Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Secrétariat général de la défense nationale

IGC/A

POLITIQUE DE CERTIFICATION CONCERNANT LES AUTORITÉS DE CERTIFICATION RACINES GOUVERNEMENTALES

Version	**:**	**2.0**
Référence	**:**	**OID : 1.2.250.1.121.1.1.2.**
Date d'approbation	**:**	**20/11/2008**
Nombre de pages	**:**	**87**

Historique des modifications

Version	Date	Objet de la modification	Statut
0.1	05/07/01	Création du document.	Ébauche
1.1	16/07/02	OID officiel : 1.2.250.1.121.1.1.1	Validé
1.1 révision A	20/04/07	Première révision du document : • intégration des préconisations issues de l'analyse juridique de la PC, principalement sur la définition des acteurs de l'IGC/A et la précision de leurs fonctions et responsabilités ; • correction des variables de temps ; • correction des formats de certificats et LAR ; • renvoi de l'annexe sur les rôles dans la DPC ; • précisions sur l'enregistrement ; • remise en forme. (Cette révision n'intègre pas d'informations complémentaires concernant la publication de listes de certificats révoqués). OID officiel : 1.2.250.1.121.1.1.1	Validé par P. Pailloux, directeur central de la sécurité des systèmes d'information Le 20/04/2007
2.0 β	05/04/08	Révision majeure du document intégrant : • la fonction de révocation ; • la présentation de la nouvelle organisation des services de l'IGC/A ; • la précision des gabarits de certificats ; • la présentation suivant le plan du standard RFC3647.	Version pilote
2.0	20/11/08	Ajout des différents types d'autorités administratives, en conformité avec l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. OID officiel : 1.2.250.1.121.1.1.2	Validé par P. Pailloux, directeur central de la sécurité des systèmes d'information Le 20/11/2008

Sommaire

1 INTRODUCTION

1.1 Définitions et acronymes

1.1.1 Définitions

Autorité

Le terme « autorité » est employé seul pour désigner :

- soit une personne qui commande, au titre d'une fonction administrative, des agents et des services utilisant des systèmes informatiques et des informations selon une organisation et des procédures particulières ;
- soit le service représenté par cette personne.

Cette définition est plus précise que celle généralement employée dans les textes techniques de référence dans le domaine des IGC (cf. annexe 2 Documents techniques). En effet, l'autorité y est souvent définie comme une « entité », terme ambigu pouvant désigner à la fois une personne ou un groupe de personnes et un système informatique. Or pour que des responsabilités puissent lui être valablement attribuées, il est nécessaire de faire apparaître l'autorité comme une personne. Néanmoins, le certificat qui est délivré à une autorité n'identifie pas une personne physique, mais l'organisme qu'elle représente.

La définition juridique d'une autorité prise comme référence dans cette PC est mentionnée à l'ANNEXE 1 : Glossaire.

Autorité administrative

L'expression « autorité administrative » employée dans la suite du document doit être comprise dans le sens de l'ordonnance [ORD05-1516] c'est-à-dire « les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L.223-16 et L.351-21 du code du travail et les autres organismes chargés de la gestion d'un service public administratif ».

Autorité de certification racine

Une autorité de certification racine (ACR) est l'autorité responsable de la gestion des certificats électroniques délivrés par la ou les IGC d'un organisme tout au long de leur cycle de vie, vis-à-vis des porteurs et des utilisateurs de ces certificats. Dans le cadre de cette PC, les ACR considérées sont un cas particulier de ce que la [PRIS] définit comme un prestataire de service de confiance ; elles représentent chacune une ou plusieurs autorités administratives. L'ACR émet et révoque les certificats des autorités de certification qu'elle fédère sous la forme d'une hiérarchie dont elle constitue le sommet (ou la racine, si l'on modélise cette hiérarchie sous la forme d'un arbre dont les feuilles sont les certificats des utilisateurs finaux). Elle signe elle-même (auto-signe) les certificats de ses propres bi-clés de signature. Elle peut néanmoins utiliser les certificats délivrés par une autre ACR à laquelle elle fait confiance. Elle porte la responsabilité de l'application de la PC des AA qui l'ont mandatée, et des ACR qui lui délivrent des certificats dès lors qu'elle les utilise.

