Politique et Pratiques de Certification

Netcom Seal Qualified CA

Indices et date	Rédacteur	Vérificateur date et nom	Approbateur date et nom
Version 1.0 19/05/2021	NETCOM GROUP		
Version 1.1 22/09/2021	NETCOM GROUP		
Version 1.2 16/11/2021	NETCOM GROUP		
Version 1.3 18/02/2022	NETCOM GROUP		
Version 1.4 10/04/2024	NETCOM GROUP		

Classification : public

Table des matières

1. INTRODUCTION

1.1 Présentation générale

La société NETCOM GROUP est un Prestataire de Service de Certification Electronique (PSCE) qui délivre des certificats électroniques de cachet, qualifiés au titre du règlement eIDAS. Ces certificats permettent de créer des cachets électroniques avancés sur la base de certificats qualifiés, par exemple pour un service de signature électronique.

Dans ce cadre, ce document décrit la Politique de Certification (PC) ainsi que la Déclaration de Pratiques de Certification (DPC) de l'Autorité de Certification « NETCOM GROUP - SEAL QUALIFIED CA ».

Ce document regroupe l'ensemble des engagements et des pratiques de NETCOM GROUP dans le cadre du déploiement et de l'exploitation de l'AC « NETCOM GROUP - SEAL QUALIFIED CA », tant sur les plans techniques qu'organisationnels.

L'AC « NETCOM GROUP - QUALIFIED SEAL CA » ne peut être utilisée que pour :

- Produire des certificats qualifiés de cachet électronique ;
- Produire des Listes des Certificats Révoqués (LCR).

Les certificats qualifiés de cachet électronique sont exclusivement à destination de personnes morales.

Ces certificats sont conformes à la norme ETSI 319 411-2 au niveau QCP-l et sont qualifiés, au sens du règlement eIDAS, par l'ANSSI.

La chaîne de certification est la suivante :

- AC Racine : « NETCOM GROUP - ROOT CA »
    - AC Déléguée : « NETCOM GROUP - SEAL QUALIFIED CA »

1.2 Identification du document

Le présent document correspond à la Politique de Certification (PC) et à la Déclaration de Pratiques de l'Autorité de Certification « NETCOM GROUP - SEAL QUALIFIED CA ».

L'identifiant de ce document est l'OID : 1.3.6.1.4.1.56143.1.2.1.1

Les certificats émis selon cette politique sont des certificats qualifiés de cachet électronique émis conformément à la politique ETSI d'OID 0.4.0.194112.1.1 pour le niveau QCP-l.

Les OID peuvent évoluer en cas de modifications importantes de la PC. Lorsqu'un nouvel OID est généré, le dernier chiffre est incrémenté. La version initiale utilise le chiffre 1.

1.3 Entités intervenant dans l'IGC

1.3.1 Autorité de certification

L'AC génère des certificats et révoque des certificats à partir des demandes que lui envoie l'Autorité d'Enregistrement. L'AC met en œuvre les services de génération de certificats, de révocation de certificats, de publication des informations nécessaire, de journalisation et d'audit. NETCOM GROUP s'appuie sur ses propres capacités afin de mettre en œuvre l'ensemble des opérations cryptographiques nécessaires à la création et la gestion du cycle de vie des certificats. L'AC agit conformément à la présente PC et DPC établie par la Direction de NETCOM GROUP. NETCOM GROUP est AC au sens de la responsabilité de gestion du cycle de vie des certificats.

1.3.2 Autorité d'enregistrement

L'AE est utilisée pour la mise en œuvre des services d'enregistrement des porteurs, de demande initiale et de renouvellement de certificats, de révocation de certificats, de journalisation et d'audit. L'AE est chargée d'authentifier et d'identifier les porteurs. L'AC agit conformément à la présente PC et DPC, et en respectant les règlementations relatives à la protection des données à caractère personnel. L'AE est mise en œuvre par NETCOM GROUP.

1.3.3 Porteur de certificats (RCC)

Les certificats de cachet sont délivrés à des personnes morales, qui sont les clients de l'AC et le sujet des certificats. Un certificat de cachet est placé sous la responsabilité d'une personne physique, le Responsable du Certificat Cachet (RCC) mandaté par la personne morale détentrice du certificat. Le Responsable de Certificat Cachet a un lien contractuel, hiérarchique ou réglementaire avec cette entité et est expressément mandaté par elle.

Dans le cadre de cette PC, le RCC est désigné comme le porteur du certificat. En cas d'interruption des fonctions du RCC, l'entité sujette du certificat doit lui nommer un successeur et en informer l'AC.

Le porteur de certificat est responsable de la clé privée de cachet, et de la génération de la demande de certificat transmise à l'AE.

1.3.4 Utilisateurs de certificats

L'utilisateur de certificat est une personne ou une application qui valide un certificat de cachet émis par l'AC dans le cadre de la validation de signature électronique de données ou de document.

1.4 Usage des certificats

1.4.1. Domaines d'utilisation applicables

1.4.1.1. Bi-clés et certificats des porteurs

La présente PC traite des bi-clés et des certificats à destination de personnes morales pour créer ou vérifier des cachets électroniques dans le cadre d'échanges dématérialisés.

Aucun autre usage de la bi-clé n'est autorisé.

1.4.1.2 Bi-clés et certificat d'AC et de composantes

L'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (AC Racine de NETCOM GROUP).

La clé de signature de l'AC est utilisée pour signer les certificats générés par l'AC ainsi que les informations sur l'état des Certificats (LCR).

1.4.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies dans la présente PC et DPC. L'AC doit respecter ces restrictions et impose leur respect aux détenteurs, porteurs et utilisateurs de certificats. L'Autorité de Certification NETCOM GROUP décline toute responsabilité pour tout usage non explicitement autorisé.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

La société NETCOM GROUP est responsable de la PC. Ses coordonnées sont :

NETCOM GROUP SAS
41 rue Delizy
93500 PANTIN

1.5.2 Point de contact

Toute demande relative à la présente PC est à adresser à :
Par courrier postal :

Gestion de l'AC NETCOM GROUP
NETCOM GROUP SAS
41 rue Delizy
93500 PANTIN

Par courriel : contact-certinet@netcom-group.fr

1.5.3 Procédures d'approbation de la conformité de la DPC

Le Comité de Pilotage évalue selon ses propres critères la conformité du présent document. Il approuve les résultats des audits de conformité réalisés par les experts mandatés par lui.

1.6 Définitions et acronymes

1.6.1 Acronymes

AC Autorité de Certification
ACD Autorité de Certification Déléguée
ACR Autorité de Certification Racine
AE Autorité d'Enregistrement
ANSSI Agence Nationale de la Sécurité des Systèmes d'information
CGU Conditions Générales d'Utilisation
DN Distinguished Name
DPC Déclaration des Pratiques de Certification

eIDAS electronic IDentification, Authentication and trust Services
HSM Hardware Security Module (module cryptographique)
IDS Intrusion Detection System
IGC Infrastructure de Gestion de Clés
LAR Liste des certificats d'AC Révoqués
LCR Liste des Certificats Révoqués
OCSP Online Certificate Status Protocol
OID Object Identifier
PE Politique d'Enregistrement
PC Politique de Certification
PSCE Prestataire de Services de Certification Électronique
PSGP Politique de Signature et Gestion des Preuves
RCC Responsable du Certificat de Cachet
RSA Rivest Shamir Adelman
URL Uniform Resource Locator

1.6.2 Définitions

Les termes utilisés dans la présente PC sont les suivants :

Autorité d'Enregistrement (AE) - Au sein d'un PSCE, une Autorité d'Enregistrement a en charge, au nom et sous la responsabilité de ce PSCE, l'enregistrement des porteurs, la vérification de leur identité et le recueil des demandes de certificat et de renouvellement en application d'au moins une politique de certification.

Autorité de Certification (AC) - Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur, dans les certificats émis au titre de cette politique de certification.

Bi-clé - Une bi-clé est une clé électronique constituée d'une clé publique et d'une clé privée, mathématiquement liées entre elles, utilisées dans des algorithmes de cryptographie dits à clé publique ou asymétrique telle que la signature électronique.

Certificat électronique - Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Clé privée - clé de la bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité.

Clé publique - clé de la bi-clé asymétrique d'une entité qui peut être rendue publique.

Comité de Pilotage - le Comité de Pilotage est un comité interne à NETCOM GROUP qui est en charge du bon fonctionnement de l'IGC NETCOM GROUP.

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

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

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

Fonction de génération des certificats - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du RCC de la fonction de génération des éléments secrets du RCC. Fonction de génération des éléments secrets du RCC - Cette fonction génère la bi-clé du RCC.

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

Fonction de publication - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux RCC et/ou aux utilisateurs de certificats, hors informations d'état des certificats.

Fonction d'information sur l'état des certificats - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR).

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

Modules cryptographiques - dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée utilisée pour conserver et mettre en œuvre la clé privée d'AC, les bi-clés des RCC et réaliser des opérations cryptographiques.

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

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

Prestataire de services de certification électronique (PSCE) - Un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des RCC et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles).

