



IGC de la Gendarmerie nationale

POLITIQUE DE CERTIFICATION AC Machines Cachet serveur

HISTORIQUE DES MODIFICATIONS

Version	Date	Objet de la modification	Auteur	Statut
0.1	12/04/2017	Création	SEALWeb	Ébauche
0.2	20/09/2017	Correction adresse et OID	SEALWeb	Brouillon
0.3	22/09/2017	Relecture et corrections	BCOF/SGDC	Brouillon
1.0	25/09/2017	Validation	ST(SI) ² /SDAC COL GMD	Définitif
1.1	08/02/2018	Suppression des références à l'OCSP Modification du point de publication des documents relatifs à l'IGC Modification de l'url des certificatePolicies Modification du keyUsage	ADC DHN	Définitif
1.2	02/03/2018	Modification de la fréquence de génération de la CRL Corrections mineures	ADC DHN	Définitif
1.3	30/08/2018	Précision sur les vérifications portant sur la qualité des bi-clés et leurs paramètres de génération	ADC DHN	Définitif
1.4	20/01/2020	- Précision « Machine Cachet serveur » à la place de Machine (pour lever le doute sur les certificats SSL Serveur) - Modification de la durée d'indisponibilité de la fonction de révocation telle que prévue par le RGS** et par le contrat de service avec le STIG. - ajout du délai de création du certificat cachet serveur suite à l'acceptation de la demande par l'autorité d'enregistrement et réception du dossier par autorité de certification - ajout de l'information ANSSI contacté immédiatement en cas de révocation d'une composante de l'IGC - Ajout de la définition de l'autorité d'enregistrement cachet serveur	CNE CRZ	Projet
1.5	20/02/2020	Projet validé en COPIL le 20/02/2020	CNE CRZ	Définitif
1.6	15/05/2020	- Suppression d'un carré invisible qui tronque le texte - suppression 2 hyperliens incorrects (II.1) - ajout du processus de publication via Itop avec Gsop en copie pour mise à jour du script de contrôle d'intégrité (II.4) - BCSSI → BASSI - ajout précision usage CRL et non OCSP - ajout du script GSOP pour supervision des CRL - Mise à jour des rôles / ajout de la référence au document « rôles et responsabilités » - Ajout du renvoi des rôles incompatibles entre eux définis dans le	CNE CRZ	Projet

		document [GESTION ROLES] » - ajout du rôle d' autorité		
2.0	04/06/2020	Projet de PC dans le cadre de la qualification eIDAS : - ajout de la présence des certificats expirés dans les CRL - précision du script de surveillance des CRL (signature AC + présence certificats) - ajout RGS + eIDAS → III.1.2.2 ajout organizationIdentifier - Modification profil de certificat : → ajout URI de l'autorité émettrice (AuthorityInformationAccess) → ajout OrganizationIdentifier → Ajout du lien vers les pc sur le site internet de la gendarmerie. (permet l'accès de tous aux PC) → Extensions « QC Statements »	CNE CRZ	projet
2.1	12/06/2020	Version validée en COPIL	CNE CRZ	Définitif
2.2	07/07/2020	- Modification de la formulation II.1 et II.4 - IX.13 : Dispositions concernant la résolution de conflits → ajout mention IGGN + adresse mail - ajout d'utilisation de la clé des certificats : + DigitalSignature - formalisation du format des certificats de test - V.3.2 : vérification des antécédents judiciaires → remplacement de la vérification tous les 3 ans avec bulletin du casier jud, par le criblage initial + remontée des condamnations à l'institution - ajout destruction des disques dur par démagnétisation puis déchiquetage (V.1.7) - modification IX.5 : L'ensemble des moyens de l'infrastructure de gestion des clés respecte et applique la législation et la réglementation en vigueur sur le territoire français. - ajout du mécanisme et période d'information sur les amendements. (IX.12.2) - IX.1.6 : l'état est propre assureur - V.1.3 : suppression du terme « politique de sécurité de l'ARA, par le respect des normes en vigueur, qui correspond aux pratiques mises en place pour la sécurité des installations. - V.1.5 : Prévention et protection incendie.	CNE CRZ	projet

		<p>suppression du terme « politique de sécurité de l'ARA, par le respect des normes en vigueur, qui correspond aux pratiques mises en place pour la sécurité des installations.</p> <ul style="list-style-type: none"> - V.3.2 : procédures de vérification des antécédents. Mention d'une procédure dans la DPC. - V.2.3 identification et authentification pour chaque rôle : rajout de la mention des actions effectuées dans la DPC - V.1.6 : modification « L'AC doit faire » par « l'AC fait ». - IX.17 : L'AC n'a pas d'autres dispositions que celles exposées précédemment - IV.9.12 : L'AC n'autorise pas les suspensions de certificat. - V.3.5 : L'AC n'établit aucune de règle concernant la fréquence de rotation entre les différentes attributions - V.4.7 La notification de l'enregistrement des événements est réalisée lors de la signature des CGU. - V.4.6 : ajout : Les journaux d'événements sont centralisés dans un outils de collecte. - VI.4.3 : ajout « Il n'y a pas d'autres aspects lié aux données d'activation. » - VI.6.3 : ajout : « La DPC décrit les processus d'évaluation sécurité » - IX.2.2 : autre ressources financière : sans objet - IX.2.3 : ajout : Tout usage non explicitement permis est interdit et engage la responsabilité du responsable du certificat. - IX.3.2 : information hors confidentielle : ajout « Les informations publiques sont les politiques de certification, les certificats d'AC ainsi que les CRL». - V.5.4 : procédure de sauvegarde des archives → renvoi vers la DPC 		
2.3	12/11/2020	Validation en COPIL	CNE CRZ	Validée
2.4	08/01/2021	<p>- Modification URI de l'AC Racine gendarmerie URI=http://crl.gendarmerie.fr/ac-racine-gn-v3.crl URI=http://crl.gendarmerie.interieur.ader.gouv.fr/ac-racine-gn-v3.crl URI=http://crl.gendarmerie.interieur.gouv.fr/ac-racine-gn-v3.crl</p> <p>- Ajout S pour http d'accès aux informations de l'AC émettrice et aux</p>	CNE CRZ	Validée projet

		politiques de certification (PC)		
2.5	11/06/2021	Validation en COPIL	CNE CRZ	Validée
2.6	17/01/2022	- Mise à jour de la liste des AC - Correction de diverses coquilles	CNE CRZ	Projet
2.7	14/02/2022	Validation en COPIL	CNE CRZ	Validée
2.8	06/10/2022	I.4.5 : L'IGC GN ne fait pas appel à des mandataires de certification. IV.9 : - harmonisation de la description des fréquences de révocation IV.1.2 : - modification de la procédure de génération pour coller aux pratiques	CEN CRZ	Projet
2.9	14/10/2022	Validation	CEN CRZ	Validée

Table des matières

I. Introduction.....	13
I.1. Présentation générale.....	13
I.1.1. Objet du document.....	13
I.1.2. Architecture de l'IGC.....	13
I.2. Identification du document.....	14
I.3. Définitions et acronymes.....	14
I.3.1. Acronymes.....	14
I.3.2. Définitions.....	15
I.4. Entités intervenant dans l'IGC.....	17
I.4.1. Autorités de certification.....	17
I.4.2. Autorité d'enregistrement.....	18
I.4.3. Responsables de certificats électroniques de services applicatifs.....	19
I.4.4. Utilisateurs de certificats.....	19
I.4.5. Autres participants à l'IGC GN.....	19
I.5. Usage des certificats.....	19
I.5.1. Domaines d'utilisation applicables.....	19
I.5.2. Domaines d'utilisation interdits.....	20
I.6. Gestion de la PC.....	20
I.6.1. Entité gérant la PC.....	20
I.6.2. Point de contact.....	20
I.6.3. Entité déterminant la conformité d'une DPC avec cette PC.....	20
I.6.4. Procédures d'approbation de la conformité de la DPC.....	20
II. Responsabilités concernant la mise à disposition des informations devant être publiées.....	21
II.1. Entités chargées de la mise à disposition des informations.....	21
II.2. Informations devant être publiées.....	21
II.3. Délais et fréquences de publication.....	21
II.4. Contrôle d'accès aux informations publiées.....	22
III. Identification et authentification.....	23
III.1. Nommage.....	23
III.1.1. Types de noms.....	23
III.1.2. Nécessité d'utilisation de noms explicites.....	23
III.1.3. Pseudonymisation des services applicatifs.....	24
III.1.4. Règles d'interprétation des différentes formes de nom.....	24
III.1.5. Unicité des noms.....	24
III.1.6. Identification, authentification et rôle des marques déposées.....	24
III.2. Validation initiale de l'identité.....	24
III.2.1. Méthode pour prouver la possession de la clé privée.....	24

III.2.2. Validation de l'identité d'un organisme.....	24
III.2.3. Validation de l'identité d'un individu.....	25
III.2.4. Informations non vérifiées d'un RC ou d'un service applicatif.....	25
III.2.5. Validation de l'autorité du demandeur.....	25
III.3. Identification et validation d'une demande de renouvellement des clés.....	26
III.3.1. Identification et validation pour un renouvellement courant.....	26
III.3.2. Identification et validation pour un renouvellement après révocation.....	26
III.4. Identification et validation d'une demande de révocation.....	26
IV. Exigences opérationnelles sur le cycle de vie des certificats.....	27
IV.1. Demande de certificat.....	27
IV.1.1. Origine d'une demande de certificat.....	27
IV.1.2. Processus et responsabilités pour l'établissement d'une demande de carte.....	27
IV.2. Traitement d'une demande de certificat.....	27
IV.2.1. Exécution des processus d'identification et de validation de la demande.....	27
IV.2.2. Acceptation ou rejet de la demande.....	27
IV.2.3. Durée d'établissement du certificat.....	27
IV.3. Délivrance du certificat.....	27
IV.3.1. Actions de l'AC concernant la délivrance du certificat.....	27
IV.3.2. Notification par l'AC de la délivrance du certificat au RC.....	28
IV.4. Acceptation du certificat.....	28
IV.4.1. Démarche d'acceptation du certificat.....	28
IV.4.2. Publication du certificat.....	28
IV.4.3. Notification par l'AC aux autres entités de la délivrance du certificat.....	28
IV.5. Usages de la bi-clé et du certificat.....	28
IV.5.1. Utilisation de la clé privée et du certificat par le RC.....	28
IV.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat.....	28
IV.6. Renouvellement d'un certificat.....	28
IV.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé.....	29
IV.7.1. Causes possibles de changement d'une bi-clé.....	29
IV.7.2. Origine d'une demande d'un nouveau certificat.....	29
IV.7.3. Procédure de traitement d'une demande d'un nouveau certificat.....	29
IV.7.4. Notification au RC de l'établissement du nouveau certificat.....	29
IV.7.5. Démarche d'acceptation du nouveau certificat.....	29
IV.7.6. Publication du nouveau certificat.....	29
IV.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat.....	29
IV.8. Modification du certificat.....	29
IV.9. Révocation et suspension des certificats.....	30
IV.9.1. Causes possibles d'une révocation.....	30
IV.9.2. Origine d'une demande de révocation.....	30

IV.9.3. Procédure de traitement d'une demande de révocation.....	30
IV.9.4. Délai accordé au RC pour formuler la demande de révocation.....	31
IV.9.5. Délai de traitement par l'AC d'une demande de révocation.....	31
IV.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats.....	32
IV.9.7. Fréquence d'établissement et durée de validité des LCR.....	32
IV.9.8. Délai maximum de publication d'une LCR.....	32
IV.9.9. Exigences sur la vérification en ligne de la révocation et de l'état des certificats.....	32
IV.9.10. Autres moyens disponibles d'information sur les révocations.....	32
IV.9.11. Exigences spécifiques en cas de compromission de la clé privée.....	32
IV.9.12. Causes possibles d'une suspension.....	33
IV.9.13. Origine d'une demande de suspension.....	33
IV.9.14. Procédure de traitement d'une demande de suspension.....	33
IV.9.15. Limites de la période de suspension d'un certificat.....	33
IV.10. Fonction d'information sur l'état des certificats.....	33
IV.10.1. Caractéristiques opérationnelles.....	33
IV.10.2. Disponibilité de la fonction d'information sur l'état des certificats.....	33
IV.10.3. Dispositifs optionnels.....	33
IV.11. Fin de la relation entre le RC et l'AC.....	33
IV.12. Séquestre de clé et recouvrement.....	33
IV.12.1. Politique et pratiques de recouvrement par séquestre des clés.....	33
IV.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session.....	33
V. Mesures de sécurité non techniques.....	34
V.1. Mesures de sécurité physique.....	34
V.1.1. Situation géographique et construction des sites.....	34
V.1.2. Accès physique.....	34
V.1.3. Alimentation électrique et climatisation.....	34
V.1.4. Vulnérabilité aux dégâts des eaux.....	34
V.1.5. Prévention et protection incendie.....	34
V.1.6. Conservation des supports.....	34
V.1.7. Mise hors service des supports.....	35
V.1.8. Sauvegardes hors site.....	35
V.2. Mesures de sécurité procédurales.....	35
V.2.1. Rôles de confiance.....	35
V.2.2. Nombre de personnes requises par tâches.....	36
V.2.3. Identification et authentification pour chaque rôle.....	36
V.2.4. Rôles exigeant une séparation des attributions.....	36
V.3. Mesures de sécurité vis-à-vis du personnel.....	36
V.3.1. Qualifications, compétences et habilitations requises.....	36
V.3.2. Procédures de vérification des antécédents.....	37