Selon l'organisation définie pour l'IGC dont elle a la responsabilité, l'ACR peut s'appuyer sur une autorité d'enregistrement, rendre compte à une autorité responsable d'application, etc. Pour des raisons de simplification, seule l'ACR sera mentionnée dans ce document. Charge à cette ACR de transmettre à qui de droit, selon sa politique de certification, les informations échangées avec les services de l'IGC/A.

ACR gouvernementale

On désigne par « ACR gouvernementale » une autorité de certification racine de chaînes de certification d'un ministère ou d'un service du Premier ministre.

ACR AAI

On désigne par « ACR AAI » :

- une autorité de certification racine de chaînes de certification d'une autorité indépendante ;
- l'une des institutions ou juridictions suivantes :
    - la Présidence de la République ;
    - le Conseil constitutionnel ;
    - le Conseil supérieur de la magistrature ;
    - l'Assemblée nationale ;
    - le Tribunal des conflits ;
    - le Sénat ;
    - la Cour de justice de la République ;
    - le Conseil économique et social ;
    - le Conseil d'État ;
    - la Cour de cassation ;
    - la Cour des comptes.

ACR territoriale

On désigne par « ACR territoriale » une autorité de certification racine de chaînes de certification agissant sous la responsabilité d'une ou plusieurs collectivités territoriales.

ACR EPCA

On désigne par « ACR EPCA » une autorité de certification racine de chaînes de certification agissant sous la responsabilité d'un ou plusieurs établissements publics à caractère administratif.

ACR RPS

On désigne par « ACR RPS » une autorité de certification racine de chaînes de certification agissant sous la responsabilité d'un ou plusieurs organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L.223-16 et L.351-21 du code du travail.

ACR SPA

On désigne par « ACR SPA » une autorité de certification racine de chaînes de certification agissant sous la responsabilité d'un ou plusieurs organismes chargés de la gestion d'un service public administratif

Utilisateur final ou porteur de certificat

En règle générale, l'utilisateur final (UF) est une personne physique ou morale, ou un système informatique, qui utilise une bi-clé et le certificat de clé publique associé qui lui a été délivré par l'autorité de certification (AC) d'une IGC (l'AC peut lui délivrer également la bi-clé). Dans le cas présent de l'IGC/A, les utilisateurs finaux sont exclusivement des autorités de certification racines

auxquelles l'IGC/A délivre des certificats pour des bi-clés générées par elles-mêmes et non pas par l'IGC/A. On préférera employer dans cette PC le terme « porteur de certificat » pour les ACR, pour ne pas apporter de confusion avec les certificats délivrés aux personnes ou systèmes par les AC terminales de la chaîne de validation.

Utilisateur de certificats

On désigne par « utilisateurs de certificat (UC)» les personnes ou les systèmes informatiques qui prennent connaissance des informations portées dans un certificat de clé publique, dans le but d'en vérifier l'intégrité et l'origine, ainsi que l'état (encore valide ou révoqué) à un moment donné. Pour un certificat délivré par une AC d'une chaîne de confiance certifiée par l'IGC/A cette vérification peut être automatique si le système informatique utilisé (applications clientes ou serveurs, matériel de communication) a enregistré les certificats de l'IGC/A dans sa liste de certificats d'autorités de confiance.

Les définitions d'autres termes relatifs aux IGC sont portées en annexe 1.