Responsable du Certificat de Cachet - Voir au chapitre 1.3.5

Utilisateur de certificat – Voir au chapitre 1.3.4

2. REPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1 Entités chargées de la mise à disposition des informations

NETCOM GROUP a mis en place une page regroupant les publications à l'adresse suivante :

https://certinet.netcom-group.fr

2.2 Informations devant être publiées

NETCOM GROUP publie, pour cette AC, les informations suivantes :

- La politique de certification ;
- La liste de révocation (LCR) ;
- Le certificat de l'AC et de son AC Racine ;
- Les CGU pour les certificats qualifiés de cachet.

Les PC et les certificats sont accompagnés d'une empreinte (algorithme SHA256) permettant d'en vérifier l'intégrité. Un espace du lieu de publication est réservé à l'archivage des anciennes versions des données publiées.

2.3 Délais et fréquences de publication

Les délais et fréquences de publication sont les suivants:

- La PC est publiée avant toute émission d'un certificat final contenant l'OID correspondant ;
- Les LCR sont publiées quotidiennement ;
- Les certificats d'AC sont publiés suite à leur émission et avant toute signature d'un certificat final ;
- Les CGU sont publiées suite à chacune de leur mise à jour.

Le Comité de Pilotage NETCOM GROUP décide des différentes parties (utilisateurs, organismes de contrôle...) à informer lors de la publication effective ou à venir d'une nouvelle PC (version initiale ou modification d'une PC existante) selon la nature des évolutions apportées.

2.4 Contrôle d'accès aux informations publiées

Toutes les informations publiées indiquées ci-dessus, sont publiques et ne sont accessibles qu'en lecture.

L'accès en modification aux données publiées est restreint aux équipes internes NETCOM GROUP en charge de publier les informations sur l'espace de publication. Un contrôle d'accès fort et nominatif est mis en place dans ce cadre.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500. Dans chaque certificat X509v3, l'AC (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" (DN) conforme aux exigences de la norme ETSI EN 319 412.

3.1.2 Nécessité d'utilisation de noms explicites

Les informations portées dans le champ "Subject" du certificat désignent de manière explicite la personne morale détentrice du certificat, via les attributs suivants :

Champs de base	Valeur
Common name	Nom de la personne morale sujet du certificat associé, de manière optionnel, au nom d'un service applicatif
Organization identifier	Identifiant de la personne morale sujet du certificat formaté selon la norme EN 319 412-2. Pour une entité immatriculée en France, cet identifiant est de la forme NTRFR-SIREN
Organization	Nom de l'entité (raison sociale) tel qu'indiqué dans les registres officiels utilisés pour l'enregistrement
Country	Code ISO 3166-1 sur 2 lettres du pays d'immatriculation de l'entité

3.1.3 Anonymisation ou pseudonymisation des porteurs

L'anonymat ainsi que les pseudonymes ne sont pas autorisées.

3.1.4 Règles d'interprétation des différentes formes de noms

Les attributs des noms des sujets sont basés sur documents officiels justifiant de l'existence de la personne morale (typiquement le Kbis). Le formatage du champ « Organization identifier » est décrit dans la norme EN 319 412-2.

3.1.5 Unicité des noms

Pour assurer l'unicité des noms, l'AE vérifie que, pour l'entité identifiée dans l'attribut OI du DN, le nom de service fourni dans le champ CN n'a pas déjà été utilisé pour un service distinct.

3.1.6 Identification, authentification et rôle des marques déposées

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L. 711-1 et suivants du Code de la Propriété intellectuelle (codifié par la loi n° 92-957 du 1er juillet 1992 et ses modifications ultérieures) appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires. L'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par la communauté d'utilisateur et les clients des marques déposées, des marques notoires et des signes distinctifs, ainsi que des noms de domaine.

3.2 Validation de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

La preuve de la possession de la clé privée par le porteur est fournie sous la forme d'une CSR contenant la clé publique signée par la clé privée.

3.2.2 Validation de l'identité d'un organisme

L'identité de la personne morale sujet du certificat est vérifiée au moyen de toute pièce valide lors de la demande de certificat (extrait Kbis ou certificat d'identification au répertoire national des entreprises et de leurs établissements ou inscription au répertoire des métiers…) attestant de l'existence de l'entité et portant le numéro SIREN de celle-ci ou, à défaut, une autre pièce attestant l'identification unique de l'entité qui figurera dans le certificat.
L'authenticité des informations de la demande du certificat est vérifiée en comparant celles-ci aux informations recueillies dans les bases de données officielles de référence.

3.2.3 Validation de l'identité d'un porteur

L'identité du porteur (RCC) est vérifiée par l'examen d'une pièce d'identité présentée en face à face physique. Les pièces d'identité acceptées sont les titres authentiques en cours de validité parmi les suivants :

- Carte nationale d'identité ;
- Passeport ;
- Carte de séjour.

3.2.4 Informations non vérifiées du porteur

Sans objet.

3.2.5 Validation de l'autorité d'un porteur

La validation de l'autorité du porteur (RCC) à demander un certificat pour le compte de l'entité est vérifiée avec :

- Pour une entreprise : une habilitation du RCC, sous la forme d'une délégation de pouvoirs, à demander des certificats pour le compte de l'entité, signée par le représentant légal (si le RCC n'est pas lui-même le représentant légal) ou une personne autorisée ;
- Pour une administration : toute pièce valide lors de la demande de certificat, portant délégation ou subdélégation de l'autorité responsable de la structure administrative ;

3.2.6 Certification croisée d'AC

Sans objet.

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

Le renouvellement de certificat, impliquant un renouvellement de la bi-clé, est réalisé conformément aux procédures initiales.

3.4 Identification et validation d'une demande de révocation

La demande de révocation doit être réalisée avec un formulaire dédié signé par le demandeur et adressé à l'autorité d'enregistrement.

L'opérateur d'enregistrement des certificats de cachet vérifie la signature du formulaire et recontacte le demandeur ou le responsable légal de l'entité détentrice du certificat afin d'authentifier l'origine de la demande et l'autorité du demandeur. Des informations issues du dossier d'enregistrement peuvent être utilisées pour cette vérification d'identité.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Toute demande de certificat est déposée directement auprès de l'Autorité d'Enregistrement par le RCC.

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

Le RCC doit :

- Générer la bi-clé de cachet puis la CSR conformément aux exigences de cette PC (voir 6.1);
- Réunir les pièces justificatives de l'identité de la personne morale sujet du certificat et de l'habilitation du RCC à demander le certificat ;
- Signer le formulaire de demande, le formulaire de consentement au recueil des données personnelles ainsi que les conditions générales d'utilisation du certificat ;
- Se présenter devant l'AE avec un justificatif d'identité.

4.2 Traitement d'une demande de certificat

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

L'autorité d'enregistrement s'assure de la conformité de la demande et de l'authenticité des justificatifs présentés. La demande doit comprendre :

- Les pièces justificatives de l'identité de la personne morale sujette du certificat ;
- L'habilitation du RCC à demander le certificat (délégation de pouvoirs) ;
- Le formulaire de demande ;
- Le formulaire de consentement au recueil des données personnelles par lequel le RCC donne son accord à la conservation de son titre officiel d'identité pour la demande et une éventuelle révocation ;
- Le justificatif d'identité du RCC ;
- La CSR.

4.2.2 Acceptation ou rejet de la demande

Si l'autorité d'enregistrement ne détecte aucun problème, elle valide les informations contenues dans la demande et transmet cette dernière au service de génération des certificats.

4.2.3 Durée d'établissement des certificats

Dès la demande de certificat reçue par le service de génération des certificats, le certificat est établi.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Après avoir authentifié l'origine et vérifié l'intégrité de la demande provenant de l'Autorité d'Enregistrement, l'AC déclenche le processus de génération du Certificat.

Une fois généré, l'opérateur AC envoie le certificat produit à l'opérateur AE qui le transmet au RCC par courriel.

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

Le RCC est prévenu par courriel ainsi que par un message de type SMS de la mise à disposition du certificat par l'autorité d'enregistrement.

4.3.3 Durée de vie du certificat

La durée de vie des certificats est de 10 ans maximum, conformément aux exigences des normes ETSI et de l'ANSSI.
La fin de validité du certificat de cachet ne peut en aucun cas dépasser la période de validité du certificat de l'AC.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Le RCC doit signifier à l'AE, par courrier ou email, son acceptation du certificat après en avoir vérifié le contenu. Un certificat refusé par le RCC ou non accepté dans un délai de trente (30) jours après sa mise à disposition est révoqué par l'AC.
Toute utilisation du certificat vaut pour acceptation tacite de celui-ci.

4.4.2 Publication du certificat

L'AC ne publie pas les certificats de cachet émis. Le certificat est accessible dans chaque document signé avec celui-ci ou sur demande du RCC à l'AE.

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

L'AC envoie le certificat émis à l'AE.

4.5 Usage de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée et du certificat par le RCC est limitée à la création et à la vérification de cachet, usage indiqué dans le certificat (attribut key usage et). Le RCC et les utilisateurs du certificat sont tenus de vérifier la validité du certificat et la conformité de son utilisation.

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

L'utilisation de la clé publique et du certificat est limitée à la vérification de cachet, usage indiqué dans le certificat (attribut key usage et). Les utilisateurs du certificat sont tenus de vérifier la validité du certificat et la conformité de son utilisation.