V.3.3. Exigences en matière de formation initiale.....	37
V.3.4. Exigences et fréquence en matière de formation continue.....	37
V.3.5. Fréquence et séquence de rotation entre différentes attributions.....	37
V.3.6. Sanctions en cas d'actions non autorisées.....	37
V.3.7. Exigences vis-à-vis du personnel des prestataires externes.....	37
V.3.8. Documentation fournie au personnel.....	37
V.4. Procédures de constitution des données d'audit.....	37
V.4.1. Type d'événements à enregistrer.....	37
V.4.2. Fréquence de traitement des journaux d'événements.....	39
V.4.3. Période de conservation des journaux d'événements.....	39
V.4.4. Protection des journaux d'événements.....	39
V.4.5. Procédure de sauvegarde des journaux d'événements.....	39
V.4.6. Système de collecte des journaux d'événements.....	39
V.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement.....	39
V.4.8. Évaluation des vulnérabilités.....	39
V.5. Archivage des données.....	39
V.5.1. Types de données à archiver.....	39
V.5.2. Période de conservation des archives.....	40
V.5.3. Protection des archives.....	40
V.5.4. Procédure de sauvegarde des archives.....	40
V.5.5. Exigences d'horodatage des données.....	40
V.5.6. Système de collecte des archives.....	40
V.5.7. Procédures de récupération et de vérification des archives.....	41
V.6. Changement de clé d'AC.....	41
V.7. Reprise suite à compromission et sinistre.....	41
V.7.1. Procédures de remontée et de traitement des incidents et des compromissions.....	41
V.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données).....	42
V.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante.....	42
V.7.4. Capacités de continuité d'activité suite à un sinistre.....	42
V.8. Fin de vie de l'IGC.....	42
VI. Mesures de sécurité techniques.....	44
VI.1. Génération et installation de bi-clés.....	44
VI.1.1. Génération des bi-clés.....	44
VI.1.2. Transmission de la clé privée à son propriétaire.....	44
VI.1.3. Transmission de la clé publique à l'AC.....	44
VI.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats.....	45
VI.1.5. Tailles des clés.....	45
VI.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité.....	45
VI.1.7. Objectifs d'usage de la clé.....	45

VI.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques.....	45
VI.2.1. Standards et mesures de sécurité pour les modules cryptographiques.....	45
VI.2.2. Contrôle de la clé privée par plusieurs personnes.....	45
VI.2.3. Séquestre de la clé privée.....	45
VI.2.4. Copie de secours de la clé privée.....	45
VI.2.5. Archivage de la clé privée.....	46
VI.2.6. Transfert de la clé privée vers / depuis le module cryptographique.....	46
VI.2.7. Stockage de la clé privée dans un module cryptographique.....	46
VI.2.8. Méthode d'activation de la clé privée.....	46
VI.2.9. Méthode de désactivation de la clé privée.....	46
VI.2.10. Méthode de destruction des clés privées.....	46
VI.2.11. Niveau de qualification du module cryptographique et des dispositifs de protection des éléments secrets.....	47
VI.3. Autres aspects de la gestion des bi-clés.....	47
VI.3.1. Archivage des clés publiques.....	47
VI.3.2. Durées de vie des bi-clés et des certificats.....	47
VI.4. Données d'activation.....	47
VI.4.1. Génération et installation des données d'activation.....	47
VI.4.2. Protection des données d'activation.....	47
VI.4.3. Autres aspects liés aux données d'activation.....	48
VI.5. Mesures de sécurité des systèmes informatiques.....	48
VI.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques.....	48
VI.5.2. Niveau de qualification des systèmes informatiques.....	48
VI.6. Mesures de sécurité des systèmes durant leur cycle de vie.....	48
VI.6.1. Mesures de sécurité liées au développement des systèmes.....	48
VI.6.2. Mesures liées à la gestion de la sécurité.....	48
VI.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes.....	49
VI.7. Mesures de sécurité réseau.....	49
VI.8. Horodatage / Système de datation.....	49
VII. Profils des certificats et des LCR.....	50
VII.1. Format du certificat de l'AC GN Machines Cachet serveur.....	50
VII.2. Format des certificats de cachet des services applicatifs.....	51
VII.3. Format des listes de révocation (LCR) émises par l'AC GN Machines Cachet serveur.....	53
VII.4. Format des certificats de test de cachet des services applicatifs.....	53
VIII. Audit de conformité et autres évaluations.....	55
VIII.1. Fréquences et / ou circonstances des évaluations.....	55
VIII.2. Identités / qualifications des évaluateurs.....	55
VIII.3. Relations entre évaluateurs et entités évaluées.....	55
VIII.4. Sujets couverts par les évaluations.....	55

VIII.5. Actions prises suite aux conclusions des évaluations.....	55
VIII.6. Communication des résultats.....	55
IX. Autres problématiques métiers et légales.....	56
IX.1. Tarifs.....	56
IX.1.1. Tarifs pour la fourniture ou le renouvellement de certificats.....	56
IX.1.2. Tarifs pour accéder aux certificats.....	56
IX.1.3. Tarifs pour accéder aux informations d'état et de révocation des certificats.....	56
IX.1.4. Tarifs pour d'autres services.....	56
IX.1.5. Politique de remboursement.....	56
IX.2. Responsabilité financière.....	56
IX.2.1. Couverture par les assurances.....	56
IX.2.2. Autres ressources.....	56
IX.2.3. Couverture et garantie concernant les entités utilisatrices.....	56
IX.3. Confidentialité des données professionnelles.....	56
IX.3.1. Périmètre des informations confidentielles.....	56
IX.3.2. Informations hors du périmètre des informations confidentielles.....	57
IX.3.3. Responsabilités en termes de protection des informations confidentielles.....	57
IX.4. Protection des données à caractère personnel.....	57
IX.4.1. Politique de protection des données à caractère personnel.....	57
IX.4.2. Données à caractère personnel.....	57
IX.4.3. Données à caractère non personnel.....	57
IX.4.4. Responsabilité en termes de protection des données à caractère personnel.....	57
IX.4.5. Notification et consentement d'utilisation des données à caractère personnel.....	57
IX.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives.....	57
IX.4.7. Autres circonstances de divulgation de données à caractère personnel.....	57
IX.5. Droits de propriété intellectuelle.....	58
IX.6. Interprétations contractuelles et garanties.....	58
IX.6.1. Autorités de Certification.....	58
IX.6.2. Service d'enregistrement.....	59
IX.6.3. RC.....	59
IX.6.4. Utilisateurs de certificats.....	59
IX.6.5. Autres participants.....	59
IX.7. Limite de garantie.....	59
IX.8. Limite de responsabilité.....	59
IX.9. Indemnités.....	59
IX.10. Durée et fin anticipée de validité de la PC.....	59
IX.10.1. Durée de validité.....	59
IX.10.2. Fin anticipée de validité.....	60
IX.10.3. Effets de la fin de validité et clauses restant applicables.....	60

IX.11. Notifications individuelles et communications entre les participants.....	60
IX.12. Amendements à la PC.....	60
IX.12.1. Procédures d'amendements.....	60
IX.12.2. Mécanisme et période d'information sur les amendements.....	60
IX.12.3. Circonstances selon lesquelles l'OID doit être changé.....	60
IX.13. Dispositions concernant la résolution de conflits.....	60
IX.14. Juridictions compétentes.....	60
IX.15. Conformité aux législations et réglementations.....	61
IX.16. Dispositions diverses.....	61
IX.16.1. Accord global.....	61
IX.16.2. Transfert d'activités.....	61
IX.16.3. Conséquences d'une clause non valide.....	61
IX.16.4. Application et renonciation.....	61
IX.17. Autres dispositions.....	61
IX.17.1. Force majeure.....	61
X. Annexe 1 : Documents cités en référence.....	62
X.1. Réglementation.....	62
X.2. Documents techniques.....	62

I. Introduction

I.1. Présentation générale

I.1.1. Objet du document

La Gendarmerie nationale a mis en place et exploite une IGC, disposant d'une autorité de certification (AC) racine et d'AC subordonnées. L'IGC de la Gendarmerie nationale sera notée « IGC/GN » dans ce document.

Le présent document constitue la politique de certification (PC) de l'Autorité de Certification (AC) subordonnées « AC GN Machines Cachet serveur ».

Dans le cadre de cette politique de certification, cette AC émet des certificats de cachet pour des machines de la gendarmerie nationale.

Une PC est un ensemble de règles, identifié par un nom, qui définit les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et qui indique l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes.

Une PC décrit quelles sont les modalités de gestion et d'usage des certificats. Les pratiques mises en œuvre pour atteindre les garanties offertes sur ces certificats sont présentées dans un autre document : la « Déclaration des pratiques de certification », ci-après nommée DPC.

La gestion d'un certificat comprend toutes les phases du cycle de vie d'un certificat, de la demande d'attribution à la fin de vie de ce certificat. Le but de la présente PC est de fournir aux opérateurs et aux utilisateurs de certificats les informations relatives aux garanties offertes sur les certificats émis par l'IGC de la Gendarmerie nationale, ainsi que les conditions d'utilisation de ces certificats.

La présente PC fera l'objet de révisions périodiques afin de tenir compte de l'évolution des technologies et des recherches dans le domaine de la cryptographie.

Cette PC vise la conformité aux exigences du RGS v2 et eIDAS selon la norme ETSI EN 319 411-2 au niveau QCP-n-qscd. Elle a été élaborée à partir de la PC Type du RGS.

I.1.2. Architecture de l'IGC

L'architecture de l'IGC/GN est composée de :

- l'AC racine de la Gendarmerie nationale dont le certificat n'est pas auto-signé, car il est émis et certifié par l'IGC/A ;
- trois AC subordonnées internes pour la production de certificats pour les personnes physiques :
 - une AC subordonnée « AC GN Personnes Authentification vX » pour l'authentification,
 - une AC subordonnée « AC GN Personnes Chiffrement vX » pour le chiffrement,
 - une AC subordonnée « AC GN Personnes Signature vX » pour la signature ;
- une AC subordonnée interne « AC GN Machines Cachet serveur » pour la production de certificats de signature pour les machines ;
- deux AC subordonnées internes « AC PN Machines » et « AC GN Machines » pour la production de certificats d'authentification, de chiffrement et de signature pour les machines (par exemple, des serveurs) au profit de la police et de la gendarmerie nationales ;
- une AC non signée par la racine, servant à la production de certificats de tests.

Les certificats issus d'AC subordonnées à l'AC Racine Gendarmerie sont limités à un usage professionnel dans le cadre des échanges internes à la gendarmerie ou dans le cadre d'échanges avec d'autres organismes.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	13 / 62

En ce qui concerne les certificats issus des AC GN Machines Cachet serveur et des AC GN et PN Machines, leur usage n'est autorisé que :

- sur les équipements de la gendarmerie mis en place par le STIG ou le ST(SI)² et ne contrevenant pas aux dispositions de la PSSI,
- sur des équipements relevant de la sécurité intérieure administrés par la gendarmerie.

I.2. Identification du document

Le présent document est dénommé "Politique de certification de l'autorité de certification subordonnées pour les machines de la Gendarmerie nationale".

Ce document constitue la Politique de Certification (PC) pour l'AC subordonnée « AC GN Machines Cachet serveur », identifiée par l'OID 1.2.250.1.189.1.1.1.5.1.

La construction de l'OID est réalisée ainsi :

{iso(1) member-body(2) fr(250) type-org(1) gendarmerie(189) igc(1) documentation(1) PC(1) Machines(5) Cachet serveur(1)}

I.3. Définitions et acronymes

I.3.1. Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
AGeC@PE	Application de Gestion des Cartes Professionnelles Électroniques
AE	Autorité d'Enregistrement
APSE	Automate de Personnalisation des Secure Elements
ANSSI	Agence nationale de la sécurité des systèmes d'information
BCOF	Bureau du Contrôle Opérationnel des fichiers
BASSI	Bureau de l'audit de la sécurité des systèmes d'information
BEJ	Bureau des Enquêtes Judiciaires
CGU	Conditions Générales d'Utilisation
CNAU	Centre National d'Assistance aux Utilisateurs
DGGN (le)	Directeur Général de la Gendarmerie Nationale
DGGN (la)	Direction Générale de la Gendarmerie Nationale
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
GCMP	Groupe des Chargés de Mission et de Projets
GN	Gendarmerie nationale
IGC	Infrastructure de Gestion de Clés
IPMS	Infrastructure de Production Mutualisée et Secourue

LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OSSIN	Officier de Sécurité des Systèmes d'Information National
PC	Politique de Certification
PSCE	Prestataire de Services de Certification Électronique
RC	Responsable du Certificat de service applicatif
RSA	Rivest Shamir Adleman
SCT	Section Contrôle Technique
SDAC	Sous-Directeur des Applications de Commandement
SGDC	Section de la Gestion de la Donnée Classifiée
SSI	Sécurité des Systèmes d'Information
STIG	Service de Traitement de l'Information Gendarmerie
URL	Uniform Resource Locator

I.3.2. Définitions

Les termes utilisés dans la présente PC sont les suivants :

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins de cachet du service applicatif auquel le certificat est rattaché.

Autorité responsable d'application (ARA) - Une ARA est l'autorité responsable d'une infrastructure de gestion de clés (IGC), tant pour la technologie mise en œuvre que pour le cadre réglementaire et contractuel. Elle confie l'élaboration de la PC à une autorité administrative et sa mise en œuvre à des autorités de certification.

L'ARA de l'IGC de la Gendarmerie nationale est représentée par le chef du Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure par délégation du Directeur Général de la Gendarmerie Nationale (DGGN).

Autorité administrative - L'AA est l'autorité qui élabore la/ou les PC d'une IGC et les DPC afférentes, et qui est garante de leur application.