1.1.2 Acronymes

AA	Autorité Administrative
AC	Autorité de Certification
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement
AQSSI	Autorité Qualifiée en matière de Sécurité des Systèmes d'Information
COSSI	Centre Opérationnel en Sécurité des Systèmes d'Information
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DPC	Déclaration des Pratiques de Certification
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information
HFD	Haut Fonctionnaire de Défense
HFDS	Haut Fonctionnaire de Défense et de Sécurité
IGC	Infrastructure de Gestion de Clés
ISO	International Organization for Standardization
LAR	Liste des certificats d'AC Révoqués
OID	Object Identifier (Identifiant d'Objet)
PC	Politique de Certification
RSA	Rivest Shamir Adelman
SGDN	Secrétariat Général de la Défense Nationale

SHA-1	Secure Hash Algorithm version 1
SP	Service de Publication
UC	Utilisateur de Certificats
UF	Utilisateur final
URL	“Uniform Resource Locator”

1.2 Présentation générale

L'infrastructure de gestion de la confiance de l'administration, dite IGC/A, est un ensemble de services de certification électronique opérés par la direction centrale de la sécurité des systèmes d'information (DCSSI), au sein du secrétariat général de la défense nationale (SGDN), service du Premier ministre.

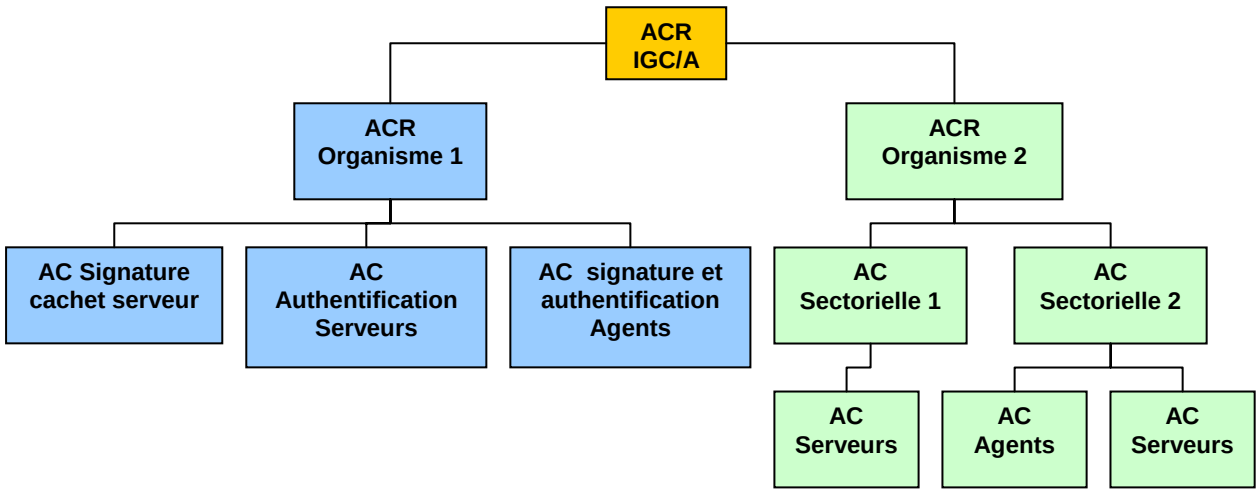
L'IGC/A participe à la validation par l'État français des certificats électroniques utilisés dans les échanges entre les usagers et les autorités administratives et entre les autorités administratives (AA). L'objectif de cette validation est de mettre à disposition des usagers de systèmes d'information les éléments permettant de s'assurer de l'origine des certificats électroniques utilisés par les AA et leurs agents. A cette fin l'IGC/A délivre des certificats aux autorités de certification racine (ACR) qui répondent aux conditions définies par la présente politique de certification (PC) et par les décrets d'application relatifs à l'article 10 de l'ordonnance [ORD05-1516]. Elle instaure ainsi un domaine de confiance de l'administration française, qui facilite la mise en relation des infrastructures de gestion de clés (IGC) des AA et la diffusion des certificats utilisés par de nombreuses applications, en particulier les télé-services.