4.6 Renouvellement d'un certificat

Le processus de renouvellement de certificat a lieu dans les mêmes conditions que la demande initiale de délivrance d'un certificat. Il est mis en œuvre de façon impérative au moins trois (3) mois avant que le certificat atteigne une durée de validité de trois (3) ans à compter de sa délivrance.

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

La cause principale de la délivrance d'un nouveau certificat est l'arrivée à la date de fin de validité du certificat. Les bi-clés doivent être en effet périodiquement renouvelées afin de minimiser les risques d'attaque cryptographique. Un renouvellement peut être aussi réalisé de manière anticipée, suite à un événement ou un incident déclaré par le porteur, les plus fréquents étant la perte des secrets d'activation ou une suspicion de compromission. Une modification des informations contenues dans le certificat entraîne également la délivrance d'un nouveau certificat (avec renouvellement de la bi-clé).

La délivrance d'un nouveau certificat est réalisée de manière identique au processus de délivrance initiale.

4.8 Modification du certificat

La modification d'un certificat émis n'est pas autorisée par cette PC. En cas de nécessité, un nouveau certificat doit être délivré après révocation de l'ancien.

4.9 Révocation 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 des présentes PC :

- Le certificat est refusé après sa délivrance ;
- Le certificat n'a pas confirmé la réception du certificat dans le délai de trente (30) jours prévu au titre de la présente politique
- La clé privée du certificat est perdue, compromise ou suspectée de compromission ;
- Les données d'activation de la clé ont été perdues compromises ou suspectées de compromission ;
- Les informations ou les attributs de l'entité figurant dans son 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 et ne sont plus considérés sûrs ;
- Il a été démontré que le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le certificat d'AC doit être révoqué ou a été révoqué ;
- L'entité demande la révocation après avoir cessé d'utiliser le certificat ;
- L'entité a cessé d'exister.

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.

Les causes de révocation ne sont jamais publiées.

4.9.2 Origine d'une demande de révocation

Les entités qui peuvent demander la révocation d'un certificat objet des présentes PC sont les suivantes :

- Le RCC du certificat ;
- Le responsable légal de l'entité détentrice du certificat ;
- L'AE ;
- L'AC.

4.9.3 Procédure de traitement d'une demande de révocation

La demande de révocation est réalisée par l'envoi d'un formulaire de demande à l'Autorité d'Enregistrement. Ce formulaire identifie sans ambiguïté le certificat à révoquer par l'indication des informations suivantes :

- Numéro de série et dates de validité du certificat ;
- Nom apparaissant dans le certificat ;
- Nom du RCC responsable du certificat.

Le formulaire doit préciser les informations de contact du RCC ou du responsable légal pour vérification de l'origine de la demande. L'autorité d'enregistrement peut utiliser les informations du dossier d'enregistrement pour effectuer cette vérification (signature par exemple). L'autorité d'enregistrement vérifie de plus l'applicabilité de la cause de révocation invoquée.

Après cette validation, le service de gestion des révocations transmet la demande au service d'état des certificats chargé d'ajouter le n° de série du certificat à révoquer dans les prochaines LCR à générer et à publier.

Une fois le certificat effectivement révoqué, l'opérateur d'enregistrement et de révocation contacte le RCC par téléphone pour l'informer de la révocation du certificat et lui adresse un courriel de confirmation de cette opération.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

La demande de révocation doit être formulée par le RCC ou le responsable légal dès connaissance de l'évènement correspondant.

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

Par nature, une demande de révocation doit être traitée en urgence. La fonction de gestion des révocations est disponible 24h/24h et 7j/7j. Toute demande de révocation d'un certificat de cachet doit être formulée par courriel à l'adresse contact-certinet@netcom-group.fr et sera traitée dans un délai inférieur à 24 heures. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

Une astreinte est mise en place afin de couvrir les demandes de révocation pendant les jours non ouvrables, congés et jours fériés.

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

Les utilisateurs des certificats doivent vérifier la non-révocation des certificats sur lesquels ils vont baser leur confiance. Cette vérification se fait en consultant les LCR publiées par l'AC.

Les certificats révoqués restent présents dans la LCR même après leur date d'expiration d'origine.

4.9.7 Fréquence d'établissement des LCR

Les LCR sont générées à minima, toutes les 24h. Chaque LCR contient la date et l'heure prévisionnelles de publication de la LCR suivante.

4.9.8 Délai maximum de publication d'une 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

Sans objet, se reporter au chapitre 4.10.2

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

Cf. chapitre 4.9.6

4.9.11 Autres moyens disponibles d'information sur les révocations

Aucun autre moyen n'est mis en œuvre.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée
En cas de compromission de sa clé privée ou de connaissance de compromission de la clé privée de l'AC ayant émis son certificat, le porteur doit interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.
La compromission de la clé privée de l'AC fera l'objet d'une information clairement diffusée sur le site Internet de l'AC.

4.9.13 Suspension de certificats

Les certificats ne peuvent être révoqués que de façon définitive. Il n'est pas envisagé de possibilité de suspension.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

Les services permettant de connaître le statut des certificats sont mis à disposition librement et gratuitement via le site Web de l'AC.

4.10.2 Disponibilité de la fonction

La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats est de 8 heures. La durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats est de trente-deux (32) heures.

4.10.3 Dispositifs optionnels

Sans objet

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

Les sites d'hébergement des services de certification NETCOM sont situés dans des locaux sécurisés.

5.1.2 Accès physique

Les zones hébergeant les systèmes informatiques de l'AC NETCOM GROUP sont physiquement protégées contre un accès extérieur non autorisé. La liste des personnels autorisés à y accéder existe et est limitée au strict besoin du bon fonctionnement du service. L'accès des personnels autorisés est contrôlé par un moyen physique et enregistré.

5.1.3 Alimentation électrique et climatisation

Des systèmes de protection de l'alimentation électrique et de la climatisation sont mis en œuvre afin d'assurer la continuité des services délivrés. Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et/ou constructeurs.

5.1.4 Exposition aux dégâts des eaux

Les systèmes informatiques de l'AC ne sont pas situés en zone inondable, ni du fait d'intempéries, ni du fait de tuyauteries défaillantes.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de protection contre les incendies mis en œuvre par l'IGC permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC, en matière de disponibilité.

5.1.6 Conservation des supports

Des sauvegardes des supports sont réalisées quotidiennement.
Les sites dans lesquels sont conservées les sauvegardes sont protégés contre les risques d'incendies et d'inondation. De plus, les accès physiques et logiques sont protégés et soumis à une gestion des droits et à une authentification forte.
S'il y a utilisation de documents papiers, ou de supports amovibles telles qu'un CD, une clé USB de stockage, un disque dur externe ou une carte à puce, ceux-ci seront conservés dans un coffre-fort accessible par le responsable du Comité de Pilotage.
Des procédures de gestion protègent les supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

5.1.7 Mise hors service des supports

La mise hors service des différents supports varie en fonction de leur nature. En ce qui concerne les documents papiers, les CD, les clés USB de stockage, les cartes à puce, ils seront broyés en fin de vie (fin d'utilisation ou obsolescence). Les supports de stockage seront vidés, puis détruits. Les HSM seront mis hors service en suivant les directives du constructeur.

5.1.8 Sauvegarde hors site

Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, disposent d'une sauvegarde hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.). Les fonctions de sauvegarde et de restauration seront effectuées par des administrateurs autorisés conformément aux mesures de sécurité procédurales.
Les sauvegardes hors sites sont réalisées dans un environnement sécurisé en accès physique et logique, et sécurisé contre les risques d'incendie et d'inondation.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

NETCOM GROUP met en œuvre les rôles suivants :

- **Responsable de sécurité** : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats ainsi que de la gestion des habilitations sur l'IGC ;
- **Ingénieur système et Administrateur HSM** : Il est chargé de l'installation et de la configuration technique des équipements informatiques des composants de l'IGC, de l'administration technique des systèmes et des réseaux des composantes de l'IGC, de l'exploitation des composantes de l'IGC, de la gestion de l'administration des HSM de l'AC ainsi que de la révocation d'urgence en période d'astreinte ;
- **Opérateur d'enregistrement et de révocation (opérateur AE)**: Il est chargé de vérifier les informations requises pour la délivrance d'un certificat de cachet ou sa révocation et approuve, en tant qu'autorité d'enregistrement, les demandes de délivrance de révocation des certificats de cachet ;
- **Opérateur de certification (opérateur AC)** : Cet opérateur de l'autorité de certification génère et révoque les certificats des AC sur la base de demandes approuvées par l'Autorité d'Enregistrement ;
- **Auditeur système** : L'auditeur système est chargé de procéder de manière régulière à l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

En plus de ces rôles de confiance au sein de l'IGC, une AC distingue en tant que rôle de confiance, les rôles de porteurs de parts de secrets d'IGC. Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés.

Toutes les personnes opérant un rôle de confiance au sein de l'IGC en sont notifiées, et acceptent formellement ce rôle préalablement à leur prise de fonction.

5.2.2 Nombre de personnes requises par tâche

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, il est demandé de répartir les fonctions sensibles sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC.