L'AA de l'IGC de la Gendarmerie nationale est représentée par le Sous-Directeur des Applications de Commandement (SDAC).

Autorité de certification racine (ACR) - L'ACR est l'autorité qui dispose d'une infrastructure de gestion de clés lui permettant d'enregistrer, de générer, d'émettre et de révoquer des certificats, principalement des certificats d'autorités de certification subordonnées, conformément à la PC et à la DPC définies par son AA. L'ACR de la Gendarmerie nationale n'est pas auto-certifiée, c'est-à-dire que son certificat n'est pas auto-signé. En revanche, le certificat de cette ACR étatique est signé par l'ACR de l'IGC/A. L'ACR est opérée par le BCOF. Les différentes opérations sont menées sur convocation des représentants des différents services.

L'ACR de l'IGC de la Gendarmerie nationale est représentée par le chef du BCOF.

Autorité de certification subordonnée (AC subordonnée) - L'AC subordonnée est l'autorité qui dispose d'une infrastructure de gestion de clés (qui peut être le même que l'ACR de l'IGC) lui permettant d'enregistrer, de générer, d'émettre et de révoquer des certificats finaux (personnes ou machines), conformément à ses propres PC et DPC. Le certificat de cette AC subordonnée est signé

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	15 / 62

par l'ACR de l'IGC/GN. Les autorités de certification subordonnées sont représentées par le chef du BCOF.

Autorité d'enregistrement cachet serveur (AE Cachet serveur) – L'AE cachet serveur est l'autorité qui a pour rôle de vérifier la validité d'une demande de certificat cachet serveur et en suit l'instruction.

L'AE cachet serveur de l'IGC de la Gendarmerie nationale est représentée par le secrétaire de la Sous-Direction des Applications de Commandement (SDAC).

Cachet serveur – Signature numérique effectuée par un serveur applicatif sur des données dans le but de pouvoir être utilisée soit dans le cadre d'un service d'authentification de l'origine des données, soit dans le cadre d'un service de non répudiation dans le cadre d'échanges dématérialisés entre usagers et l'administration ou entre différentes administrations.

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

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptographie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC..

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

Dispositif de protection des éléments secrets - Un dispositif de protection des éléments secrets désigne un dispositif de stockage des éléments secrets remis au RC.

Entité - Désigne une administration ou une entreprise au sens large.

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

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 RC et les utilisateurs de certificats.

Porteur de certificat - Le porteur de certificat est normalement la personne physique identifiée dans le certificat comme porteur de la clé privée liée à la clé publique figurant dans le certificat. Dans le contexte de cette PC consacrée également à une AC délivrant des certificats à une machine, il faut interpréter le terme porteur comme le Responsable du certificat.

Responsable du certificat – Personne en charge et responsable du certificat électronique de service applicatif de cachet ou d'authentification du serveur.

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives. Selon le contexte, un usager peut être un porteur ou un utilisateur de certificats.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	16 / 62

Utilisateur de certificat - Entité ou personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique ou une authentification provenant d'un service applicatif ou d'une personne physique disposant d'un certificat dédié à cet usage.

Nota - Un agent d'une administration qui procède à des échanges électroniques avec une autre administration est, pour cette dernière, un usager.

I.4. Entités intervenant dans l'IGC

I.4.1. Autorités de certification

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (IGC).

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine, la décomposition fonctionnelle de l'IGC qui est retenue dans la présente PC est la suivante :

- **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'AE et de la clé publique du service provenant soit du RC, soit de la fonction de génération des éléments secrets du service, si c'est cette dernière qui génère la bi-clé du service applicatif.
- **Fonction de remise au RC** - Cette fonction remet au RC le certificat du service applicatif ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif de protection des éléments secrets, clé privée du service applicatif, codes d'activation,...).
- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux RCs et/ou aux utilisateurs de certificats, hors informations d'état des certificats.
- **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 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 oeuvre par une publication à intervalles réguliers de LCR.

D'autres fonctions de l'IGC (contrôles d'identité, remise, révocation...) sont mises en oeuvre par les valideurs et sont détaillées au chapitre ci-dessous.

D'autres entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment (voir les définitions au §I.3.2 et les descriptions des fonctions dans les paragraphes suivants) :

- Responsable du certificat
- Utilisateur de certificat.

L'autorité de certification est le tiers de confiance de référence reconnu par l'ensemble de ses utilisateurs. À ce titre, l'AC engage sa responsabilité sur le respect des exigences décrites dans la présente PC, et s'engage à ce que les composantes de l'IGC, internes et externes à l'AC, respectent aussi les exigences qui les concernent.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	17 / 62

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, l'AC s'engage, en tant que responsable de l'ensemble de l'IGC, au respect des exigences suivantes :

- Être une entité légale au sens de la loi française.
- Être en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats de services applicatifs de cette entité. L'AC peut aussi, le cas échéant, être en relation contractuelle / hiérarchique / réglementaire avec le ou les mandataires de certification choisis par l'entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux RC, aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, notamment en matière de génération des certificats, de remise au RC, de gestion des révocations et d'information sur l'état des certificats.
- Élaborer, mettre en œuvre, contrôler et maintenir de façon itérative les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, et correspondant au minimum aux exigences de la présente PC, notamment en termes de fiabilité, de qualité et de sécurité. À ce titre, elle doit posséder un ou des systèmes de gestion de la qualité et de la sécurité de l'information adaptés aux services de certification qu'elle assure.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats et de LCR), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux RC et utilisateurs de certificats.
- Suivre les demandes en capacité et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacité de traitement et de stockage.

I.4.2. Autorité d'enregistrement

L'AE a pour rôle de vérifier l'identité du futur RC et les informations liées au service applicatif. Pour cela, l'AE assure les tâches suivantes :

- La prise en compte et la vérification des informations du futur RC et du service applicatif, ainsi que de leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à la fonction de génération de l'IGC ;
- L'archivage des pièces du dossier d'enregistrement;
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du RC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

Les fonctions de l'Autorité d'Enregistrement de l' « AC GN Machines Cachet serveur » sont exercées par le secrétariat de la sous-direction des applications de commandement.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	18 / 62

I.4.3. Responsables de certificats électroniques de services applicatifs

Un RC est une personne physique qui est responsable de l'utilisation du certificat électronique identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité identifiée dans ce certificat. Le RC a un lien contractuel / hiérarchique / réglementaire avec cette entité.

Le RC respecte les conditions qui lui incombent définies dans cette PC. Cependant, cette PC se limitant aux usages de cachet serveur, le cycle de vie est simplifié. En effet, ce certificat sera intégré dans la plate-forme de signature et la clé privée associée générée au sein d'un HSM. Par conséquent, les opérations se résument à la signature d'une requête de certification, l'implantation du certificat dans le socle technique cachet-serveur, la révocation du certificat cachet-serveur en cas de renouvellement, de cessation de l'activité cachet-serveur, de compromission ou suspicion de compromission de la clé privée. À aucun moment le RC ne dispose d'un accès à la clé privée.

Il est à noter que le certificat étant attaché à un service de la gendarmerie disposant d'un cachet serveur et non au RC, ce dernier peut être amené à changer en cours de validité du certificat. C'est la raison pour laquelle chaque opération du cycle de vie (génération, révocation) fait l'objet d'une demande du responsable de l'unité (ou d'un de ses adjoints) au profit de laquelle le certificat cachet-serveur a été ou va être émis. Dans le cadre de cette demande, le responsable de l'unité désigne un RC pour chaque opération.

I.4.4. Utilisateurs de certificats

Un utilisateur de certificats électroniques peut être notamment :

- Une personne destinataire de données signées par un service applicatif de cachet et qui utilise le certificat électronique du cachet ainsi qu'un module de vérification de cachet afin d'authentifier l'origine de ces données transmises.
- Un service applicatif destinataire de données provenant d'un autre service applicatif et qui utilise le certificat électronique de cachet et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises.
- Un service applicatif qui signe des données électroniques.

I.4.5. Autres participants à l'IGC GN

L'IGC GN ne fait pas appel à des mandataires de certification.

I.5. Usage des certificats

I.5.1. Domaines d'utilisation applicables

I.5.1.1 Bi-clés et certificats du service applicatif

Les usages sont le scellement électronique de données et la vérification de cachet électronique. Ces données peuvent être, par exemple, un accusé de réception suite à la transmission d'informations par un usager à un service applicatif, une réponse automatique à une demande formulée par un usager, un jeton d'horodatage, un code applicatif ou encore une archive.

Les certificats ne doivent être utilisés que dans le strict cadre prévu par le service applicatif titulaire, en interne à la Gendarmerie nationale, ou pour des relations dûment autorisées avec des organismes en relation avec la Gendarmerie..

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	19 / 62

I.5.1.2 Bi-clés et certificats d'AC et de composantes

Cette PC comporte également des exigences concernant les bi-clés et certificats des AC (signature des certificats des services applicatifs et des LCR) ainsi que des clés, bi-clés et certificats des composantes de l'IGC (sécurisation des échanges entre composantes, authentification des opérateurs, etc.).

Chaque AC génère et signe différents types d'objets : certificats et LCR. Pour signer ces objets, l'AC dispose d'une seule et même bi-clé, dont le certificat est émis par l'AC Racine. Cette bi-clé et ce certificat ne sont utilisés qu'à cette fin.

I.5.2. Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre IV.5 ci-dessous, en fonction du niveau de sécurité. L'AC doit respecter ces restrictions et imposer leur respect par les RC et ses utilisateurs de certificats.

À cette fin, elle doit communiquer à tous les RC et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

I.6. Gestion de la PC

I.6.1. Entité gérant la PC

Cette PC et la DPC afférente sont élaborées et maintenues par l'Autorité Administrative (AA), représentée par le Sous-Directeur des Applications de Commandement (SDAC).

I.6.2. Point de contact

Pour toute remarque ou question relative à cette PC, le point de contact est :

Direction Générale de la Gendarmerie Nationale
Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure
Sous-Direction des Applications de Commandement
4 rue Claude Bernard
CS 60003
92136 Issy les Moulineaux Cedex
FRANCE

I.6.3. Entité déterminant la conformité d'une DPC avec cette PC

Les personnes habilitées à déterminer la conformité de la DPC avec les PC sont nommées par l'AA. Il s'agit des personnels de la SGDC. Un contrôle est également effectué par le BASSI lors des audits internes.

I.6.4. Procédures d'approbation de la conformité de la DPC

L'AA dispose d'un processus de gestion (mise à jour, révisions) de la DPC et d'approbation de sa conformité avec la PC.

Toute nouvelle version de la PC est publiée, conformément aux exigences du paragraphe II.2 sans délai.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	20 / 62

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

II.1. Entités chargées de la mise à disposition des informations

Les AC, objet de cette PC, disposent d'une fonction de publication et d'une fonction d'information sur l'état des certificats.

Les documents sont publiés à destination des porteurs et des utilisateurs de certificats à l'adresse suivante :

<http://stsisi.psi.minint.fr/securite/1598/igc/>

<https://www.gendarmerie.interieur.gouv.fr/igc/pc>

La publication de ces éléments se fait manuellement. Elle est de la responsabilité de l'AA.

Les informations d'état des certificats sont publiées sous forme de liste de certificats révoqués (LCR) aux adresses suivantes :

<http://crl.gendarmerie.fr>

Des répliques sont faites sur les adresses suivantes :

<http://crl.gendarmerie.interieur.gouv.fr>

<http://crl.gendarmerie.interieur.ader.gouv.fr>

La publication de ces éléments est automatisée pour les CRLs signées par les AC subordonnées. Elle est manuelle pour la LAR de l'AC Racine gendarmerie. Elle est de la responsabilité de l'ACR (qui est également ACD).

L'ensemble des certificats tant révoqués que expirés sont présents dans la CRL.

Un script mis en place au groupe de sécurité opérationnelle (GSOP STIG) automatise la surveillance des publications de CRL, vérifie la signature de l'AC, et vérifie la persistance des numéros de série des certificats (révoqués et expirés) au fil des CRL et remonte une alarme en cas de détection d'anomalie.

Aucun service OCSP n'est disponible.

II.2. Informations devant être publiées

Sur internet et intranet :

- la présente PC ;
- les certificats de la chaîne de certification des AC en cours de validité
- les listes des certificats révoqués (LCR) délivrées et signées par les AC subordonnées ;
- les conditions générales d'utilisation applicables aux services de certification ;

Les documents sont rédigés en français.

II.3. Délais et fréquences de publication

Les informations sont publiées dans les meilleurs délais après la disponibilité d'une nouvelle version.

En particulier,

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	21 / 62

- les informations liées à l'IGC (PC, conditions générales...) sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC ;
- les certificats d'AC sont diffusés préalablement à toute diffusion de certificats de services applicatifs et/ou de LCR correspondants ;
- les délais et fréquences de publication des informations d'état des certificats sont décrits aux chapitres IV.9 et IV.10.

Les informations ont une disponibilité de 24h/24 et 7j/7, des contraintes de disponibilité particulières étant définies pour les informations d'état des certificats aux chapitres IV.9 et IV.10.

II.4. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC. La publication est lancée automatiquement par l'IGC dès lors qu'une nouvelle CRL est générée.

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées de l'IGC. La publication est gérée par le BCOF qui transmet les informations à publier au GCMP via un ticket de changement.

Le GSOP exécute un script de contrôle de l'intégrité. Il est mis en copie du ticket de changement de toutes les demandes de publication afin de mettre à jour les informations d'intégrité (hash).

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	22 / 62

III. Identification et authentification

III.1. Nommage

III.1.1. Types de noms

Les noms utilisés sont conformes aux spécifications du [RGS].