Les clés cryptographiques certifiées par l'ACR de l'IGC/A sont générées et initialement certifiées par les ACR demandeuses. Celles-ci organisent selon leurs besoins la délégation de leurs services de certification à des autorités de certification (AC) subalternes, pour délivrer des certificats d'authentification, de signature ou de chiffrement à des utilisateurs finaux qui peuvent être des personnes physiques ou morales ou des machines[1].

La validation d'un certificat d'utilisateur final ou d'une AC, nécessite la validation du certificat de l'AC qui a émis ce certificat. Les mécanismes de vérification[2] sont récurrents et s'arrêtent lorsque le certificat analysé est celui d'une AC connue et de confiance. C'est le cas des certificats de l'ACR de l'IGC/A, qui ont vocation à être intégrés dans les logiciels de communication installés sur les ordinateurs des usagers et des administrations, et sont officiellement publiés au journal officiel de la République française.

Ainsi les chaînes de certification servant à la validation des certificats aboutissent à un même certificat d'ACR centrale, l'ACR de l'IGC/A.

Exemple d'organisation des autorités de certification racines autour de l'ACR de l'IGC/A



[1] Voir les domaines d'utilisation autorisés et interdits au chapitre 1.5 Usage des certificats.
[2] Définis notamment par le standard [RFC5280].

La présente PC définit les objectifs de sécurité pour le processus de certification de l'IGC/A. Elle expose les règles de gestion et d'utilisation qui s'imposent tant à l'ACR de l'IGC/A qu'aux ACR certifiées par l'IGC/A.

Cette version 2.0 régit l'usage des certificats délivrés dans le cadre d'une nouvelle phase du projet IGC/A initié en 2001. Cette « phase 2 » est caractérisée par un audit préalable et systématique des ACR souhaitant obtenir un certificat électronique de l'IGC/A, et par la capacité de révoquer les certificats émis. Elle s'accompagne également d'un nouveau corpus documentaire, qui compte plusieurs guides à l'attention des autorités administratives, pour les aider à constituer la documentation réglementaire de leur IGC et à en évaluer elles-mêmes la sécurité.

Le plan de cette PC suit les recommandations du document [RFC3647], et tire également parti des PC-types de la politique de référencement intersectorielle de sécurité v2.0 [PRIS].

1.3 Identification de la PC

L'identifiant d'objet unique – ou « OID » - de la présente PC de l'IGC/A défini par la DCSSI, à laquelle l'AFNOR a attribué la racine d'identifiant OID 1.2.250.1.121, est le suivant :

- OID : 1.2.250.1.121.1.1.2.

1.4 Acteurs et utilisateurs concernés par l'IGC/A

1.4.1 Les autorités de l'IGC/A

Les autorités administratives

Le code de la défense, modifié par le décret [DEC07-584], stipule que :

« Le Premier ministre assure la mise en œuvre par le Gouvernement des décisions prises en application des dispositions des articles L. 1111-3, L. 1121-1 et L. 1121-2 et dispose, à cette fin, du secrétariat général de la défense nationale. »

« Dans le cadre de la politique définie par le Gouvernement, le secrétaire général de la défense nationale veille à la cohérence des actions entreprises en matière de sécurité des systèmes d'information. »

Le décret [DEC2001-693] précise :

« Article 1 - Il est créé une direction centrale de la sécurité des systèmes d'information, placée sous l'autorité du secrétaire général de la défense nationale et chargée de l'assister dans l'exercice des compétences qui lui sont conférées […]. »

« Article 2 - La direction centrale de la sécurité des systèmes d'information apporte son concours aux services de l'État, dans le domaine défini par l'article 1er, et assure la cohérence du cadre juridique de leur action. »

Enfin, l'article 6 de l'instruction générale interministérielle [IGI1300] relatif aux attributions du SGDN précise :

*« Dans le cadre des accords de sécurité internationaux, il assure les fonctions d'**autorité nationale de sécurité** (ANS) et, au titre de la coordination interministérielle, il est l'interlocuteur des ANS étrangères. »*

Par conséquent l'autorité administrative responsable de la mise en œuvre de l'IGC/A est le secrétaire général de la défense nationale. Il délègue la mise en œuvre au directeur central de la sécurité des systèmes d'information.