5.2.3 Identification et authentification pour chaque rôle

Toute personne intervenant dans le fonctionnement de l'IGC doit avoir préalablement reçu le rôle correspondant.
L'accès physique est autorisé aux seules personnes qualifiées. L'accès logiciel est protégé par des politiques de sécurité contraignantes, imposant une authentification forte au minimum pour les ingénieurs système, exploitants et opérateurs de certification.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Les cumuls suivants sont interdits :

- Opérateur d'enregistrement et Opérateur de certification ;
- Opérateur de certification et ingénieur système ou exploitant ;
- Auditeur système et ingénieur système ou exploitant.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Tout le personnel amené à travailler au sein de composantes de l'IGC est soumis à une clause de confidentialité vis-à-vis de NETCOM GROUP.
Le personnel amené à travailler au sein de l'IGC NETCOM GROUP, occupera un poste correspondant à ses compétences professionnelles. Le personnel occupant un rôle de confiance devra posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.

L'AC informe toutes les personnes intervenant dans des rôles de confiance de l'IGC :

- De ses responsabilités relatives aux services de l'IGC,
- Des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer

5.3.2 Procédures de vérification des antécédents

NETCOM GROUP s'assure de l'honnêteté de son personnel amené à travailler au sein de la composante en mettant en œuvre des moyens respectant le cadre légal et les réglementations en vigueur.

Ainsi, il est procédé à la vérification des curriculum vitae des collaborateurs lors de leur intégration tandis que leur comportement au sein de NETCOM GROUP fait également l'objet d'un contrôle.
En outre, ces personnes signent, lors de leur désignation à un rôle de confiance, une attestation sur l'honneur de ne n'avoir pas fait l'objet de condamnation pénale ou de poursuite judiciaire pour des agissements incompatibles avec leurs fonctions.
Enfin, NETCOM GROUP s'assure que les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications seront menées préalablement à l'affectation à un rôle de confiance.

5.3.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

5.3.4 Exigences en matière de formation continue et fréquences des formations

Le personnel concerné sera informé et disposera d'une formation adéquate préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.
Le personnel est régulièrement (annuellement) formé aux pratiques à l'état de l'art de la sécurité informatique et est formé à la gestion et à la remontée des incidents de sécurité.

5.3.5 Fréquence et séquence de rotations entre différentes attributions

La présente PC ne formule aucune exigence sur le sujet.

5.3.6 Sanctions en cas d'actions non autorisées

Les sanctions et procédures disciplinaires associées sont définies dans le règlement intérieur et la charte informatique fournie à l'ensemble des employés de NETCOM GROUP. Celles-ci sont plus ou moins importantes en fonction de l'impact que peut avoir une action non autorisée.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Toutes les exigences de la section 5.3 s'appliquent aux prestataires externes à qui serait confié un rôle de confiance.

5.3.8 Documentation fournie au personnel

Le personnel dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, il doit lui être remis la ou les politique(s) de sécurité l'impactant.

5.4 Procédures de constitution de données d'audit

5.4.1 Type d'évènement à enregistrer

Les fonctions mises en œuvre dans le cadre de l'IGC journalises les évènements tels que décrits ci-dessous, sous forme électronique. La journalisation est automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Traces d'activité (logs) des pare-feux et des routeurs ;
- Evènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements sont recueillis, par des moyens électroniques et/ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- Les actions de maintenance et de changements de la configuration des systèmes, qui sont journalisées dans un document électronique et/ou papier signé et horodaté ;
- Les changements apportés au personnel, qui sont journalisés dans un document électronique et/ou papier signé et horodaté ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les RCC,...), qui sont journalisées dans un document électronique et/ou papier signé et horodaté ;

En plus de ces exigences de journalisation communes à toutes les composantes et fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment :

- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation / rejet d'une demande de certificat ;
- Evènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- Génération des certificats des RCC ;
- Transmission des certificats aux RCC.
- 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 LCR.

Chaque enregistrement d'un évènement dans un journal doit contenir au minimum les champs suivants :

- Type de l'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;
- Date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) ;

- Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants :

- Destinataire de l'opération
- Nom du demandeur de l'opération ou référence du système effectuant la demande
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes)
- Cause de l'évènement
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat)

En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement

5.4.2 Fréquence de traitement des journaux d'évènements

Cf. chapitre 5.4.8 ci-dessous

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur les serveurs qui les ont produits pendant au maximum 90 jours. Ils sont archivés au minimum sous un délai de 1 mois.

5.4.4 Protection des journaux d'évènements

Les journaux d'évènements ne sont rendus accessibles qu'au personnel de confiance.

5.4.5 Procédure de sauvegarde des journaux d'évènements

L'ensemble des journaux d'événements sont sauvegardés quotidiennement

5.4.6 Système de collecte des journaux d'évènements

La collecte des journaux d'événements se fait au travers d'un système de centralisation des logs.

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

Aucune notification n'est délivrée suite à l'enregistrement d'un événement.

5.4.8 Evaluation des vulnérabilités

NETCOM GROUP procède ou fait procéder à une analyse des vulnérabilités. Pour ce faire, plusieurs éléments sont analysés:

- Une analyse des accès physiques, afin de détecter toute intrusion non autorisée ;
- Une analyse complète des journaux d'événements en vue d'une détection en échec d'événement ou d'opération est réalisée en continue. Le personnel disposant d'un rôle de confiance est notifié par mail lors qu'une anomalie est détectée

- Une analyse automatique via un outil de gestion des vulnérabilités. Un scan hebdomadaire est effectué et un rapport envoyé au personnel disposant d'un rôle de confiance.

5.5 Archivage des données

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage sont mises en place par l'ACP. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.
Les données à archiver sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques
- Les PC
- Les DPC
- Les certificats, LAR et LCR tels qu'émis ou publiés
- Les engagements signés par le responsable du Comité de Pilotage
- Les journaux d'évènements des différentes entités de l'IGC
- Les dossiers d'enregistrements
- La trace d'acceptation du certificat par le RCC

L'Opérateur d'enregistrement conserve dans un coffre-fort ainsi que d'une manière dématérialisée et sécurisée les documents suivants :

- les CGU signées par le RCC
- l'extrait KBIS de moins de trois mois
- La copie du titre officiel d'identité du RCC et, le cas échéant, de son mandataire
- Le formulaire de demande de certificat signée
- Le cas échéant, la délégation de pouvoir en faveur du mandataire
- Le formulaire de consentement au recueil de données personnelles

5.5.2 Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté sera archivé 10 ans pour les besoins de fourniture de la preuve de la démarche de certification dans des procédures légales.
La durée de conservation des dossiers d'enregistrement est portée à la connaissance du RCC dans les conditions générales d'utilisation.

Certificats, LAR et LCR émis par l'AC

Les certificats de cachet et d'AC, ainsi que les LCR / LAR produites, sont archivés pendant au moins 7 années après leur expiration.

Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 sont archivés pour une durée de 10 ans après leur génération.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, seront :

- Protégées en intégrité ;
- Accessibles seulement aux personnes autorisées ;

- Disponibles pour relecture et exploitation pendant toute la durée de l'archivage.

5.5.4 Procédure de sauvegarde des archives

L'archivage est réalisé soit de manière automatique, soit de manière manuelle par du personnel autorisé.
Ces archives sont dupliquées sur plusieurs data centers distincts afin de garantir leur disponibilité.

5.5.5 Exigences d'horodatage des données

Chaque évènement contient la date et l'heure précise de réalisation. Les archives quotidiennes sont horodatées via un procédé de datation sûre. Les composants en charge de la fonction de révocation sont synchronisés quotidiennement avec une source de temps UTC.

Le temps fourni par ce serveur de temps doit être utilisé pour établir l'heure :

- Du début de validité d'un certificat de l'AC;
- De la révocation d'un certificat de l'AC;
- De l'affichage de mises à jour de LCR.

5.5.6 Système de collecte des archives

Les systèmes de collecte des archives de NETCOM GROUP sont internes.

5.5.7 Procédures de récupération et de vérification des archives

Les archives peuvent être récupérées dans un délai maximum de 2 jours ouvrés. Seules les personnes occupant un rôle de confiance peuvent réaliser les opérations de récupération et de vérification des archives.

5.6 Changement des clés 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 de ce 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 doit être 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 doit être 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

Les procédures de génération d'un nouveau certificat d'AC sont décrites en section 6. L'AC informera les entités clientes, les RCC et les utilisateurs de la génération d'un nouveau certificat d'AC sur son site de publication.

5.7 Reprise suite à compromission et sinistre

5.7.1 Procédure de remontée et traitement des incidents et des compromissions

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation

de ses personnels et au travers de l'analyse des différents journaux d'événements. 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 la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé ...).

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

Conformément à l'analyse de risque qu'elle réalise, l'AC dispose d'un plan de continuité dans lequel sont décrites les procédures de reprise.

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

Ce point est couvert par les plans de continuité et de reprise d'activité. La compromission d'une clé de l'AC entraîne immédiatement la révocation des certificats délivrés. Dans ce cas, les différents acteurs et entités concernés (les RCC en particulier) seront avertis de cette révocation et informés de la conduite à tenir. Des mesures similaires sont prises si la robustesse de l'algorithme utilisé ou celle des paramètres utilisés par l'AC devient insuffisante pour les usages de l'AC.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de cette PC.