Dans chaque certificat, l'AC émettrice (issuer) et le service applicatif (subject) sont identifiés par un "Distinguished Name" (DN).

III.1.2. Nécessité d'utilisation de noms explicites

III.1.2.1 Nommage des Autorités de Certification

Le DN de l'AC GN Machines Cachet serveur est construit comme suit :

Attribut	Valeur	Commentaires
C	FR	Pays
O	Gendarmerie nationale	Organisation
OU	0002 157000019	Numéro SIREN de la DGGN, obligatoire pour le respect du RGS
CN	AC GN Machines Cachet serveur	Identification de l'AC parmi celles de l'IGC/GN

Le DN de l'autorité, sous forme littérale, est :

C = FR, O = Gendarmerie nationale, OU = 0002 157000019, CN = AC GN Machines Cachet serveur

III.1.2.2 Nommage des services applicatifs

Les noms choisis pour désigner les services applicatifs dans les certificats sont explicites. L'identification de l'entité à laquelle le service applicatif est rattaché est obligatoire.

Le DN des services applicatifs est construit comme suit :

Attribut	Valeur	Commentaires
C	FR	Pays
O	Gendarmerie nationale	Organisation
organizationIdentifier	NTRFR-157000019	Obligatoire pour le eIDAS
OU	0002 157000019	Numéro SIREN de la DGGN, obligatoire pour le respect du RGS
OU	Machines Cachet serveur	Indication de l'AC émettrice du certificat
CN	<i>Nom du service applicatif</i>	Nom (<u>non ambigu</u>) du service applicatif Pour identifier un service applicatif, on peut par exemple utiliser la notation : [Nom du bureau responsable du serveur].[Nom du service applicatif]

Par exemple, un DN de service peut être :

C = FR, O = Gendarmerie nationale, OU = 0002 157000019, OU = Machines, CN = BCOF.STARAC

III.1.3. Pseudonymisation des services applicatifs

S'agissant de certificats délivrés à des services applicatifs, les notions d'anonymisation ou de pseudonymisation sont sans objet.

III.1.4. Règles d'interprétation des différentes formes de nom

Sans objet.

III.1.5. Unicité des noms

L'identification unique d'un service applicatif est assurée par la méthode de construction de l'attribut CN du DN du certificat. Ce dernier repose sur le nom de l'application et le nom de l'entité ayant demandé le certificat. Les unités gendarmerie étant toutes répertoriées dans un référentiel unique, il n'existe pas d'ambiguïté.

Durant toute la durée de vie de l'AC, le nom du service applicatif de création de cachet rattaché à une entité ne peut être attribué à une autre entité.

III.1.6. Identification, authentification et rôle des marques déposées

L'AC est responsable de l'unicité des noms des services applicatifs et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

III.2. Validation initiale de l'identité

L'enregistrement d'un service applicatif pour lequel un certificat doit être délivré se fait via une demande de certificat du commandant d'unité (ou d'un de ses adjoints) qui désigne éventuellement un RC pour le représenter.

Un RC peut être amené à changer en cours de validité du certificat électronique correspondant. Dans ce cas, tout nouveau RC fera également l'objet d'une procédure d'enregistrement.

L'enregistrement d'un RC, et du service applicatif objet de la demande se fait directement auprès de l'AE. Celle-ci procède aux validations initiales suivantes :

- validation de l'identité "personne morale" de l'entité de rattachement du RC
- validation de l'identité "personne physique" du RC.

III.2.1. Méthode pour prouver la possession de la clé privée

Le RC fournit à l'AC, via l'AE, une preuve de possession de la clé privée correspondant à la clé publique contenue dans la demande de certificat électronique, sous forme de requête de certificat au format PKCS#10, signée par la clé privée.

III.2.2. Validation de l'identité d'un organisme

Sans objet.

III.2.3. Validation de l'identité d'un individu

III.2.3.1 Enregistrement d'un RC pour un certificat de service applicatif à émettre

Le futur RC prépare un formulaire de demande de certificat rempli et signé par l'autorité hiérarchique dont dépend l'entité au profit de laquelle le service applicatif signera. Cette demande doit être datée de moins de 3 mois. Ce formulaire comprend :

- L'identité du demandeur : Nom, prénom, grade, NIGEND ;
- L'identité du RC : Nom, prénom, grade, NIGEND ;
- Le service d'appartenance du demandeur ;
- Le nom du service applicatif pour lequel la demande est réalisée ;
- Un mandat désignant le futur RC comme étant habilité à être responsable pour le service applicatif pour lequel le certificat doit être délivré ;
- Les conditions générales d'utilisation du certificat cachet ;

Le RC fournit le formulaire ainsi que la requête de certificat au format PKCS#10 à l'opérateur AC traitant la demande au cours d'un face à face Le RC s'authentifie par présentation d'un document officiel d'identité en cours de validité comportant une photographie d'identité (notamment carte professionnelle de la gendarmerie, carte nationale d'identité, passeport), et dont l'opérateur AC conserve une copie. Le formulaire est signé par le RC et l'opérateur avant que le certificat ne soit généré et remis en séance.

La génération de la requête PKCS#10 ne fait pas partie du périmètre de l'IGC et n'est pas explicitée dans la DPC.

III.2.3.2 Enregistrement d'un nouveau RC pour un certificat électronique déjà émis

Sans objet.

Un RC est une personne physique qui est responsable de l'utilisation du certificat électronique identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité identifiée dans ce certificat. Le RC a un lien contractuel / hiérarchique / réglementaire avec cette entité.

Le RC respecte les conditions qui lui incombent définies dans cette PC. Cependant, cette PC se limitant aux usages de cachet serveur, le cycle de vie est simplifié. En effet, ce certificat sera intégré dans la plate-forme de signature et la clé privée associée générée au sein d'un HSM. Par conséquent, les opérations se résument à la signature d'une requête de certification, l'implantation du certificat dans le socle technique cachet-serveur, la révocation du certificat cachet-serveur en cas de renouvellement, de cessation de l'activité cachet-serveur, de compromission ou suspicion de compromission de la clé privée. À aucun moment le RC ne dispose d'un accès à la clé privée.

Il est à noter que le certificat étant attaché à un service de la gendarmerie disposant d'un cachet serveur et non au RC, ce dernier peut être amené à changer en cours de validité du certificat. C'est la raison pour laquelle chaque opération du cycle de vie (génération, révocation) fait l'objet d'une demande du responsable de l'unité (ou d'un de ses adjoints) au profit de laquelle le certificat cachet-serveur a été ou va être émis. Dans le cadre de cette demande, le responsable de l'unité désigne un RC pour chaque opération.

III.2.4. Informations non vérifiées d'un RC ou d'un service applicatif

Sans objet.

III.2.5. Validation de l'autorité du demandeur

Cette validation est faite par l'AE lors de l'enregistrement du RC.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	25 / 62

Les entités de la Gendarmerie nationale susceptibles de demander des certificats machines pour un service de cachet peuvent être :

- La direction générale ;
- Le cabinet ;
- Les entités composant la DGGN jusqu'au niveau sous-direction
- L'inspection de la gendarmerie nationale ;
- Le commandement des écoles ;
- Un service ;
- Une direction ;
- Une sous-direction ;
- Un bureau ;
- Une section ;
- Une région de gendarmerie ;
- Le Pôle Judiciaire de la Gendarmerie Nationale
- Le commandement de la gendarmerie d'outre-mer ;
- Un groupement de gendarmerie départementale ou mobile ;
- Toute unité d'un niveau équivalent à celles citées précédemment.

L'authentification doit permettre d'identifier l'entité de façon unique et non ambiguë. Elle est réalisée par l'AE par l'authentification de l'identité du représentant de cette entité. L'AE pourra contacter tout membre de la chaîne fonctionnelle de sécurité des systèmes d'information désigné par lui pour vérification ou procéder à des vérifications directement auprès de la chaîne de commandement.

III.3. Identification et validation d'une demande de renouvellement des clés

Le renouvellement de la bi-clé d'un service applicatif entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat de service applicatif ne peut pas être fourni au RC sans renouvellement de la bi-clé correspondante (cf. chapitre IV.6).

III.3.1. Identification et validation pour un renouvellement courant

A chaque renouvellement, l'AE, saisie de la demande, identifie le RC et le service applicatif selon la même procédure que pour l'enregistrement initial.

III.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial

III.4. Identification et validation d'une demande de révocation

Les exigences concernant les informations à fournir dans une demande de révocation sont décrites au chapitre IV.9.3.

La demande de révocation est effectuée par un responsable hiérarchique de l'entité responsable du service applicatif ou par le RC du certificat concerné. Elle est réalisée par écrit dans un formulaire signé (manuellement ou éventuellement de manière électronique) et confirmée par un face à face avec l'AC (sauf en cas d'urgence, par téléphone). Le responsable hiérarchique de l'AC authentifie le demandeur par sa connaissance directe et personnelle de ses interlocuteurs ou par la voie hiérarchique.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	26 / 62

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.1. Demande de certificat

IV.1.1. Origine d'une demande de certificat

Un certificat peut être demandé par le commandant d'unité ou par toute personne exerçant la continuité de son commandement.

IV.1.2. Processus et responsabilités pour l'établissement d'une demande de carte

Le RC (ou futur RC) établit le dossier de demande et le signe conjointement avec son responsable hiérarchique. Le contenu de ce dossier est détaillé au §III.2.3.1.

Le RC transmet le dossier de demande à l'AE.

IV.2. Traitement d'une demande de certificat

IV.2.1. Exécution des processus d'identification et de validation de la demande

Les identités "personne physique" et "personne morale" sont vérifiées conformément aux exigences du chapitre III.2. L'AE effectue les opérations suivantes :

- Validation de l'identité du RC ;
- Vérification de la cohérence des justificatifs présentés ;
- Vérification de la prise de connaissance par le RC des modalités applicables pour l'utilisation du certificat.

Une fois ces opérations effectuées, l'AE enregistre la demande de génération du certificat. Elle conserve le dossier de demande, contenant les justificatifs présentés.

IV.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le RC en justifiant le rejet.

IV.2.3. Durée d'établissement du certificat

En cas d'acceptation de la demande, les certificats sont générés au plus tôt, et au plus tard deux semaines après la transmission du dossier à l'autorité de certification.

IV.3. Délivrance du certificat

IV.3.1. Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de la conformité de la demande, l'opérateur AC qui traite la demande (il est aussi l'opérateur AE), déclenche la fonction de génération de la clé privée et du certificat par l'AC.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres V et VI ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre V.2).

IV.3.2. Notification par l'AC de la délivrance du certificat au RC

La remise du certificat se fait en mains propres au RC par l'opérateur AC.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	27 / 62

IV.4. Acceptation du certificat

IV.4.1. Démarche d'acceptation du certificat

L'opérateur AC ouvre le certificat produit devant le RC et obtient de sa part la confirmation de l'acceptation du certificat. Cette confirmation est explicitement mentionnée sur le formulaire de remise.

Le formulaire de remise est conservé par l'AC, le RC en obtient une copie.

IV.4.2. Publication du certificat

Le certificat ne fait pas l'objet d'une publication par l'AC. Le RC peut publier le certificat avec ses moyens propres et seulement s'il le souhaite.

IV.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

Le rôle de l'AE étant pris en charge par un opérateur AC, il n'y a pas lieu de notifier une autre entité de l'IGC.

IV.5. Usages de la bi-clé et du certificat

IV.5.1. Utilisation de la clé privée et du certificat par le RC

L'utilisation de la clé privée par le service applicatif et du certificat associé est strictement limitée à la fonction de sécurité de création de cachet (cf. §I.5.1.1). Les RC doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé du service applicatif et du certificat associé est par ailleurs être indiqué dans le certificat lui-même, via les extensions concernant les usages des clés. Cet usage est également clairement explicité dans cette PC, ainsi que dans les conditions générales d'utilisation. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du RC par l'AC avant d'entrer en relation contractuelle

IV.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Cf. chapitre précédent et chapitre I.5.

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

IV.6. Renouvellement d'un certificat

La notion de "renouvellement de certificat", conformément au [RFC3647], correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique du service applicatif).

Cependant, dans le cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. L'AC demande au RC de s'engager, dans les conditions générales d'utilisation, à ce que toute demande de renouvellement de certificat soit basée sur une nouvelle bi-clé. L'IGC de son côté est configurée afin de refuser toute certification de clé publique pour laquelle elle aurait déjà émis un certificat.

IV.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé

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

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	28 / 62

IV.7.1. Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelés afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des services applicatifs, et les certificats correspondants, seront renouvelés au minimum à une fréquence définie au point VI.3.2.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du service applicatif (cf. chapitre IV.9, notamment le chapitre [IV.9.1.1] pour les différentes causes possibles de révocation).

Nota - Dans la suite du présent chapitre, le terme utilisé est "fourniture d'un nouveau certificat".

IV.7.2. Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat électronique est à l'initiative du RC.

L'entité peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un service applicatif qui lui est rattaché.

Afin d'éviter l'expiration non anticipée d'un certificat, l'AC peut prévenir le RC de l'approche de la fin de vie du certificat et l'inviter à procéder au renouvellement.

IV.7.3. Procédure de traitement d'une demande d'un nouveau certificat

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre III.3 ci-dessus.

Pour les actions de l'AC, cf. chapitre IV.3.1.

IV.7.4. Notification au RC de l'établissement du nouveau certificat

Cf. chapitre IV.3.2.

IV.7.5. Démarche d'acceptation du nouveau certificat

Cf. chapitre IV.4.1.

IV.7.6. Publication du nouveau certificat

Cf. chapitre IV.4.2.

IV.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Cf. chapitre IV.4.3.

