1.2 *Certificats des AC opérationnelles*

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 lors de la cérémonie des clés
Signature	Sha256WithRSAEncryption
Issuer	• CN=AC RACINE PRINCIPAUTE DE MONACO • OU=0206 20A00001 • orgID=NTRMC-20A00001 • O=AMSN • C=MC
Subject	• CN=<à définir par ACD> • OU=<à définir par ACD> • orgID=<à définir par ACD> • O=<à définir par ACD> • C=<à définir par ACD>
Validity	• notBefore: Date de création • notAfter: notBefore + 10 ans
Subject Public Key Info	RSA 4096 bits

7.1.2.2 Extensions du certificat

Le tableau suivant présente les extensions :

Champ	OID	Criticité	Valeur
authorityKeyIdentifier	2.5.29.35	Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le certificat
subjectKeyIdentifier	2.5.29.14	Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le certificat
keyUsage	2.5.29.15	Oui	keyCertSign, CRLSign, digitalSignature
basicConstraints	2.5.29.19	Oui	• CA: true • Maximum Path Length : absent
cRLDistributionPoints	2.5.29.31	Non	Full Name: • URI:https://icn.amsn.mc/icn/icn4096.crl • URI:https://icn.monaco.fr/icn/icn4096.crl
authorityInfoAccess	1.3.6.1.5.5.7.1.1	Non	CA Issuers - URI:https://icn.amsn.mc/icn/acr.crt

7.2 LISTE DE CERTIFICATS REVOQUES

7.2.1 *LAR de l'« AC RACINE PRINCIPAUTÉ DE MONACO »*

7.2.1.1 Champs de base

Le tableau suivant présente les champs de base :

Champ	Valeur
Version	1 (pour version 2)
Signature	SHA256WithRSA
Issuer	• CN=AC RACINE PRINCIPAUTE DE MONACO • OU=0206 20A00001 • orgID=NTRMC-20A00001 • O=AMSN • C=MC
Validity	45 jours
Revoked Certificates	• Serial Number • Revocation Date

7.2.1.2 Extensions

Le tableau suivant présente les extensions :

Champ	OID	Criticité	Valeur
authorityKeyIdentifier	2.5.29.35	Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
cRLNumber	2.5.29.20	Non	Défini par l'outil

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

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

D'autres audits externes seront réalisés, notamment pour obtenir des certifications de conformité aux normes ETSI ou des qualifications de service de confiance dans le cadre du règlement eIDAS et le Référentiel Général de Sécurité de la Principauté.

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. Il est recommandé dans ce cadre de recourir à un PASSI qualifié.

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 sa DPC.

8.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

A l'issue d'un audit de sécurité, l'équipe d'audit rend à l'AC un avis parmi les suivants : « conforme », « non conforme », « avec réserve ».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes. En cas d'avis :

- non conforme, et selon l'importance des non-conformités relevées, 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 ;
- avec réserve, 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 ;
- conforme, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et de la DPC.

9 AUTRES PROBLEMES METIERS ET LEGALES

9.1 TARIF

Sans objet.

9.2 RESPONSABILITE FINANCIERE

9.2.1 *Couverture par les assurances*

L'Opérateur Technique est couvert par une assurance responsabilité civile pour les actions qu'il engage dans le cadre de sa relation contractuelle auprès de l'AC.

9.2.2 *Autres ressources*

L'AC engage les ressources financières nécessaires pour assurer ses activités et notamment la gestion de la fin de vie d'AC. Cela comprend notamment les ressources permettant de maintenir la publication des statuts des certificats qui ont été émis par l'AC, les certificats et documents (Politiques de Certification et CGU) associés.

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 ;
- 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 révocations.

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 ayant le besoin d'en connaître. L'AMSN 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 *Définition*

Les données personnelles propres à la racine regroupent les identités des rôles de confiance et des porteurs de secrets.

9.4.2 *Politique de protection des données personnelles*

Des mesures techniques, procédurales et organisationnelles sont mises en place pour garantir la protection des données personnelles recueillies conformément à la réglementation en place. Une déclaration à la CCIN a par ailleurs été faite.

9.4.3 *Informations à caractère personnel*

Les informations à caractère personnel sont les informations nominatives concernant les attributaires d'un rôle de confiance, enregistrées au sein du dossier de suivi des rôles de confiance de l'Infrastructure de Confiance Nationale (ICN). Il s'agit des informations nom / prénom / adresse postale professionnelle, numéro de téléphone professionnel, email professionnel.

9.4.4 *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 règlementation en vigueur.

9.4.5 *Notification et consentement d'utilisation des données personnelles*

Voir paragraphe 0

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

Les enregistrements seront mis à disposition aux autorités en cas de réquisition.

9.4.7 *Autres circonstances de divulgation d'informations personnelles*

Sans objet.

9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

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

9.6 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 0) ;
- 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.

9.6.1 *Autorités de Certification*

L'AMSN, en tant qu'AC, est 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.

L'AMSN, en tant qu'AC, n'est pas responsable, sauf à démontrer qu'il a été commis une 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'AMSN 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.

9.6.2 *Autorités d'enregistrement*

Le contrôle des ACO est traité dans les PC de chacune des ACO.

9.6.3 *Responsable de certificat d'AC*

Le responsable de certificat d'AC a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- respecter les conditions d'utilisation du service ;
- informer l'AC de toute modification concernant les informations contenues dans son certificat ;
- demander le renouvellement de son certificat avec un délai raisonnable avant son expiration ;
- faire, sans délai, une demande de révocation de son certificat en cas de compromission ou de suspicion de compromission de ses données d'activation ou de sa clé privée.

9.6.4 *Utilisateurs de certificats*

Les utilisateurs des certificats doivent :

- vérifier et respecter l'usage pour lequel un certificat a été émis ;
- pour chaque certificat de la chaîne de certification, de celui du porteur à celui de l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et en contrôler sa validité (dates de validité, statut de révocation).

9.6.5 *Autres participants*

Sans objet.

9.7 LIMITE DE GARANTIE

Sans objet.

9.8 LIMITE DE RESPONSABILITE

La responsabilité de l'AMSN ne peut être engagée qu'en cas de manquement aux dispositions prévues par la présente politique.

L'AMSN 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.

L'AMSN décline toute responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées.

L'AMSN ne saurait être tenue responsable, 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.

9.9 INDEMNITES

Sans objet.

9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1 *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.

9.10.2 *Fin anticipée de validité*

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

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

Sans objet.

9.11 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 rendue nécessaire par la législation, la réglementation en vigueur ou par les résultats des contrôles.

Le responsable de l'AC, est responsable de la procédure d'amendement de la PC.

9.12 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 les concernant.

9.13 CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE

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

9.14 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

Une procédure de conciliation à l'amiable pour la résolution des conflits est mise en place.

9.15 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 tribunaux monégasques avec seule application de la loi monégasque.

9.16 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

L'AMSN, dans toutes ses composantes et y compris documentaires, est régie par la législation et la réglementation monégasques qui lui sont applicables et ce bien que ses activités qui découlent de la présente politique puissent avoir des effets juridiques en dehors du territoire 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, est tenue d'en informer le C2SC.

9.17.6 *Autres dispositions*

Sans objet.