5.8 Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses. Par exemple, il se peut que l'entité propriétaire de l'AC fasse l'objet d'un rachat, d'une fusion, ou d'une transformation (changement de statut, de capital…).

L'AC dispose et maintient à jour un plan de cessation ou de transfert d'activité afin de garantir aux porteurs et utilisateurs des certificats un impact minimal. En particulier, ce plan prévoit :

- En cas d'expiration ou de cessation d'activité de l'AC :
  - La révocation de l'ensemble des certificats non expirés émis par cette AC ;
  - La génération et la publication d'une dernière liste de révocation ayant comme date de fin de validité le 31 décembre 9999, 23h59m59s ;
- Le maintien de la disponibilité des informations nécessaires à la vérification des certificats qu'elle a émis (chaines de certificats de l'AC, informations de révocation), par les moyens propres de NETCOM GROUP ou à défaut par une tierce partie. L'AC s'efforcera de garantir la publication des informations aux adresses nominales définies par la PC, et à défaut informera les porteurs et utilisateurs des certificats des modalités de récupération de ces éléments ;
- L'information préalable des clients, des porteurs et utilisateurs de certificats, ainsi que des tierces parties impactées et liées à l'AC, de la cessation ou du transfert d'activité à venir ;
- L'information des organismes d'audit ayant certifié l'AC, et de l'organe de contrôle national (ANSSI) ;

- La clôture des autorisations et des contrats avec des fournisseurs ou sous-traitants prenant part à la fourniture du service de certification de l'AC et dont les activités ne sont plus nécessaires ;
- Le maintien du service d'archivage de tous les éléments de preuve conservés au titre de la présence PC (dossiers d'enregistrement, informations de statut de révocation des certificats et journaux d'événements) pour l'entièreté de la durée prévue, par les moyens propres de NETCOM GROUP ou à défaut par une tierce partie ;
- La destruction définitive des clés privées des composantes de l'AC (en particulier la clé privée de signature de l'AC) et de toutes leurs copies afin qu'elles ne puissent plus être utilisées ;
- La définition des dispositions nécessaires pour couvrir les coûts permettant de respecter les exigences minimales dans le cas où l'AC serait en faillite ou, pour d'autres raisons, serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

En cas de cessation d'activité, l'AC s'efforce d'identifier d'autres AC susceptibles de se voir transférer l'activité ou de fournir des solutions de niveau équivalent aux porteurs disposant de certificats encore valides.

6. MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation de bi clés

6.1.1 Génération de bi clés

La génération et l'installation des données d'activation d'un module cryptographique de l'AC se fait lors de la phase d'initialisation et de personnalisation de ce module. Les données d'activation sont stockées sur des cartes à puce. Ces cartes sont fournies aux porteurs de secrets qui doivent les stocker de manière sécurisée, en les protégeant contre le vol, la détérioration, et l'utilisation non autorisée.

Les clés de l'AC sont générées :

- Lors d'une cérémonie des clés devant témoins ;
- Sous le contrôle d'au moins deux personnes ayant des Rôle de Confiance (voir 5.2.1) ;
- Dans des locaux sécurisés (voir 5.1.1) ;
- Au sein d'un HSM répondant aux exigences définies dans la section 6.2.11.

La génération des clés de l'AC est réalisée selon une procédure précise et donne lieu à la rédaction d'un procès-verbal en fin de cérémonie.

Les bi-clés à certifier des porteurs doivent être générées dans des dispositifs cryptographiques conformément aux exigences de l'Annexe 1 et des sections 6.1.5 et 6.1.6. Les clés publiques des porteurs sont transmises à l'AC dans les conditions prévues à la section 6.1.3.

6.1.2 Transmission de la clé privée au service de création de cachet

Sans objet

6.1.3 Transmission de la clé publique à l'AC

La clé publique de cachet est transmise à l'AE par le RCC lors de la demande de certificat, au format PKCS#10 et la transmission est authentifiée par l'AE. L'opérateur AE transmet cette clé en main propre à un opérateur AC.

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

Le certificat de l'AC est publié sur le site de publication décrit en section 2. Le certificat contient les informations figurant au chapitre 7 de la présente PC.

6.1.5 Tailles des clés

Les clefs d'AC ont ces caractéristiques :

- Algorithme utilisé : RSA.
- Taille minimale des clefs : 4096 bits.

Les clefs des certificats de cachet ont ces caractéristiques :

- Algorithme utilisé : RSA.
- Taille minimale des clefs : 4096 bits.

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

L'équipement de génération de bi-clés de l'AC est un module cryptographique conforme aux exigences du chapitre 6.2.1, paramétré et exploité conformément aux préconisations de son fournisseur, ce qui garantit la qualité des bi-clés générées.
Le RCC doit générer sa bi-clé dans un dispositif cryptographique conforme aux exigences de l'Annexe 1.

6.1.7 Objectifs d'usage de la clé

L'usage du certificat est rappelé en section 1.4.1.
Le Porteur s'engage à utiliser le certificat conformément :

- A la PC ;
- Aux conditions générales d'utilisation qu'il a accepté lors de la demande ;
- A l'extension KeyUsage ou tout autre extension contraignant l'utilisation de la clé, définie dans le certificat émis

Les utilisateurs sont tenues de :

- Déterminer que l'utilisation du certificat est conforme aux conditions prévues par la PC ;
- Déterminer que le certificat est utilisé en conformité avec l'extension KeyUsage définie dans celui-ci;
- Vérifier les dates de validité et le statut de révocation du certificat.

L'AC exclut toute responsabilité en cas d'utilisation du certificat non conforme à cette PC ou aux conditions générales d'utilisation.

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

Les modules cryptographiques utilisés par l'AC pour la génération et la mise en œuvre de ses clés de signature sont des modules cryptographiques matériels certifiés répondant aux exigences de la section 6.2.11. L'AC s'assure de la sécurité de ces modules tout au long de leur cycle de vie. En particulier, l'AC met en place les procédures nécessaires pour :

- S'assurer de leur intégrité durant leur transport depuis le fournisseur;
- S'assurer de leur intégrité durant leur stockage précédant la cérémonie des clés;
- S'assurer que les opérations d'activation, de sauvegarde et de restauration des clés de signature sont réalisées sous le contrôle de deux personnels ayant des Rôles de Confiance;
- S'assurer qu'ils sont en bon état de fonctionnement;
- S'assurer que les clés qu'ils contiennent sont détruites lorsqu'ils sont décommissionnés

Le dispositif cryptographique du RCC doit être conforme aux exigences de l'Annexe 1.

6.2.2 Contrôle des clés privées par plusieurs personnes

La clé privée de l'AC est contrôlée par des données d'activation stockées sur des cartes à puce remises à des porteurs de secrets lors de la cérémonie des clés. Un partage de secret du HSM est mis en œuvre par l'AC.
Le RCC doit s'assurer de la mise en place de mesures techniques et organisationnelles assurant l'usage de la clé privée de cachet par les seules personnes autorisées en conformité avec les exigences de l'Annexe 1.

6.2.3 Séquestre de la clé privée

Les clés privées ne font pas l'objet de séquestre

6.2.4 Copie de secours de la clé privée

Les clés privées de l'AC font l'objet de copies de sauvegarde :

- Soit hors d'un module cryptographique mais sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant offre un niveau de sécurité équivalent au stockage au sein du module cryptographique et, 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. Ces copies de sauvegarde des clés privées de l'AC sont stockées dans un coffre- fort sécurisé et accessible uniquement par des personnes ayant des Rôles de Confiance.
- Soit dans un module cryptographique équivalent opéré dans des conditions de sécurité similaires ou supérieures. Les sauvegardes sont réalisées sous le contrôle de deux personnes ayant des Rôles de Confiance.

Toute copie de secours de la clé privée de cachet du RCC doit garantir le même niveau de sécurité que le dispositif cryptographique utilisé pour sa génération.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC ne sont pas archivée. Les clés privées des porteurs ne sont pas archivées ni par l'AC ni par aucune des composantes de l'IGC.

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

Pour les clés privées d'AC, tout transfert se fera sous forme chiffrée, conformément aux exigences précitées.

En dehors des copies de secours, les clés privées de l'AC sont générées dans son module cryptographique et ne sont donc pas transférées. Lors de la génération d'une copie de secours, le transfert opéré met en place un mécanisme de chiffrement permettant de garantir qu'aucune information sensible ne transite de manière non sécurisée

6.2.7 Stockage de la clé privée dans le module cryptographique

Les clés privées d'AC sont stockées dans un module cryptographique répondant aux exigences du chapitre 6.2.11 pour le niveau de sécurité considéré.

6.2.8 Méthode d'activation de la clé privée

L'activation des clés privées est contrôlée par des données spécifiques dites données d'activation. Pour l'AC, elle est réalisée au sein d'un module cryptographique répondant aux exigences du chapitre 6.2.11 sous le contrôle de deux personnes ayant des Rôles de Confiance.
L'activation de la clé privée de cachet du RCC est contrôlée via des données d'activation qui lui sont propres et permet de répondre aux exigences définies à l'Annexe 1.