IV.8. Modification du certificat

La modification d'un certificat, conformément au [RFC3647], correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre IV.7) et autres qu'uniquement la modification des dates de validité (cf. chapitre IV.6).

La modification de certificat n'est pas autorisée dans la présente PC.

IV.9. Révocation et suspension des certificats

IV.9.1. Causes possibles d'une révocation

IV.9.1.1 Certificats de services applicatifs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat électronique :

- les informations du service figurant dans le certificat ne sont plus en conformité avec l'identité du service ou l'utilisation prévue dans le certificat (par exemple, modification du nom), ceci avant l'expiration normale du certificat ;

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	29 / 62

- le RC n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le RC et/ou l'entité, n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- la clé privée du service applicatif est suspectée de compromission, est compromise, est perdue ou est volée, (éventuellement les données d'activation associées) ;
- le RC ou une entité autorisée (représentant légal de l'entité exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du service applicatif et/ou de son support) ;
- l'arrêt définitif du service applicatif ou la cessation d'activité de l'entité du RC de rattachement du service applicatif.

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.

IV.9.1.2 Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats ou la signature de LCR) :

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant la composante.

IV.9.2. Origine d'une demande de révocation

IV.9.2.1 Certificats de services applicatifs

Les personnes / entités qui peuvent demander la révocation d'un certificat électronique sont les suivantes :

- le RC ou le responsable de l'entité du service applicatif ;
- l'AC.

IV.9.2.2 Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice. La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

IV.9.3. Procédure de traitement d'une demande de révocation

IV.9.3.1 Révocation d'un certificat de service applicatif

IV.9.3.1.1 Révocation par le RC

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre III.4.

Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- le nom du service applicatif figurant dans le certificat ;
- le nom du demandeur de la révocation ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série,...) ;
- la cause de révocation.

Le traitement de la demande est décrit au §IV.9.3.1.4 ci-dessous.

IV.9.3.1.2 Révocation par l'AE

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	30 / 62

Cf. chapitre IV.9.3.1.3.

IV.9.3.1.3 Révocation par l'AC émettrice du certificat

Un opérateur de l'AC peut directement révoquer un certificat émis par cette AC.

La demande de révocation est enregistrée dans le système, avec les données suivantes :

- le nom du service applicatif figurant dans le certificat ;
- l'identité de l'opérateur agissant pour le compte de l'AC ;
- le numéro de certificat à révoquer
- la cause de la révocation (obligatoire dans ce cas)

Le traitement de la demande est décrit au §IV.9.3.1.4 ci-dessous.

IV.9.3.1.4 Traitement de la demande de révocation

Une fois la demande authentifiée et contrôlée, l'AC (via sa fonction de gestion des révocations) révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée via une LCR signée par l'AC elle-même.

Le demandeur de la révocation et le RC sont informés du bon déroulement de l'opération et de la révocation effective du certificat.

L'opération est enregistrée dans les journaux d'événements avec toutes les informations disponibles sur les causes initiales ayant entraîné la révocation du certificat (ces causes ne sont pas publiées).

IV.9.3.2 Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé. Le point de contact identifié sur le site www.ssi.gouv.fr doit être immédiatement informé.

La DPC précise les procédures mises en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

IV.9.4. Délai accordé au RC pour formuler la demande de révocation

Dès que le RC (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

IV.9.5. Délai de traitement par l'AC d'une demande de révocation

IV.9.5.1 Révocation d'un certificat de service applicatif

Par nature, une demande de révocation doit être traitée en urgence.

IV.9.5.2 Disponibilité du système de traitement des demandes de révocation

La fonction de gestion des révocations est disponible 24h/24 et 7j/7. Cette fonction a une durée maximale d'indisponibilité de 2h par interruption de service (panne ou maintenance) et de 8h en cumulé sur un mois.

Toute demande de révocation d'un certificat est traitée dans un délai inférieur à 24h. 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 (publication de la LCR).

IV.9.5.3 Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	31 / 62

effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé. Le point de contact identifié sur le site www.ssi.gouv.fr doit être immédiatement informé.

IV.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat électronique est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante par consultation des LCR et LAR appropriées.

IV.9.7. Fréquence d'établissement et durée de validité des LCR

Les LCR sont publiées au moins une fois par 24h.

Afin d'assurer une continuité du service dans le cas où un incident sur la publication des LCR survienne, la durée de validité des LCR est de 6 jours.

L'AC objet de cette PC n'a pas d'AC subordonnées et ne publie donc pas de LAR. Se référer à la PC de l'AC Racine pour obtenir des informations sur les fréquences et durées de vie des LAR concernant l'AC de cette PC.

IV.9.8. Délai maximum de publication d'une LCR

Une fois générées, les LCR sont publiées immédiatement et en tout état de cause dans un délai maximum de 30 minutes suivant leur génération.

IV.9.9. Exigences sur la vérification en ligne de la révocation et de l'état des certificats

Sans objet car l'AC ne propose pas de service en ligne OCSP.

IV.9.10. Autres moyens disponibles d'information sur les révocations

Sans objet.

IV.9.11. Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de services applicatifs, les entités autorisées à effectuer une demande de révocation sont tenues de le faire sans délai après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, outre les exigences du chapitre IV.9.3.2 ci-dessus, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

IV.9.12. Causes possibles d'une suspension

L'AC n'autorise pas les suspensions de certificat.

IV.9.13. Origine d'une demande de suspension

Sans objet.

IV.9.14. Procédure de traitement d'une demande de suspension

Sans objet.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	32 / 62

IV.9.15. Limites de la période de suspension d'un certificat

Sans objet.

IV.10. Fonction d'information sur l'état des certificats

IV.10.1. Caractéristiques opérationnelles

Des LCR et des LAR sont mises à la disposition des utilisateurs de certificats pour vérifier le statut d'un certificat final, y compris celui des AC de sa chaîne de certification. Ces LCR / LAR sont au format V2.

IV.10.2. Disponibilité de la fonction d'information sur l'état des certificats

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7.

Cette fonction a une durée maximale d'indisponibilité de 4h par interruption de service (panne ou maintenance) et de 16h en cumulé sur un mois.

IV.10.3. Dispositifs optionnels

Sans objet.

IV.11. Fin de la relation entre le RC et l'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et l'entité de rattachement du service applicatif avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

De plus, l'AC doit révoquer un certificat électronique pour lequel il n'y a plus de RC explicitement identifié.

IV.12. Séquestre de clé et recouvrement

Les clés privées des services applicatifs et les clés privées d'AC ne sont en aucun cas séquestrées.

IV.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

IV.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

V. Mesures de sécurité non techniques

V.1. Mesures de sécurité physique

V.1.1. Situation géographique et construction des sites

Les sites d'hébergement des composantes de l'IGC/GN se trouvent sur le territoire national dans les deux data centers de la gendarmerie nationale

V.1.2. Accès physique

La plate-forme de certification de l'IGC/GN est hébergée et utilisée dans une zone protégée, au sens des articles 413-7, et R. 413-1 à R. 413-5 du Code pénal.

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. La sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. Toute personne entrant dans ces zones physiquement sécurisées n'est jamais laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

V.1.3. Alimentation électrique et climatisation

La prévention physique contre des incidents matériels, y compris concernant l'alimentation électrique et climatisation, est effectuée conformément aux normes s'appliquant aux établissements et aux locaux hébergeant une ou plusieurs composantes de l'infrastructure.

Ces dispositions garantissent les engagements de disponibilité des différents services pris dans cette PC.

De plus, la plate-forme de l'IGC/GN est protégée contre les signaux parasites compromettants lors de la mise en œuvre des fonctions et informations dont le besoin de confidentialité est élevé.

V.1.4. Vulnérabilité aux dégâts des eaux

La plate-forme de l'IGC/GN est hébergée dans des locaux protégés contre les dégâts des eaux, de façon à garantir les engagements de disponibilité des différents services pris dans cette PC.

V.1.5. Prévention et protection incendie

La prévention physique contre des incidents matériels, y compris concernant la prévention et la protection incendie, est effectuée conformément aux normes s'appliquant aux établissements et aux locaux hébergeant une ou plusieurs composantes de l'infrastructure.

Ces dispositions garantissent les engagements de disponibilité des différents services pris dans cette PC.

Les consignes de sécurité incendie sont vérifiées et connues des utilisateurs de la plate-forme de l'IGC/GN.

V.1.6. Conservation des supports

La conservation des informations sensibles ou classifiées de défense, sur quelque medium que ce soit, est effectué conformément à la réglementation pour les documents sensibles ou classifiés de défense.

Les différentes informations intervenant dans les activités de l'IGC sont identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité). L'AC maintient un inventaire de ces

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	34 / 62

informations. L'AC met en place des mesures pour éviter la compromission et le vol de ces informations.

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils sont manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion protègent ces 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.

V.1.7. Mise hors service des supports

La destruction des articles contrôlés de la sécurité des systèmes d'information (ACSSI) et des supports d'informations sensibles sera réalisée conformément à la réglementation en vigueur pour les documents sensibles ou classifiés de défense.

Ainsi les disques durs seront démagnétisés puis déchiquetés.

V.1.8. Sauvegardes hors site

Dans le cadre d'un plan anti-sinistre, l'ARA a mis en place des politiques et procédures qui permettent de rétablir les opérations dès que possible en cas d'accident, y compris la compromission des clés de signature privées des AC. Ces mesures garantissent une disponibilité des fonctions de l'IGC conforme aux engagements pris dans cette PC. Le rétablissement des opérations se fait dans le respect des exigences de sécurité exposées dans cette PC.

Le responsable du plan anti-sinistre est chef du STIG.

Les modalités de déclenchement du plan anti-sinistre sont définies par l'ARA.

V.2. Mesures de sécurité procédurales

V.2.1. Rôles de confiance

Les rôles définis pour l'AC subordonnées sont :

- **Autorité** : personne physique ayant un rôle de responsabilité dans l'IGC. Ce rôle est défini à la section II, III et IV de [\[GESTION_ROLES\]](#).
- **Responsable d'AC subordonnée** : la personne physique responsable d'une AC subordonnée, notamment de l'utilisation de son certificat et de sa bi-clé correspondante. Ce rôle est défini à la section V de [\[GESTION_ROLES\]](#).
- **Administrateur** : responsable du bon fonctionnement de l'ensemble des services rendus par l'autorité de certification, notamment de l'organisation et du bon déroulement des séances nécessitant la mise en œuvre d'un outil cryptographique par un opérateur. Il est responsable de l'ensemble des services rendus par l'AC. Responsable également de la préparation des documentations relatives à : l'installation de l'application, l'initialisation des ressources cryptos, la cérémonie des clés, les scripts additionnels (génération des CRLs, supervision, ...), configuration initiale d'EJBCA avant coupure/limitation des accès aux personnes physiques, supervision des services rendus par le STIG (CRL-eyes). Ce rôle est défini à la section VII, XVIII et XIX de [\[GESTION_ROLES\]](#).
- **Auditeur** : personne désignée par l'AC de la Gendarmerie nationale et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre de la politique de certification et des services effectivement fournis par l'AC. Responsable de la vérification de la conformité des procédures, vérification de l'application des procédures, vérification de la configuration des éléments de l'IGC, vérification du suivi de l'IGC (COPIL, indicateurs). Ce rôle est défini aux sections XV, XVI et XX de [\[GESTION_ROLES\]](#).
- **Ingénieur système** : il est chargé de la mise en route, de la configuration et de la maintenance technique de la plate-forme informatique hébergeant l'AC. Il assure l'administration de l'ensemble des composants nécessaires à la plate-forme (Machines virtuelles, SGBD, réseaux,

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	35 / 62

supervision). Ce rôle est défini aux sections VI, IX, X, XI, XII, XIII, XIV et XXVI de [\[GESTION_ROLES\]](#).

- **Opérateur** : l'opérateur de l'AC est responsable du traitement des demandes de délivrance des certificats cachet serveur et du traitement des demandes de révocation des certificats cachet serveur. Il réalise l'exploitation des services offerts par l'autorité, dans le cadre de ses attributions. Il est chargé de lancer l'exécution des fonctions cryptographiques. Ce rôle est défini à la section XXIII de [\[GESTION_ROLES\]](#).
- **Responsable de sécurité de l'AC** : il est responsable de l'application de la politique de sécurité physique et fonctionnelle de l'AC. Il gère les contrôles d'accès physiques à la plateforme informatique et est chargé de mettre en œuvre la politique de sécurité. Ce rôle est défini à la section XXII de [\[GESTION_ROLES\]](#).
- **Responsable de publication** : il est responsable de la publication des documents de l'IGC sur le site de publication. Ce rôle est défini à la section XXIV de [\[GESTION_ROLES\]](#).
- **Porteur de secret** : il est responsable de la conservation d'une part du secret des AC, soit en tant que commandant d'une unité détentrice, soit en tant que représentant temporaire du porteur. Ce rôle est défini à la section XVII et XXV de [\[GESTION_ROLES\]](#).

Le nom et la fonction de tous les personnels amenés à travailler au sein de composantes de l'IGC/GN sont explicitement précisés dans le document [\[GESTION_ROLES\]](#)

Les personnes ayant un rôle de confiance sont habilitées. Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

V.2.2. Nombre de personnes requises par tâches

Selon le type d'opérations effectuées, le nombre et le type de rôles et de personnes devant nécessairement être présentes (en tant qu'acteurs ou témoins) peuvent être différents. L'annexe « Rôles par opération » de la DPC permet de définir un nombre d'exploitants minimum nécessaires par type d'opérations.

V.2.3. Identification et authentification pour chaque rôle

L'identification et l'authentification des personnes commandant une action en fonction d'un rôle ayant trait à la gestion d'un certificat s'appuient sur des mesures organisationnelles.