L'autorité de certification racine

L'ACR de l'IGC/A est garante de l'application des règles de gestion de l'IGC/A décrites dans le corpus documentaire qu'elle a validé, et dont elle confie la définition et l'exécution à ses services.

L'ACR de l'IGC/A est le directeur central de la sécurité des systèmes d'information.

L'ACR délègue à l'autorité d'enregistrement de l'IGC/A le traitement des dossiers de demandes de certification et de révocation.

L'autorité d'enregistrement

L'AE de l'IGC/A traite les demandes de certification et de révocation après en avoir vérifié la recevabilité ainsi que la complétude des dossiers. Elle commande la publication des modalités d'accès aux services de l'IGC/A. L'AE rend compte à l'ACR de l'IGC/A en cas de litige sur la recevabilité des demandes de certification, et systématiquement en cas de demande de révocation.

L'autorité d'enregistrement (AE) de l'IGC/A est le chef du bureau conseil de la DCSSI. Il s'appuie sur plusieurs agents de la DCSSI pour l'exécution de ses missions.

L'autorité d'homologation et la commission d'homologation

Le directeur central de la sécurité des systèmes d'information est l'autorité qui prononce l'homologation de l'IGC/A, sur l'avis de la commission d'homologation. Cette commission, présidée par le directeur adjoint de la DCSSI, est saisie à chaque modification fonctionnelle de la plate-forme IGC/A et chaque fois que l'évolution de l'état de l'art en cryptographie le nécessite. Elle est également saisie pour le renouvellement de l'homologation, cette décision étant prononcée généralement pour une durée de cinq ans. La commission se prononce sur la base d'un dossier d'homologation présentant le motif détaillé de la saisine et justifiant l'impact sur la sécurité de l'IGC/A.

1.4.2 Les autres acteurs de l'IGC/A

La déclaration des pratiques de certification (DPC) de l'IGC/A précise l'implication des différents bureaux de la DCSSI dans l'exécution, le développement et le maintien en conditions opérationnelles des services de l'IGC/A. Ces personnes agissent sous l'autorité de l'ACR de l'IGC/A.

Le mandataire de l'ACR

Le mandataire a pour rôle de représenter l'autorité de certification racine faisant l'objet de la demande de certificat. A ce titre il doit vérifier l'intégrité et l'authenticité des informations proposées à la signature par l'IGC/A, concernant son autorité de certification. Il doit également, tout comme les autres participants de la cérémonie, signaler tout incident ou anomalie qu'il constaterait, et attester du bon déroulement de la cérémonie. Le mandataire signe le registre de cérémonie ; par cet acte il notifie l'acceptation officielle du certificat émis pour l'autorité de certification racine qu'il représente. Le mandataire est invité à respecter les consignes régissant le bon déroulement de la cérémonie, et s'engage à ne divulguer aucune des informations à diffusion restreinte ou confidentielles dont il aurait eu connaissance au cours de la cérémonie.

L'autorité chargée de la SSI

Cette autorité mandatée par l'AA pour assurer la sécurité de ses systèmes d'information, est impliquée dans les demandes de certification et de révocation, en tant qu'interlocuteur naturel et privilégié de la DCSSI.

Pour une ACR gouvernementale, cette autorité peut être le haut fonctionnaire de défense et de sécurité (HFD ou HFDS), ou le fonctionnaire de sécurité des systèmes d'information (FSSI) de l'AA que représente l'ACR.