6.2.9 Méthode de désactivation de la clé privée

Pour l'AC la désactivation de la clé privée s'opère lors de l'arrêt du module cryptographique.
Le RCC met en œuvre les conditions de désactivation de la clé privée de cachet permettant de répondre aux exigences définies à l'Annexe 1.

6.2.10 Méthode de destruction des clés privées

La destruction de la clé privée de l'AC est effectuée à partir de son module cryptographique. L'AC s'assure que toutes les copies de secours correspondantes sont également détruites.
Le RCC est responsable de la destruction de la clé privée de cachet, de manière logique ou physique, en conformité avec les exigences définies à l'Annexe 1.

6.2.11 Niveau d'évaluation sécurité du module cryptographique

Le modules cryptographique de l'AC est qualifié au niveau renforcé par l'ANSSI est évalué conformément aux critères communs au niveau minimum EAL4+ et correspondant à l'usage visé.
L'AC ne remet pas de dispositif de création de signature aux Porteurs.

6.3 Autres aspects de la gestion des bi clés

6.3.1 Archivage des clés publiques

Les clés publiques des AC sont archivées pendant 10 ans après l'expiration des certificats correspondants.

6.3.2 Durée de vie des bi clés

La durée de vie des Bi-clés et des Certificats diffère selon le type de Certificat. La taille des Bi-clés a été prise en compte lors de la définition de ces durées de vie, conformément aux exigences cryptographique exprimées dans la norme ETSI TS 119312 ou dans les recommandations ANSSI.
Le certificat de l'AC Racine a une durée de vie de 20 ans.
Le certificat de l'AC Déléguée a une durée de vie de 10 ans.
L'AC ne peut émettre des Certificats porteurs dont la durée de vie excéderait celle du Certificat de l'AC utilisé pour l'émission. Le certificat de cachet a une durée de vie de 3 ans, sauf cas d'expiration prochaine de l'AC.
Pour le certificat de l'AC Racine, les bi-clés seront renouvelées à l'expiration d'un délai de 7 ans tandis que pour l'AC déléguée, elles seront renouvelées à compter d'un délai de 3 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Les données d'activation de la clé de l'AC sont générées durant la cérémonie des clés. Ces données d'activation sont stockées sur des cartes à puce et remises à des porteurs de secret. Chaque porteur de secrets prend les mesures nécessaires pour se prémunir contre la perte, le vol, l'utilisation non autorisée ou la destruction non autorisée de sa carte à puce et des données d'activation qu'elle contient.
Le RCC génère les données d'activation de la clé privée de cachet en cohérence avec les exigences de l'Annexe 1 applicables à son dispositif cryptographique.

6.4.2 Protection des données d'activation

Les données d'activation de l'AC sont stockées sur une carte à puce nominative et personnelle. La responsabilité de cette carte à puce incombe à la personne à qui la carte est remise. La carte est protégée par un code PIN personnel au porteur de secret. Les cartes à puce sont ensuite stockées dans un coffre-fort sécurisé individuel. Chaque porteur de secret est responsable de sa part de secret d'activation. Il exprime son consentement en signant un formulaire définissant ses responsabilités.
Le RCC est responsable de la protection des données d'activation de la clé privée de cachet dans le respect des exigences de l'Annexe 1 applicables à son dispositif cryptographique.

6.4.3 Autres aspects liés aux données d'activation

La transmission des cartes à puce, contenant des données d'activation de l'AC, d'un porteur de secret vers un nouveau porteur de secret doit être réalisée de façon à protéger les données d'activation contre la perte, le vol, la modification, la divulgation non autorisée ou l'utilisation non autorisée de ces données.
Les données d'activation de l'AC sont décommissionnées de façon à se prémunir du vol, de la perte, de la modification, de la divulgation non autorisée ou de l'utilisation non autorisée de ces données.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

NETCOM GROUP a réalisé et maintient une analyse de risque concernant les processus et les infrastructures mis en œuvre dans le cadre de l'IGC. De celle-ci découle une politique de sécurité des systèmes d'information applicable à l'IGC et le suivi d'un plan de traitement des risques.

L'analyse de risque est revue régulièrement, à minima annuellement, et lors de toute évolution significative d'un système ou d'une composante d'un service de confiance. L'analyse de risque est approuvée formellement par la direction de NETCOM GROUP dans le cadre d'une homologation de sécurité. La direction accepte à cette occasion les risques résiduels identifiés.

Les objectifs de sécurité suivants sont en particulier traités :

Identification et authentification

Les systèmes, applications et bases de données identifient et authentifient de façon unique les utilisateurs. Toute interaction entre le système et un utilisateur n'est possible qu'après une

identification et une authentification réussies. Pour chaque interaction, le système peut établir l'identité de l'utilisateur qui interagit. Les informations d'authentification sont stockées de façon à ce qu'elles soient uniquement accessibles par les utilisateurs autorisés.

Contrôle d'accès

Les profils et droits d'accès aux équipements de l'AC sont définis et documentés. Ils comprennent également les procédures d'enregistrement et de désenregistrement des utilisateurs. Les systèmes, applications et bases de données sont définis de manière à distinguer et administrer les droits d'accès de chaque utilisateur, au niveau d'un utilisateur, au niveau de l'appartenance à un groupe d'utilisateurs ou aux deux niveaux. Il est ainsi possible de :

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

Tout utilisateur non autorisé ne peut accorder ou retirer des droits d'accès à un objet. De même, seuls les utilisateurs autorisés peuvent créer de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants. Les systèmes et applications gèrent des sessions de connexion, avec déconnexion automatique après un temps d'inactivité, afin de garantir que seul l'utilisateur connecté a accès aux fonctions et informations autorisés à l'authentification.

Administration et exploitation

L'utilisation de programmes utilitaires est restreinte et contrôlée sur les infrastructures de l'AC. Les procédures opérationnelles d'administration et 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 divulgation des informations sensibles qu'ils peuvent détenir. Les matériels sensibles de l'AC font l'objet de procédure de maintenance afin de garantir la disponibilité des fonctions et des informations. Les procédures associées sont documentées. Les personnels concernés par ces procédures sont désignés par la direction de l'AC. Des mesures de contrôles des actions de maintenance sont mises en application.

Intégrité des composantes

Les composantes du réseau local sont maintenues dans un environnement physiquement sécurisé. Des vérifications périodiques de conformité de leur configuration sont effectuées. Les correctifs de vulnérabilités sont appliqués, après qualification, dans un délai raisonnable suivant leur parution.

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 les différentes composantes (voir section 6.7).

Journalisation et audit

Un suivi d'activité est possible à partir des journaux d'événements. Il permet notamment d'informer les personnes concernées lorsqu'un incident de sécurité est détecté

Supervision et contrôle

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

Sensibilisation

L'AC met en œuvre des procédures appropriées de sensibilisation des personnels.

6.5.2 Niveau d'évaluation de sécurité des systèmes informatiques

Une surveillance de la qualification des matériels cryptographiques de l'AC est mise en place. Elle a lieu au minimum une fois par an.

6.6 Mesures de sécurité liées au développement des systèmes

6.6.1 Mesures liées à la gestion de la sécurité

L'AC s'assure, lors de la mise en production d'un élément logiciel, de son origine et de son intégrité et assure une traçabilité de l'ensemble des modifications apportées sur son système d'information. Les infrastructures de développement et d'essai sont distinctes des infrastructures de production de l'AC.

L'AC s'assure que la mise à jour des logiciels est réalisée de façon à assurer la sécurité du système. L'AC s'assure que le service met en œuvre une politique de révision des composants techniques à intervalles définis Les mises à jour sont réalisées par des personnels ayant un Rôle de Confiance de l'AC.

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 sécurité réseau

L'ensemble des exigences et pratiques décrites dans la politique de certification s'applique.

Les AC soumises à la présente PC, sont des AC en ligne déployées dans un environnement physiquement sécurisé et périodiquement audités. Des dispositifs de protection du réseau (pare-feux, solutions de détection d'intrusion (IDS), VPN) contribuent à la sécurité du réseau. Les flux non explicitement autorisés sont interdits par défaut. Le réseau d'administration des systèmes informatiques et logiquement séparé du réseau d'exploitation. Des postes d'administration, sécurisés spécifiquement, sont dédiés à l'administration système. La redondance des accès sur les services exposés sur Internet est assurée. La configuration des équipements réseau est périodiquement auditée. Des tests d'intrusion sont réalisés de façon périodique. (À voir avec Samuel)

6.8 Horodatage / système de datation

L'ensemble des serveurs de l'AC est synchronisé avec la même source de temps (UTC) au moins une fois par jour. La synchronisation des serveurs est régulièrement contrôlée.