Chaque composante met en place une gestion des droits d'accès selon les besoins et les autorisations définies par la présente PC qui respecte la séparation des rôles.

La déclaration des pratiques de certification décrit les actions effectuées.

V.2.4. Rôles exigeant une séparation des attributions

L'attribution des rôles aux différentes personnes se fait en évitant au maximum le cumul des attributions.

Les rôles incompatibles entre eux sont définis dans le document [\[GESTION_ROLES\]](#)

V.3. Mesures de sécurité vis-à-vis du personnel

V.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis au secret professionnel (gendarmes ou personnels civils relevant de la branche SIC).

Chaque entité opérant une composante de l'IGC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	36 / 62

Les AC de l'IGC/GN informent toute personne intervenant dans des rôles de confiance de l'IGC/GN :

- de ses responsabilités relatives aux services de l'IGC/GN,
- des procédures liées à la sécurité du système et au contrôle du personnel.

En particulier, les personnes intervenant dans des rôles de confiance doivent y être formellement affectées par l'encadrement supérieur chargé de la sécurité.

V.3.2. Procédures de vérification des antécédents

Afin de s'assurer de l'honnêteté et de la capacité d'une personne à tenir son rôle dans l'infrastructure de gestion des clés, la gendarmerie nationale effectue des vérifications.

Ces procédures sont décrites dans la déclaration des pratiques de certification.

V.3.3. Exigences en matière de formation initiale

Le personnel exécutant est formé aux logiciels, matériels et procédures internes de fonctionnement de la composante pour laquelle il opère.

V.3.4. Exigences et fréquence en matière de formation continue

Tout nouvel exploitant doit suivre une formation initiale au système, aux politiques de sécurité, au plan de secours, aux logiciels et opérations qu'il doit mettre en œuvre. Chaque employé devra assister à une formation après toute évolution importante du système.

V.3.5. Fréquence et séquence de rotation entre différentes attributions

L'AC n'établit aucune de règle concernant cette partie.

V.3.6. Sanctions en cas d'actions non autorisées

L'AA en concertation avec l'ARA décide des sanctions à appliquer lorsqu'un acteur abuse de ses droits ou effectue une opération non conforme à ses attributions.

V.3.7. Exigences vis-à-vis du personnel des prestataires externes

Les personnels contractants doivent respecter les mêmes conditions que celles énoncées dans les rubriques V.3.1, V.3.2, V.3.3 et V.3.4

V.3.8. Documentation fournie au personnel

Les documents dont doit disposer le personnel, en fonction de son besoin d'en connaître pour l'exécution de sa mission, sont les suivants :

- PC de l'IGC/GN ;
- DPC de l'IGC/GN ;
- documents constructeurs des matériels et logiciels utilisés ;
- procédures internes de fonctionnement.

Les AC et l'AE veillent à ce que leur personnel respectif (comme défini dans la DPC) possède bien les documents identifiés ci-dessus en fonction de leur besoin d'en connaître comme le précise la DPC.

V.4. Procédures de constitution des données d'audit

La journalisation d'événements consiste à les enregistrer de façon manuelle ou automatique. Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

V.4.1. Type d'événements à enregistrer

Les entités opérant une composante de l'IGC journalisent au minimum les événements suivants :

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	37 / 62

- événements physiques dont la trace n'est pas fournie automatiquement par le système,
 - autres registres dépendants de la configuration du site physique, à préciser dans la DPC tels que :
 - journaux des accès des personnes,
 - changements concernant les personnes,
 - changement de configuration du système,
 - opérations menées sur les postes informatiques de l'IGC/GN et relatives aux opérations rendues par l'IGC/GN ;
 - opérations menées sur les postes informatiques et matériels du réseau de l'AC subordonnée ;
 - actions menées en cérémonie de clés, consignées dans les procès-verbaux de cérémonie, comme :
 - initialisation de secrets,
 - affectation de secrets à des porteurs de secrets,
 - utilisation de secrets,
 - destruction de secrets.
 - publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- événements généraux tracés par le système ou une application :
 - démarrage et arrêt des applications,
 - connexion / déconnexion des utilisateurs ayant des rôles de confiance
 - modification de paramètres de configuration,
 - installation et désinstallation d'un logiciel ou périphérique matériel,
 - messages d'alerte de l'application, du système d'exploitation ou du réseau ;
 - création de nouveaux comptes.
 - modification ou suppression de comptes utilisateurs
 - changements de mots de passe,
 - modifications de droits d'accès,
- événements métiers tracés par les applications :
 - demande :
 - enregistrement d'un RC ;
 - réception d'une demande de certificat ;
 - validation / rejet d'une demande de certificat ;
 - génération de certificat :
 - génération des certificats des services applicatifs ;
 - acceptation du certificat par le RC ;
 - remise du certificat au RC.
 - révocation de certificat :
 - demande de révocation,
 - révocation de certificat,
 - génération d'une LCR,
 - publication d'une LCR.
 - communications avec le service de publication ;
- remise à zéro du journal d'audit,

Pour tout événement, les informations minimales enregistrées sont :

- date et heure de l'opération,
- nom de l'exécutant,
- type de l'opération,
- résultat de l'événement

En fonction du type de l'événement, d'autres informations peuvent être ajoutées :

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	38 / 62

- organisme destinataire de l'opération,
- nom des personnes présentes,
- nom du représentant de l'ARA et des AC subordonnées,
- cause de l'événement,
- autre information caractérisant l'événement (un identifiant par exemple).

V.4.2. Fréquence de traitement des journaux d'événements

L'analyse du contenu des journaux d'événements est effectuée de manière régulière par l'AC de l'IGC/GN, au minimum une fois par semaine. Un traitement particulier pour les alertes est décrit dans la DPC.

V.4.3. Période de conservation des journaux d'événements

Les journaux sont conservés 1 mois sur site et archivés jusqu'à la fin de vie de l'IGC/GN sur le site de rétention des archives.

V.4.4. Protection des journaux d'événements

Les journaux d'événements sont protégés en intégrité et confidentialité conformément aux réglementations pour les informations classifiées « Diffusion restreinte ».

V.4.5. Procédure de sauvegarde des journaux d'événements

Chaque entité opérant une composante de l'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'événements pour la composante considérée, conformément aux exigences de la présente PC.

V.4.6. Système de collecte des journaux d'événements

Les journaux d'événements sont centralisés dans un outils de collecte.

V.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement

La notification de l'enregistrement des événements est réalisée lors de la signature des CGU.

V.4.8. Évaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée. Les journaux d'événements sont contrôlés une fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec. Ils sont analysés dans leur totalité au moins une fois par semaine.

Cette analyse donne lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'événements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) est effectué une fois par mois, ceci afin de vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.

V.5. Archivage des données

V.5.1. Types de données à archiver

L'AC prend des dispositions en matière d'archivage pour assurer la pérennité des informations ou données produites, en particulier les journaux constitués par les différentes composantes de l'IGC.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	39 / 62

L'archivage permet la conservation des preuves liées aux opérations de certification (dossiers de demande, récépissés de remise de carte...), que ces documents se trouvent sous forme papier ou électronique. Il assure leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les conditions générales d'utilisation ;
- les accords contractuels avec d'autres AC ;
- les certificats et LCR tels qu'émis et publiés ;
- les dossiers de demande ;
- les justificatifs d'identité des RC ;
- les journaux d'événements des différentes entités de l'IGC ;
- les procès-verbaux de cérémonies de clés.

V.5.2. Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé jusqu'à la fin de vie de l'IGC/GN, et au minimum 10 ans, sur le site de rétention des archives.

Certificats, LCR émis par l'AC

Les certificats de clés de services applicatifs et d'AC, ainsi que les LCR / LAR produites sont archivé jusqu'à la fin de vie de l'IGC/GN, et au minimum 10 ans, sur le site de rétention des archives.

Journaux d'événements

Les journaux d'événements traités au chapitre V.4 seront archivé jusqu'à la fin de vie de l'IGC/GN, et au minimum 10 ans après leur génération. Des mesures de contrôles d'accès, de redondance et de contrôle des conditions de stockage assurent leur intégrité.

Autres journaux

La DPC précise les moyens mis en œuvre pour archiver les autres journaux.

V.5.3. Protection des archives

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

- protégées en intégrité ;
- accessibles uniquement aux personnes autorisées ;
- disponible pour pouvoir être relues et exploitées.

La DPC précise les moyens mis en œuvre pour archiver les pièces en toute sécurité.

V.5.4. Procédure de sauvegarde des archives

La DPC décrit la procédure de sauvegarde des archives.

V.5.5. Exigences d'horodatage des données

Cf. chapitre V.4.4 pour la datation des journaux d'événements.

Le chapitre VI.8 précise les exigences en matière de datation / horodatage.

V.5.6. Système de collecte des archives

Le système de collecte des archives est interne à l'IGC et respecte les exigences de protection des archives concernées.

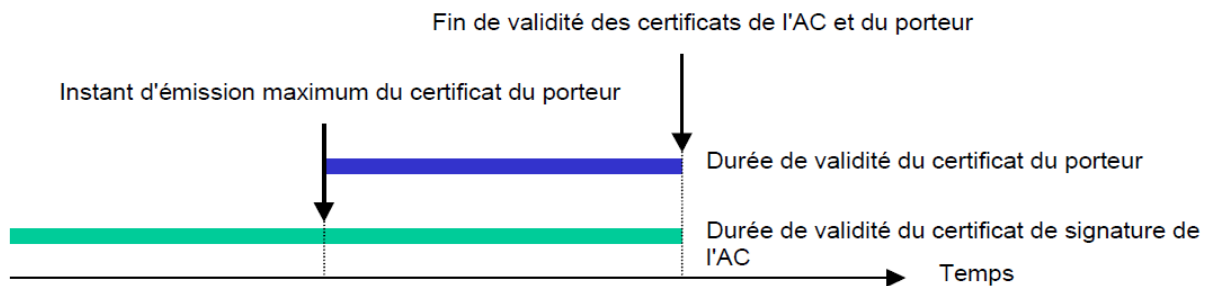
Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	40 / 62

V.5.7. Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) peuvent être récupérées dans un délai inférieur à deux (2) jours ouvrés.

V.6. Changement de clé 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.

V.7. Reprise suite à compromission et sinistre

V.7.1. Procédures de remontée et de 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. Ces procédures et moyens permettent de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

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 est traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, est faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible. L'AC doit également prévenir directement et sans délai le CERT-FR (cert-fr.cossi@ssi.gouv.fr, communication protégée en confidentialité si nécessaire).

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou les services applicatifs devient insuffisant pour son utilisation prévue restante, alors l'AC :

- informe tous les RC et les tiers utilisateurs de certificats. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- révoque tout certificat concerné.

V.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan est testé au minimum 1 fois tous les 2 ans.

V.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant est immédiatement révoqué : cf. chapitre IV.9.

En outre, l'AC respecte au minimum les engagements suivants :

- informer les entités suivantes de la compromission : tous les RC, et les tiers utilisateurs et d'autres AC ;
- indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

V.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 la présente PC.

V.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.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

Transfert d'activité ou cessation d'activité¹ affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC:

- 1) Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des services applicatifs et des informations relatives aux certificats, archivage de séquestre le cas échéant).
- 2) Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication de l'état des certificats), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC.

L'AC avisera les RC et les utilisateurs de certificats aussitôt que nécessaire, sous un délai d'un mois au minimum. L'AC établira un plan d'action circonstancié et le communiquera à l'ANSSI afin de minimiser les impacts de tous ordres de cet événement. L'AC tiendra informée l'ANSSI de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus

Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité sera progressive de telle sorte que

¹Cessation d'activité d'une composante autre que l'AC

seules les obligations ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans cette PC.

La DPC stipule les dispositions prises en cas de cessation de service, en particulier :

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

Lors de l'arrêt du service, l'AC doit :

- 1) s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- 1) prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- 2) révoquer son certificat ;
- 3) révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- 4) informer (par exemple par récépissé) tous les responsables des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre III.2.3).

VI. Mesures de sécurité techniques

VI.1. Génération et installation de bi-clés

VI.1.1. Génération des bi-clés

VI.1.1.1 Clés d'AC

Les clés de signature d'AC sont générées dans un environnement sécurisé (cf. chapitre V).

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique qualifié au niveau renforcé.

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre V.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies se déroulent suivant des scripts préalablement définis.

Le script de « Cérémonie des clés » indique :

- L'ensemble des rôles des participants de la cérémonie. Au moins deux personnes ayant des rôles de confiance et un témoin externe à l'AC et impartial participent à la cérémonie.
- Les fonctions de chacun de ces rôles et les phases auxquelles ils interviennent
- Leurs responsabilités durant la cérémonie et à l'issue de celle-ci
- Les preuves qui seront recueillis durant la cérémonie.

La cérémonie fait l'objet d'un PV signé des participants attestant qu'elle s'est déroulée conformément à la procédure prévue et démontrant que l'intégrité et la confidentialité de la génération de la paire de clé a été assurée.

La cérémonie peut inclure la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC. Les parts de secrets sont remis pendant la cérémonie à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Le PV de cérémonie liste les parts de secrets générés ou utilisés et leurs détenteurs respectifs.

VI.1.1.2 Clés du service applicatif générées par l'AC

Sans objet, l'AC ne génère pas les clés des services applicatifs.

VI.1.1.3 Clés du service applicatif générées au niveau du service applicatif

La génération de la bi-clé de cachet doit être effectuée dans un dispositif cryptographique (HSM) qualifié au niveau renforcé. Cette génération est à la charge de l'entité responsable du certificat, qui la délègue à une entité centralisée exploitant ce HSM de façon sécurisée. Les clés privées des services applicatifs et des clés d'AC sont stockées dans des HSM distincts (au moins des partitions distinctes).