7. PROFILS DES CERTIFICATS, ET DES LCR

7.1 Certificats de cachet

Les certificats qualifiés de cachet émis pour les porteurs finaux ont le gabarit suivant :

Champs de base	Valeur du champ	
Version	3	
Numéro de série	Numéro unique sur 16 octets	
Sujet (cf. 3.1)	CN = <Service (optionnel) - > <Nom de l'entité> OI = <identifiant normalisé de l'entité> O = <Nom de l'entité> C = <Code de pays d'immatriculation de l'entité>	
Emetteur	CN = NETCOM GROUP - SEAL QUALIFIED CA OI = NTRFR-453006314 O = NETCOM GROUP SAS C = FR	
Durée de validité	3 ans	
Algorithme de clé publique	RSA	
Longueur des clefs	4096 bits	
Algorithme de signature	SHA512WithRSA	
Extensions	**Criticité**	**Valeur de l'extension**
Basic Constraints	N	CA : Faux
Key Usage	O	DigitalSignature
Extended Key Usage	N	Adobe AuthenticDocumentsTrust (OID 1.2.840.113583.1.1.5)
Certificate Policies	N	1. PolicyIdentifier : 1.3.6.1.4.1.56143.1.2.1.1 Qualifier : CPS = https://certinet.netcom-group.fr 2. PolicyIdentifier : 0.4.0. 194112.1.1
Authority Key Identifier	N	Hash SHA-1 de la clé publique du certificat de l'AC
Subject Key Identifier	N	Hash SHA-1 de la clé publique de ce certificat
Authority Information Access	N	accessMethod : id-ad-caIssuers accessLocation : http://certinet-crl1.netcom-group.fr/crt/certinetqualifsealca.crt http://certinet-crl2.netcom-group.fr/crt/certinetqualifsealca.crt
CRL Distribution Points	N	URI de téléchargement de la CRL de l'AC : http://certinet-crl1.netcom-group.fr/crl/certinetqualifsealca.crl http://certinet-crl2.netcom-group.fr/crl/certinetqualifsealca.crl
qcStatements	N	esi4- qcStatement-1 = id-etsi-qcsQcCompliance esi4- qcStatement-6 = id-etsi-qct-eseal

7.2 Certificat de l'AC

Le certificat de l'Autorité de Certification NETCOM GROUP - SEAL QUALIFIED CA a le gabarit suivant :

Champs de base	Valeur du champ
Version	3
Numéro de série	Numéro unique sur 16 octets
Sujet (cf. 3.1)	CN = NETCOM GROUP - SEAL QUALIFIED CA OI = NTRFR-453006314 O = NETCOM GROUP SAS C = FR

Emetteur	CN = NETCOM GROUP - ROOT CA OI = NTRFR-453006314 O = NETCOM GROUP SAS C = FR	
Durée de validité	10 ans	
Algorithme de clé publique	RSA	
Longueur des clefs	4096 bits	
Algorithme de signature	SHA512WithRSA	
Extensions	**Criticité**	**Valeur de l'extension**
Basic Constraints	O	CA : Vrai Longueur de chemin : 0
Key Usage	O	keyCertSign et crlSign
Certificate Policies	N	PolicyIdentifier : AnyPolicy (2.5.29.32.0)
Authority Key Identifier	N	Hash SHA-1 de la clé publique du certificat de l'AC Racine
Subject Key Identifier	N	Hash SHA-1 de la clé publique de ce certificat
Authority Information Access	N	accessMethod : id-ad-caIssuers accessLocation : http://certinet-crl1.netcom-group.fr/crt/certinetrootca.crt http://certinet-crl2.netcom-group.fr/crt/certinetrootca.crt
CRL Distribution Points	N	URI de téléchargement de la CRL de l'AC Racine : http://certinet-crl1.netcom-group.fr/crl/certinetrootca.crl http://certinet-crl2.netcom-group.fr/crl/certinetrootca.crl

7.3 Liste de révocation de l'AC

Les CRL émises par l'Autorité de Certification NETCOM GROUP - SEAL QUALIFIED CA ont le gabarit suivant :

Champs de base	**Valeur du champ**	
Version	1 (version 2)	
Emetteur	CN = NETCOM GROUP - SEAL QUALIFIED CA OI = NTRFR-453006314 O = NETCOM GROUP SAS C = FR	
This Update	Date de génération de la CRL	
Next Update	7 jours après la date de génération	
Algorithme de signature	SHA512WithRSA	
Liste	**Valeur du champ**	
Revoked Certificates	Serial Number : Numéro de série du certificat révoqué Revocation Date : Date de révocation	
Extensions	**Criticité**	**Valeur de l'extension**
Authority Key Identifier	N	Hash SHA-1 de la clé publique de l'AC
CRL Number	N	Numéro séquentiel de la liste
ExpiredOnCRL	N	Date d'émission de la première CRL (les certificats révoqués ne sont jamais retirés de la CRL)

7.4 Certificat de l'AC Racine

Le certificat de l'Autorité de Certification Racine NETCOM GROUP - ROOT CA a le gabarit suivant :

Champs de base	Valeur du champ	
Version	2 (version 3)	
Numéro de série	Numéro unique sur 16 octets	
Sujet (cf. 3.1)	CN = NETCOM GROUP - ROOT CA OI = NTRFR-453006314 O = NETCOM GROUP SAS C = FR	
Emetteur	CN = NETCOM GROUP - ROOT CA OI = NTRFR-453006314 O = NETCOM GROUP SAS C = FR	
Durée de validité	20 ans	
Algorithme de clé publique	RSA	
Longueur des clefs	4096 bits	
Algorithme de signature	SHA512WithRSA	
Extensions	**Criticité**	**Valeur de l'extension**
Basic Constraints	O	CA : Vrai Longueur de chemin : aucune
Key Usage	O	keyCertSign et crlSign
Authority Key Identifier	N	Hash SHA-1 de la clé publique de ce certificat
Subject Key Identifier	N	Hash SHA-1 de la clé publique de ce certificat

8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquences et/ ou circonstances des évaluations

Des audits sont effectués par l'AC :

- Soit par des collaborateurs en interne ;
- Soit par des prestataires externes spécialistes du domaine ;
- Soit par un responsable d'audit interne à l'AC.

Un audit de certification à la norme ETSI EN 319 411-2, est réalisé tous les 2 ans par un organisme accrédité.

Un contrôle de conformité à la PC en vigueur est effectué :

- Lors de la mise en œuvre initiale du système;
- Au moins une fois par année civile (audit interne);
- Lors de la surveillance ou du renouvellement des certifications, conformément aux procédures réglementaires en vigueur;
- Lorsqu'une modification significative est effectuée

8.2 Identité / qualification des évaluateurs

Les évaluateurs doivent s'assurer que les politiques, déclarations et services sont correctement mis en œuvre par l'AC et détecter les cas de non-conformité qui pourraient compromettre la sécurité du service offert. L'AC s'engage à mandater des évaluateurs dont les compétences sont éprouvées en matière de sécurité des systèmes d'information et spécialisés dans le domaine d'activité de la composante contrôlée.

8.3 Relations entre évaluateurs et entités évalués

L'AC désigne l'évaluateur autorisé à effectuer l'audit. L'AC garantit l'indépendance et l'impartialité de l'évaluateur.

8.4 Périmètre des évaluations

L'évaluateur procède à des contrôles de conformité de la composante auditée, sur toute ou partie de la mise en œuvre :

- De la PC;
- De la DPC;
- Des composants de l'AC.

Avant chaque audit, les évaluateurs proposeront au Comité de Pilotage une liste de composantes et procédures qu'ils souhaiteront vérifier. Ils établiront ainsi le programme détaillé de l'audit.

8.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'évaluateur et son équipe rendent au Comité de Pilotage, un avis parmi les suivants : "réussite", "échec", "à confirmer". Avis "échec" : L'équipe d'audit émet des recommandations à l'AC. Le choix de la mesure à appliquer appartient à l'AC. Avis "à confirmer",

l'équipe d'audit identifie les non conformités, et les hiérarchisent. Il appartient à l'AC de proposer un calendrier de résolution des non conformités. Une vérification permettra de lever les non conformités identifiées. Avis "réussite", l'AC confirme à la composante contrôlée la conformité aux engagements de la PC et de ses pratiques annoncées.

8.6 Communication des résultats

Les résultats des audits de conformité sont transmis au Comité de Pilotage et mis à la disposition des autorités en charge de la qualification et de la certification du service.

9. AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

Les tarifs sont définis dans les relations contractuelles liant le client et NETCOM GROUP.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

NETCOM GROUP a souscrit une assurance en responsabilité civile professionnelle couvrant ses prestations de PSCO auprès d'une compagnie d'assurance.
Il appartient à l'AC d'évaluer le risque financier devant être couvert.

9.2.2 Autres ressources

L'AC met en œuvre une politique administrative et financière visant à maintenir pendant toute la durée de son activité les ressources financières nécessaires pour remplir les obligations définies par la PC.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Se référer aux Conditions Générales d'Utilisation des certificats.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles :

- Les clés privées de l'AC ;
- Les données d'activation associées aux clés privées de l'AC ;
- Les journaux d'événements ;
- Les pièces justificatives des dossiers d'enregistrement ;
- Les rapports d'audit ;
- Les causes de révocation des Certificats ;
- Les procédures internes de l'AC ;
- Les plans de continuité, de reprise et d'arrêt d'activité.

9.3.2 Informations hors du périmètre des informations confidentielles

Le site de publication de l'AC et son contenu sont considérés comme public

9.3.3 Responsabilités en termes de protection des informations confidentielles

NETCOM GROUP s'engage à respecter la législation et la réglementation en vigueur sur le territoire français, en particulier le Règlement Général de Protection des Données (RGPD).

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

L'ensemble des exigences et pratiques décrites dans la présente politique s'applique.

A cet effet, l'Autorité d'Enregistrement collecte et traite les données d'identification et de contact des futurs porteurs, des entités et représentants de ces entités, contenues dans les dossiers d'enregistrement et dans les journaux conservés à titre de preuve.

9.4.2 Informations à caractère personnel

Les données d'enregistrement du porteur et des contacts habilités telles que fournies par le RCC sont des informations considérées comme personnelles.
Les personnes physiques peuvent exercer leur droit d'accès, de rectification et de modification des données à caractère personnel les concernant et détenues par NETCOM GROUP, mais ne peuvent en aucune cas demander la modification ou la suppression des données enregistrées dans le dossier de preuve du fait de leur nature de preuve en justice.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

NETCOM GROUP respecte, pour le traitement et la protection des données à caractère personnel, la loi française no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi no 2004-801 du 6 août 2004 [CNIL], et au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 [RGPD].

9.4.5 Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne sont pas divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

Les données personnelles peuvent être mis à la disposition de la justice en cas de besoin pour servir de preuve dans le cadre d'une procédure judiciaire.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par NETCOM GROUP sont protégés par la loi, règlement et autres conventions internationales applicables.

9.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes des services de confiance sont les suivantes :

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes 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 les politiques et pratiques du service, et les documents qui en découlent ;
- Respecter et appliquer les procédures internes ;

- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par NETCOM GROUP et l'organisme de qualification ;
- Respecter les accords ou contrats qui les lient entre elles ou aux porteurs ;
- 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'AC a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un service applicatif donné et que le RCC correspondant a accepté le certificat, conformément aux exigences du chapitre 4.4 ci-dessus ;
- Garantir et maintenir la cohérence de ses pratiques avec sa PC ;
- Prendre toutes les mesures raisonnables pour s'assurer que ses RCC sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un RCC et l'AC est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC ;
- S'assurer de la conformité de sa Politique de Certification avec les exigences de la qualification visée par celle-ci ;
- Générer et exploiter les clés de signature de l'AC dans des matériels cryptographiques qualifiées et selon les recommandations d'emploi associées.

9.6.2 Service d'enregistrement

L'AE a pour obligation de :

- Respecter les procédures d'enregistrement décrites dans la présente politique ;
- Assurer la confidentialité et l'archivage des dossiers d'enregistrement des porteurs ;
- Traiter les demandes de révocation selon les engagements décrits dans la présente politique.

9.6.3 RCC (Porteur)

Les RCC ont pour obligation de :
Protéger les moyens d'accès aux clés privées et aux Certificats ;

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protéger la clé privée du service applicatif dont il a la responsabilité par des moyens appropriés à son environnement ;
- Protéger les données d'activation de cette clé privée et, le cas échéant, les mettre en œuvre ;
- N'utiliser leurs certificats que pour les usages prévus et définis dans la présente politique ;
- Révoquer ou demander la révocation de leur certificat en cas de compromission ou de suspicion de compromission ;
- Révoquer ou demander la révocation de leur certificat en cas de compromission ou de suspicion de compromission de leur données d'activation associées ;
- Révoquer ou demander la révocation de leur certificat si celui contient des informations devenues obsolètes;
- Ne plus utiliser leur clé privée en cas de compromission ou suspicion de compromission;

- informer l'AC de toute modification concernant les informations contenues dans le certificat électronique ;
- Vérifier et respecter les obligations qui leur incombent décrites dans le présent document et dans les Conditions Générales d'Utilisation.

Avant d'accorder sa confiance à un certificat, le RCC ou tout autre personne autorisée de l'entité détentrice du certificat doit impérativement vérifier sa validité en consultant les Listes des Certificats Révoqués appropriées les plus récentes, ainsi qu'en vérifiant sa validité intrinsèque, en particulier sa date d'expiration et sa signature, et l'intégrité du certificat. Le défaut de suivi de cette obligation rendra l'entité détentrice du certificat seul responsable des risques de ses actions non conformes aux exigences de la présente politique, NETCOM GROUP ne garantissant, dès lors, plus aucune valeur juridique aux certificats qu'elle a émis et qui pourraient avoir été révoqués ou qui ne seraient pas valides.

9.6.4 Utilisateur de certificats

Les utilisateurs des Certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application qui l'utilise ;
- Vérifier et respecter les obligations qui leur incombent dans le présent document et dans les Conditions Générales d'Utilisation ;
- Pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'AC qualifiée, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation).

9.6.5 Autres participants

Sans objet.

9.7 Limite de garantie

L'AC en ligne s'engage à émettre des certificats en conformité avec le présent document, ainsi qu'avec l'état de l'art et de la technique. Aucune autre garantie n'est assurée.

9.8 Limite de responsabilité

La responsabilité de NETCOM GROUP en tant que tiers de confiance ne peut être engagée qu'en cas de non-respect prouvé de ses obligations.

NETCOM GROUP ne pourra être tenue responsable dans le cas d'une faute sur le périmètre d'une entité cliente ou d'un RCC, notamment en cas:

- D'utilisation d'un Certificat expiré;
- D'utilisation d'un Certificat révoqué;
- D'utilisation d'un Certificat dans le cadre d'une application autre que celles décrites au chapitre relatif à l'usage de la bi clé et du certificat décrit dans la présente politique.

NETCOM GROUP n'est d'une façon générale pas responsable des documents et informations transmises par l'entité cliente et ne garantit pas leur exactitude ni les conséquences de faits, actions, négligences ou omissions dommageables de cette entité, de son représentant ou du RCC. L'entité cliente s'interdit de prendre un engagement au nom et pour le compte du Tiers de confiance NETCOM GROUP auquel il ne saurait en aucun cas se substituer.

9.9 Indemnités

Les indemnités sont définies dans les relations contractuelles liant le client et NETCOM GROUP.

9.10 Durée et fin anticipée de la validité de la PC

9.10.1 Durée de validité

La présente politique est rendue effective une fois validée et publiée par l'entité responsable de ce document. Elle reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de celle-ci.

9.10.2 Fin anticipée

Cette politique reste en application jusqu'à l'entrée en vigueur d'une nouvelle version, après publication de celle-ci.

9.10.3 Effets de la fin de validité et clauses restant applicables

En dépit du remplacement de la présente politique par une nouvelle version, les derniers certificats émis lorsqu'elle était encore valide entraînent l'application du présent document auxdits certificats et aux différents acteurs et ce jusqu'à l'expiration des certificats en question.

9.11 Notifications individuelles et communications entre les participants

NETCOM GROUP publie, après sa validation, toute nouvelle version sur le site de publication décrit à la section 2.2.

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

L'AC procède aux évolutions ou modifications des termes de la présente politique qui lui apparaissent nécessaires pour l'amélioration de la qualité de service ou du niveau de sécurité, tout en restant conforme aux exigences requises par la qualification au niveau visé.
Le comité de pilotage doit valider ces modifications avant publication et entrée en vigueur, excepté pour des corrections mineures (par exemple typographiques).

9.12.2 Mécanisme et période d'information sur les amendements

En cas de changement nécessitant la modification de la présente politique, la nouvelle version est publiée et une information est notifiée sur le site de l'AC. NETCOM GROUP s'efforce de publier la nouvelle version au moins un mois avant son entrée en vigueur.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

En cas de changement jugé important, ayant un impact majeur sur le service, NETCOM GROUP affecte un nouvel OID à la nouvelle version de la politique.

9.13 Dispositions concernant la résolution des conflits

L'AC s'engage à consacrer ses meilleurs efforts à la résolution amiable des litiges, avant la saisie des juridictions compétentes décrites ci-dessous.

Les procédures de résolution des litiges sont détaillées dans les relations contractuelles liant le client et NETCOM GROUP.

9.14 Juridictions compétentes

L'ensemble des documents contractuels est soumis à la législation et à la réglementation en vigueur sur le territoire français.

9.15 Conformité aux législations et réglementations

La présente politique est conforme à la législation et à la réglementation en vigueur sur le territoire français.

9.16 Dispositions diverses

9.16.1 Accord global

Sans objet.

9.16.2 Transfert d'activités

Sans objet.

9.16.3 Conséquences d'une clause non valide

Sans objet.

9.16.4 Application et renonciation

Sans objet.

9.16.5 Force majeure

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

9.17 Autres dispositions

NETCOM GROUP s'assure que les activités qu'elle réalise dans le cadre de ses services de confiance sont non discriminatoires.

Annexe 1 : Exigences de sécurité du dispositif de création de cachet

Le dispositif de création de cachet, utilisé par le serveur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- Si la bi-clé du serveur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Générer un cachet qui ne peut être falsifié sans la connaissance de la clé privée ;

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques doivent être mises en place afin de :

- Détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- Garantir la confidentialité et l'intégrité de la clé privée ;
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif ;
- Assurer pour le serveur légitime uniquement la fonction de génération des cachets électroniques et protéger la clé privée contre toute utilisation par des tiers.