Le RC s'engage explicitement dans sa demande de certificat à ce que la bi-clé ait été générée par le moyen exposé ci-dessus.

VI.1.2. Transmission de la clé privée à son propriétaire

Sans objet.

VI.1.3. Transmission de la clé publique à l'AC

Les requêtes de demande de certificat du RC sont transmises à l'AC au format PKCS#10, dont l'intégrité et l'origine sont authentifiées par l'AC.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	44 / 62

VI.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les clés publiques de vérification de signature de l'AC sont diffusées auprès des utilisateurs de certificats via le certificat de l'AC publié conformément aux dispositions du §II. La chaîne de certification remonte jusqu'au certificat de l'IGC/A dont l'intégrité peut être vérifiée sur le site de l'ANSSI.

VI.1.5. Tailles des clés

Les clés d'AC sont des clés RSA 4096 bits.

Les clés des services applicatifs sont des clés RSA 2048 bits.

Ces caractéristiques sont conformes à l'état de l'art et respectent les exigences de sécurité du RGS.

VI.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

Toutes les clés sont générées dans des composants qualifiés. Il peut s'agir des puces des cartes ou des HSM. La qualité des bi-clés et leurs paramètres de génération dépendant des équipements utilisés et ces derniers étant qualifiés dans ce cadre, elles sont réputées conformes à l'état de l'art tant que la qualification est maintenue.

VI.1.7. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats ou de de LCR / LAR.

L'utilisation de la clé privée du service applicatif et du certificat associé est strictement limitée à la fonction de sécurité concernée (cf. chapitres I.5.1.1, IV.5).

VI.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

VI.2.1. Standards et mesures de sécurité pour les modules cryptographiques

VI.2.1.1 Modules cryptographiques de l'AC

Les modules cryptographiques utilisés par l'AC, pour ses clés de signature et celles des services applicatifs, sont des modules cryptographiques qualifiés au niveau renforcé.

VI.2.1.2 Dispositifs de protection des éléments secrets des services applicatifs

Les clés privées des services applicatifs sont générées et restent protégées par un dispositif cryptographique qualifié (HSM) au niveau renforcé.

VI.2.2. Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets.

VI.2.3. Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des services applicatifs ne sont en aucun cas séquestrées.

VI.2.4. Copie de secours de la clé privée

Les clés privées des services applicatifs peuvent faire l'objet de copie de secours, par le mécanisme natif du HSM, tel qu'exposé ci-dessous pour les clés d'AC.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	45 / 62

Les clés privées d'AC font l'objet de copies de secours dans des fichiers chiffrés, générés par le mécanisme natif du module cryptographique. Ce chiffrement offre un niveau de sécurité équivalent au stockage au sein du module cryptographique.

Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne sont à aucun moment en clair en dehors du module cryptographique.

VI.2.5. Archivage de la clé privée

Les clés privées de l'AC ne sont en aucun cas archivées.

Les clés privées des services applicatifs ne sont en aucun cas archivées ni par l'AC ni par aucune des composantes de l'IGC.

VI.2.6. Transfert de la clé privée vers / depuis le module cryptographique

Pour les clés privées d'AC comme pour les clés privées de service applicatif, tout transfert (sauvegarde, restauration) se fait sous forme chiffrée, conformément aux exigences du chapitre VI.2.4.

VI.2.7. Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC et des services applicatifs sont stockées dans un module cryptographique qualifié au niveau renforcé, excepté leurs sauvegardes qui respectent des exigences du chapitre VI.2.4.

L'AC garantit, en tout état de cause, que les clés privées ne sont pas compromises pendant leur stockage ou leur transport.

VI.2.8. Méthode d'activation de la clé privée

VI.2.8.1 Clés privées d'AC

L'activation des clés privées d'AC dans le module cryptographique est contrôlée via des données d'activation (cf. chapitre VI.4) et fait intervenir au moins deux personnes dans des rôles de confiance (des porteurs de secrets).

VI.2.8.2 Clés privées des services applicatifs

L'activation des clés privées des services applicatifs dans le module cryptographique est contrôlée via des données d'activation (cf. chapitre VI.4) et fait intervenir au moins deux personnes dans des rôles de confiance (des porteurs de secrets).

VI.2.9. Méthode de désactivation de la clé privée

VI.2.9.1 Clés privées d'AC

La désactivation des clés privées d'AC dans le module cryptographique est automatique dès qu'il est arrêté, mis ou jour au niveau de sa configuration logicielle ou technique.

VI.2.9.2 Clés privées des services applicatifs

La désactivation des clés privées des services applicatifs dans le module cryptographique est automatique dès qu'il est arrêté, mis ou jour au niveau de sa configuration logicielle ou technique.

VI.2.10. Méthode de destruction des clés privées

VI.2.10.1 Clés privées d'AC

La destruction des clés privées d'AC dans le matériel cryptographique est réalisée par une fonction nominale du matériel qui garantit un effacement sécurisé. La destruction des sauvegardes est réalisée

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	46 / 62

conformément à des directives précises d'effacement sécurisé des supports (effacement et écrasements successifs).

VI.2.10.2 Clés privées des services applicatifs

La destruction des clés privées des services applicatifs dans le matériel cryptographique est réalisée par une fonction nominale du matériel qui garantit un effacement sécurisé. La destruction des sauvegardes est réalisée conformément à des directives précises d'effacement sécurisé des supports (effacement et écrasements successifs).

VI.2.11. Niveau de qualification du module cryptographique et des dispositifs de protection des éléments secrets

Le module cryptographique de l'AC et des services applicatifs est qualifié par l'ANSSI au niveau renforcé.

VI.3. Autres aspects de la gestion des bi-clés

VI.3.1. Archivage des clés publiques

Les clés publiques de l'AC et des services applicatifs sont archivées dans le cadre de l'archivage des certificats correspondants.

VI.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des services applicatifs couverts par la présente PC ont une durée de vie maximale de 3 ans.

L'AC s'interdit d'émettre des certificats dont la durée de vie dépasse celle du certificat de l'AC.

VI.4. Données d'activation

VI.4.1. Génération et installation des données d'activation

VI.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération et l'installation des données d'activation du module cryptographique de l'AC se font lors de la phase d'initialisation et de personnalisation de ce module, dans le cadre d'une cérémonie de clés. Les porteurs de ces données en sont les détenteurs exclusifs, ils les reçoivent directement en main propre et sont responsables de leur confidentialité et de leur intégrité.

VI.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du service applicatif

La génération et l'installation des données d'activation du module cryptographique de l'AC se font lors de la phase d'initialisation et de personnalisation de ce module, dans le cadre d'une cérémonie de clés. Les porteurs de ces données en sont les détenteurs exclusifs, ils les reçoivent directement en main propre et sont responsables de leur confidentialité et de leur intégrité.

VI.4.2. Protection des données d'activation

VI.4.2.1 Protection des données d'activation correspondant à la clé privée de l'AC

Cf. §VI.4.1.1.

VI.4.2.2 Protection des données d'activation correspondant aux clés privées des services applicatifs

Cf. §VI.4.1.2.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	47 / 62

VI.4.3. Autres aspects liés aux données d'activation

Il n'y a pas d'autres aspects liés aux données d'activation.

VI.5. Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques répondent à une politique de sécurité interne de la Gendarmerie nationale, qui couvre les objectifs de sécurité de l'IGC.

VI.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

La DPC décrit un ensemble de mesures permettant de répondre aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique),
- gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels,
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- protection du réseau contre toute intrusion d'une personne non autorisée,
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- fonctions d'audits (non-répudiation et nature des actions effectuées),
- éventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés secrètes ou privées des composantes de l'infrastructure font l'objet de mesures particulières de sécurité.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système sont mises en place.

VI.5.2. Niveau de qualification des systèmes informatiques

Le module cryptographique de l'AC est qualifié par l'ANSSI au niveau renforcé.

VI.6. Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité décrites dans la DPC garantissent le maintien du niveau de sécurité durant toute la durée de vie de l'IGC, donc pour le cycle de vie complet des biens sensibles.

VI.6.1. Mesures de sécurité liées au développement des systèmes

L'implémentation de l'infrastructure de l'IGC est documentée. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau sont documentées et contrôlées.

Cette implémentation répond aux objectifs de sécurité définis en amont pour l'IGC et utilise des systèmes et des produits fiables qui sont protégés contre toute modification.

VI.6.2. Mesures liées à la gestion de la sécurité

Les processus internes de gestion de configuration de l'AC garantissent l'évaluation et la documentation de toute évolution significative, afin de maintenir le niveau de sécurité et l'emploi des matériels qualifiés dans l'environnement préconisé.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	48 / 62

VI.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes

La DPC décrit les processus d'évaluation.

VI.7. Mesures de sécurité réseau

L'IGC n'est pas interconnectée avec des réseaux publics, excepté pour la publication des informations sur un site internet. Cet accès est protégé par contrôles d'accès et une restriction aux seuls protocoles nécessaires.

Les composants du réseau sont sécurisés et leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC. Les modules cryptographiques sont maintenus dans un environnement dédié physiquement sécurisé.

VI.8. Horodatage / Système de datation

Les événements consignés dans les différents journaux de l'IGC sont horodatés par l'horloge des serveurs sur lesquels ils sont générés. Tous les serveurs en ligne sont synchronisés sur une source fiable de temps UTC, au minimum à la seconde près. L'heure des serveurs hors ligne est corrigée si besoin avant la réalisation d'une opération de l'IGC.

VII. Profils des certificats et des LCR

VII.1. Format du certificat de l'AC GN Machines Cachet serveur

Le certificat de l'AC GN Machines Cachet serveur suit le gabarit suivant :

Nom du champ	Contenu
Champs de base	
Version (version)	2 (version 3)
Numéro de série (serialNumber)	Attribué par l'AC racine de l'IGC/GN
Algorithme de signature (signature)	Algorithme RSA / SHA-2 : <ul style="list-style-type: none"> Champ « algorithm » : sha256WithRSAEncryption Champ « parameters » : non présent
Émetteur (issuer)	C = FR O = Gendarmerie nationale OU = 0002 157000019 CN = AC Racine Gendarmerie nationale
Valide à partir du (validity/notBefore)	<i>Date de génération par l'AC Racine</i>
Valide jusqu'au (validity/notAfter)	<i>6 ans après la date de génération</i>
Objet (subject)	C = FR O = Gendarmerie nationale OU = 0002 157000019 CN = AC GN Machines Cachet serveur
Clé publique (subjectPublicKeyInfo)	Algorithme RSA : <ul style="list-style-type: none"> Champ « algorithm/algorithm » : rsaEncryption Champ « algorithm/parameters » : non présent Champ « subjectPublicKey » : clé publique de 4096 bits
Extensions	
Contraintes de base (basicConstraints) Critique	Champ « cA » : TRUE (certificat d'autorité de certification) Champ « pathLenConstraint » : 0 (cette AC est une AC terminale)
Identifiant de clé d'autorité (authorityKeyIdentifier) Non critique	<i>Valeur « subjectKeyIdentifier » du certificat de l'ACR de l'IGC/GN.</i> Seul le champ « keyIdentifier » sera utilisé
Identifiant de clé de sujet (subjectKeyIdentifier) Non critique	<i>Empreinte numérique SHA-1 de la clé publique de l'objet.</i>
Utilisation de clé (keyUsage) Critique	Signature de certificats, Signature de listes des certificats révoqués (keyCertSign, cRLSign)
Politiques de certification (certificatePolicies)	Champ « policyIdentifier » : contient l'identifiant de la politique de certification régissant cette AC, du type :

Nom du champ	Contenu
Non critique	OID = 1.2.250.1.189.1.1.1.6 Champ « policyQualifiers » : contient un champ « PolicyQualifierInfo » de type « CPS » contenant une adresse web pointant vers la page web des PC : URI = https://stsisi.psi.minint.fr/securite/1598/igc/
Nom alternatif de sujet (subjectAltName) Non critique	Champ « rfc822Name » : contient l'adresse de courriel suivante : igc@gendarmerie.interieur.gouv.fr
Points d'accès aux LCR/LAR (cRLDistributionPoints) Non critique	URI= http://crl.gendarmerie.fr/ac-racine-gn-v3.crl URI= http://crl.gendarmerie.interieur.ader.gouv.fr/ac-racine-gn-v3.crl URI= http://crl.gendarmerie.interieur.gouv.fr/ac-racine-gn-v3.crl
Accès aux informations de l'AC (authorityInfoAccess) Non critique	URI= https://stsisi.psi.minint.fr/securite/1598/igc/

VII.2. Format des certificats de cachet des services applicatifs

Les certificats de cachet émis par l'AC subordonnée «AC GN Machines Cachet serveur» suivent le gabarit suivant :

Nom du champ	Contenu
Champs de base	
Version (version)	2 (version 3)
Numéro de série (serialNumber)	Attribué par l'AC Gendarmerie Signature de l'IGC/GN
Algorithme de signature (signature)	Algorithme RSA / SHA-2 : <ul style="list-style-type: none"> Champ « algorithm » : sha256WithRSAEncryption Champ « parameters » : non présent
Émetteur (issuer)	C = FR, O = Gendarmerie nationale, OU = 0002 157000019, CN = AC GN Machines Cachet serveur
Valide à partir du (validity/notBefore)	<i>Date de génération par l'AC GN Machines Cachet serveur</i>
Valide jusqu'au (validity/notAfter)	<i>3 ans après la date de génération</i>
Objet (subject)	C = FR O = Gendarmerie nationale OrganizationIdentifier : NTRFR-157000019 OU = 0002 157000019 OU = Machines Cachet serveur CN= <i>Nom du service applicatif (test pour les certificats de test)</i>
Clé publique (subjectPublicKeyInfo)	Algorithme RSA : <ul style="list-style-type: none"> Champ « algorithm/algorithm » : rsaEncryption

Nom du champ	Contenu
	<ul style="list-style-type: none"> Champ « algorithm/parameters » : non présent Champ « subjectPublicKey » : clé publique de 2048 bits
Extensions	
Contraintes de base (basicConstraints) Critique	Champ « CA » : FALSE (certificat d'entité finale) Champ « pathLenConstraint » : non présent (pas de signification)
Identifiant de clé d'autorité (authorityKeyIdentifier) Non critique	Valeur « subjectKeyIdentifier » du certificat de l'AC émettrice Seul le champ « keyIdentifier » sera utilisé
Identifiant de clé de sujet (subjectKeyIdentifier) Non critique	Empreinte numérique SHA-1 de la clé publique de l'objet.
Utilisation de clé (keyUsage) Critique	Signature (nonRepudiation) DigitalSignature
Politiques de certification (certificatePolicies) Non critique	Champ « policyIdentifier » : contient l'identifiant de la politique de certification régissant cette AC, du type : OID = 1.2.250.1.189.1.1.1.5.1 Champ « policyQualifiers » : contient un champ « PolicyQualifierInfo » de type « CPS » contenant une adresse web pointant vers la page web des PC : URI = https://stsis.psi.minint.fr/securite/1598/igc/ URI = https://www.gendarmerie.interieur.gouv.fr/igc/pc
Points d'accès aux LCR/LAR (cRLDistributionPoints) Non critique	URI = http://crl.gendarmerie.fr/ac-cachet-serveur.crl URI = http://crl.gendarmerie.interieur.ader.gouv.fr/ac-cachet-serveur.crl URI = http://crl.gendarmerie.interieur.gouv.fr/ac-cachet-serveur.crl
Accès aux informations de l'AC (authorityInfoAccess) Non critique	accessMethod : OID 1.3.6.1.5.5.7.48.2 : id-ad-calssuers accessLocation : URI = http://crl.gendarmerie.fr/Certificat_AC_GN_Machines_Cachet_serveur.pem URI = http://crl.gendarmerie.interieur.ader.gouv.fr/Certificat_AC_GN_Machines_Cachet_serveur.pem URI = http://crl.gendarmerie.interieur.gouv.fr/Certificat_AC_GN_Machines_Cachet_serveur.pem
Extensions « QC Statements »	
QC Statements	Déclaration de certificat qualifié
Conformité Certificat qualifié ETSI (QCS-1)	Utilisé
Dispositif qualifié de création de signature	Utilisé

Nom du champ	Contenu
(QSCD) ETSI (QCS-4)	
Type ETSI (QCS-6)	Cachet serveur (eSeal)
URL et langue du PDS ETSI (QCS-5)	URI = https://www.gendarmerie.interieur.gouv.fr/igc/pc Langue : Français

VII.3. Format des listes de révocation (LCR) émises par l'AC GN Machines Cachet serveur

Les listes de révocation émises par l'AC GN Machines Cachet serveur suivent le gabarit suivant :

Nom du champ	Contenu
Champs de base	
Version (version)	1 (version 2)
Algorithme de signature (signature)	Algorithme RSA / SHA-2 : <ul style="list-style-type: none"> Champ « algorithm » : sha256WithRSAEncryption Champ « parameters » : non présent
Émetteur (issuer)	C = FR, O = Gendarmerie nationale, OU = 0002 157000019, CN = AC GN Machines Cachet serveur
Date d'émission (thisUpdate)	<i>Date de génération par l'AC</i>
Date de prochaine mise à jour (nextUpdate)	<i>6 jours après la date de génération</i>
Liste des certificats révoqués	
Numéro de série (userCertificat)	<i>Numéro de série du certificat révoqué</i>
Date de révocation (revocationDate)	<i>Date de révocation du certificat</i>
Laisser les certificats expirés dans la CRL (ExpiredCertsOnCRL)	<i>Utiliser</i>
Extensions de la CRL	
Identifiant de clé d'autorité (authorityKeyIdentifier) Non critique	<i>Valeur « subjectKeyIdentifier » du certificat de l'AC émettrice</i> Seul le champ « keyIdentifier » sera utilisé
Numéro de CRL (CRLNumber) Non critique	<i>Numéro séquentiel de la CRL</i>
Empreinte numérique signée (signatureValue)	<i>Suite de bits contenant le bloc de données signé par l'émetteur</i>

VII.4. Format des certificats de test de cachet des services applicatifs

Comme indiqué dans le profil de certificat, les certificats de tests reprendront les données suivantes :

CN= test (éventuellement test1, test2, ...

Ces certificats ne servent qu'à l'IGC dans le cadre des audits, des tests... et doivent être révoqués au plus tôt après la fin de leur utilisation.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	54 / 62

VIII. Audit de conformité et autres évaluations

La suite du présent chapitre concerne les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC (et non ceux de qualification RGS).

VIII.1. Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC procède à un contrôle de conformité de cette composante.

L'AC procède également régulièrement à un contrôle de conformité de l'ensemble de son IGC, 1 fois tous les 2 ans.

VIII.2. Identités / qualifications des évaluateurs

Le contrôle d'une composante est assigné par l'AC à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

VIII.3. Relations entre évaluateurs et entités évaluées

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

VIII.4. Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

L'AC est en mesure de justifier qu'il a pris les mesures nécessaires pour assurer la protection des échanges d'information entre les différentes composantes de l'IGC. Elle vérifie périodiquement les mesures de sécurité prises dans ce cadre, par exemple au moyen d'audits techniques.

VIII.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : "réussite", "échec", "à confirmer".

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

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

VIII.6. Communication des résultats

Les résultats des audits de conformité seront tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	55 / 62

IX. Autres problématiques métiers et légales

IX.1. Tarifs

Sans objet, les services de l'IGC/GN n'étant pas facturés aux AC subordonnées ni aux entités finales.

IX.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

Sans objet.

IX.1.2. Tarifs pour accéder aux certificats

Sans objet.

IX.1.3. Tarifs pour accéder aux informations d'état et de révocation des certificats

Sans objet.

IX.1.4. Tarifs pour d'autres services

Sans objet.

IX.1.5. Politique de remboursement

Sans objet.

IX.2. Responsabilité financière

IX.2.1. Couverture par les assurances

L'état étant le propre assureur, tous les frais seront couverts par le ministère de l'intérieur.

IX.2.2. Autres ressources

Sans objet

IX.2.3. Couverture et garantie concernant les entités utilisatrices

Tout usage non explicitement permis est interdit et engage la responsabilité du responsable du certificat.

IX.3. Confidentialité des données professionnelles

IX.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- la DPC de l'AC,
- les clés privées de l'AC, des composantes et des services applicatifs porteurs de certificats,
- les données d'activation associées aux clés privées d'AC et des services applicatifs,
- tous les secrets de l'IGC,
- les journaux d'événements des composantes de l'IGC,
- les dossiers d'enregistrement des RC,
- les causes de révocations, sauf accord explicite du RC.

IX.3.2. Informations hors du périmètre des informations confidentielles

Les informations publiques sont les politiques de certification, les certificats d'AC ainsi que les CRL.

IX.3.3. Responsabilités en termes de protection des informations confidentielles

L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre IX.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'AC en garantit l'intégrité.

L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des RC à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au RC.

IX.4. Protection des données à caractère personnel

IX.4.1. Politique de protection des données à caractère personnel

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

IX.4.2. Données à caractère personnel

Les données considérées comme personnelles sont au moins les suivantes :

- les causes de révocation des certificats des services applicatifs (qui sont considérées comme confidentielles sauf accord explicite du RC) ;
- le dossier d'enregistrement du RC.

IX.4.3. Données à caractère non personnel

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

IX.4.4. Responsabilité en termes de protection des données à caractère personnel

Cf. IX.15.

IX.4.5. Notification et consentement d'utilisation des données à caractère personnel

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

IX.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Cf. IX.15.

IX.4.7. Autres circonstances de divulgation de données à caractère personnel

Sans objet.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	57 / 62

IX.5. Droits de propriété intellectuelle

L'ensemble des moyens de l'infrastructure de gestion des clés respecte et applique la législation et la réglementation en vigueur sur le territoire français.

IX.6. Interprétations contractuelles et garanties

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

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre VII-VIII) et l'organisme de qualification,
- respecter les accords ou contrats qui les lient entre elles ou aux RC, 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.

IX.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 son RC a accepté le certificat, conformément aux exigences du chapitre IV.4 ci-dessus.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.
- Prendre toutes les mesures raisonnables pour s'assurer que les RC 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 RC 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.

L'AC est responsable de la conformité de sa Politique de Certification avec les exigences émises dans la présente PC. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la présente PC, par elle-même ou l'une de ses composantes. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des RC à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AC.

En cas de non-respect ponctuel des obligations décrites dans la présente PC, l'Administration se réserve le droit de refuser temporairement ou définitivement les certificats de l'AC conformément à la réglementation en vigueur.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	58 / 62

IX.6.2. Service d'enregistrement

Cf. les obligations pertinentes du chapitre IX.6.1.

IX.6.3. RC

Le RC a le devoir de :

- 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 oeuvre ;
- protéger l'accès à la base de certificats du service applicatif ;
- respecter les conditions d'utilisation de la clé privée du service applicatif et du certificat correspondant ;
- informer l'AC de toute modification concernant les informations contenues dans le certificat électronique ;
- faire, sans délai, une demande de révocation du certificat électronique dont il est responsable auprès de l'AC en cas de compromission ou de suspicion de compromission de la clé privée correspondante (ou de ses données d'activation).

La relation entre le RC et l'AC ou ses composantes est formalisée par un engagement du RC visant à certifier l'exactitude des renseignements et des documents fournis.

IX.6.4. Utilisateurs de certificats

Les utilisateurs utilisant les certificats doivent :

- vérifier et respecter l'usage pour lequel un certificat a été émis ;
- pour chaque certificat de la chaîne de certification, du certificat du service applicatif jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC ;
- contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application qu'ils utilisent.

IX.6.5. Autres participants

Sans objet

IX.7. Limite de garantie

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

IX.8. Limite de responsabilité

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

IX.9. Indemnités

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

IX.10. Durée et fin anticipée de validité de la PC

IX.10.1. Durée de validité

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

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	59 / 62

IX.10.2. Fin anticipée de validité

La présente PC peut être remplacée par une version plus récente (cf. IX.12). La présente PC peut par exemple évoluer suite à la publication d'une nouvelle version de la PC Type du RGS.

Une évolution de la PC n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

IX.10.3. Effets de la fin de validité et clauses restant applicables

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

IX.11. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes.
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

IX.12. Amendements à la PC

IX.12.1. Procédures d'amendements

L'AC devra contrôler que tout projet de modification de sa PC reste conforme aux exigences de la PC Type du RGS et des éventuels documents complémentaires du [RGS]. En cas de changement important, l'AC fera appel à une expertise technique pour en contrôler l'impact.

IX.12.2. Mécanisme et période d'information sur les amendements

Les nouvelles politiques de certification seront proposées au comité de pilotage qui en validera les modifications. Après validation, elles seront publiées dans le mois suivant et rentreront en application dès leur publication.

Les changements majeurs modifiant la relation avec le porteur feront l'objet d'un nouvel OID qui ne s'appliquera qu'aux nouveaux certificats.

IX.12.3. Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des RC et des services applicatifs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

En particulier, l'OID de la PC de l'AC doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC) intervient dans les exigences de la PC Type des certificats électroniques de services applicatifs.

IX.13. Dispositions concernant la résolution de conflits

Toute réclamation doit être adressée à l'inspection générale de la gendarmerie nationale.

L'adresse courriel de l'inspection générale de la gendarmerie nationale est : iggn@gendarmerie.interieur.gouv.fr

IX.14. Juridictions compétentes

Application de la législation et de la réglementation en vigueur sur le territoire français.

Diffusion	Politique Certification	Identifiant du document	Page
Publique	AC GN Machines Cachet serveur	1.2.250.1.189.1.1.1.5.1	60 / 62

IX.15. Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre X ci-dessous.

IX.16. Dispositions diverses

IX.16.1. Accord global

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

IX.16.2. Transfert d'activités

Cf. chapitre V.8-11.

IX.16.3. Conséquences d'une clause non valide

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

IX.16.4. Application et renonciation

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

IX.17. Autres dispositions

L'AC n'a pas d'autres dispositions que celles exposées précédemment

IX.17.1. Force majeure

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

X. Annexe 1 : Documents cités en référence

X.1. Réglementation

[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005

X.2. Documents techniques

[RGS]	Référentiel Général de Sécurité - Version 2.0
[RGS_A1]	RGS - Fonction de sécurité « Cachet » - Version 3.0
[RGS_A4]	RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 3.0
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 2.03
[ETSI 319 412]	EN EN 319 412 - 319 412-1 v1.1.1: Overview and common data structures - 319 412-2 v2.1.1: Certificate profile for certificates issued to natural persons - 319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons - 319 412-4 v1.1.1: Certificate profile for web site certificates issued to organisations - 319 412-5 v2.1.1: QCStatements
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version d'août 2005 (complétée par les correctifs techniques Corrigendum 1 de janvier 2007 et Corrigendum 2 de novembre 2008)
[PC_AC_RACINE]	Politique de certification de l'AC Racine de la Gendarmerie Nationale
[GESTION_ROLE S]	Rôles et responsabilités de l'IGC de la Gendarmerie Nationale
[Cessation d'activité]	Procédure_cessation_activité