1.4.3 Les porteurs de certificats délivrés par l'IGC/A

Les porteurs de certificats IGC/A : les autorités de certification racines

Une ACR est le porteur des certificats qui lui sont délivrés par l'IGC/A, dans le sens où ces certificats attestent que la bi-clé cryptographique qu'elle utilise pour signer les certificats qu'elle délivre elle-même est de confiance, principalement parce que :

- la bi-clé est en la possession exclusive de l'ACR dûment identifiée, et le reste grâce aux bonnes pratiques de certification de l'ACR, vérifiées régulièrement ;
- les éléments cryptographiques utilisés par l'ACR sont potentiellement à l'état de l'art pour la durée de validité du certificat, ou bien les conditions de leur utilisation sont de nature à limiter les risques induits par les progrès de la cryptographie.

Les ACR pouvant être porteuses d'un certificat délivré par l'IGC/A sont distinguées selon la nature de l'autorité administrative qu'elles représentent[3] :

- ACR gouvernementale ;
- ACR AAI ;
- ACR territoriale ;
- ACR EPCA ;
- ACR RPS ;
- ACR SPA.

Nota : Cette liste est susceptible d'évoluer avec les décrets d'application de l'ordonnance [ORD05-1516].

ATTENTION : La présente PC ne concerne que les ACR gouvernementales. Les conditions s'appliquant aux autres ACR seront définies dans une version ultérieure de la PC.

ACR gouvernementales

Les règles suivantes s'appliquent aux ACR gouvernementales concernées par la présente PC :

- l'ACR doit être le représentant officiel d'une administration de l'État français ;
- l'ACR doit fédérer toutes les AC de l'autorité administrative concernée ; dans le cas contraire, l'accord du haut fonctionnaire de défense et de sécurité (HFD ou HFDS), ou du fonctionnaire de sécurité des systèmes d'information (FSSI) de l'autorité administrative est un pré-requis à sa demande de certification par l'IGC/A ;
- l'ACR doit disposer d'une bi-clé de signature de certificats d'AC et de listes de certificats d'autorités révoqués certifiée par l'ACR elle-même (certificat auto-signé) ;
- l'ACR doit être capable de réaliser un audit de la sécurité de son IGC et d'autoriser l'ACR de l'IGC/A à contrôler ou faire contrôler la conformité de ses pratiques au [guide_audit_ACR].

1.4.4 Les utilisateurs des certificats de l'IGC/A

Les certificats délivrés par l'IGC/A sont librement utilisables à des fins de vérification de l'origine d'un certificat d'utilisateur final ou d'AC.

[3] se reporter au titre 1.1 Définitions et acronymes pour la signification de ces termes.

Cas particulier d'utilisateurs de certificats : les éditeurs de produits de communication

Les éditeurs de produits de communications qui souhaitent intégrer les certificats racine de l'IGC/A sont invités à se reporter à l'ANNEXE 6 : modalités de vérification des certificats de l'IGC/A et conditions de leur intégration dans les produits de communication de la présente PC.

1.5 Usage des certificats

1.5.1 Domaine d'utilisation applicable

L'IGC/A délivre exclusivement des certificats de signature de certificats et de listes de révocation pour les ACR définies au §1.4.3.

La présente PC ne s'applique qu'à la certification des ACR gouvernementales.

Une condition pour la délivrance d'un certificat par l'IGC/A et son maintien est que toutes les AC subalternes à l'ACR gouvernementale appartiennent à une autorité administrative (AA) au sens de l'ordonnance tel qu'indiqué au §1.1.1.Ces AC subalternes doivent donc appartenir à l'AA à laquelle appartient l'ACR ou à une autre AA.

En conséquence, une AC n'appartenant pas à une autorité administrative ne peut pas faire partie d'une chaîne de confiance certifiée par l'IGC/A.

Toute dérogation à ces règles ne peut être prononcée que par l'ACR de l'IGC/A.

Nota : L'ACR de l'IGC/A se réserve le droit de limiter la longueur du chemin de confiance entre l'ACR et les certificats des usagers, c'est-à-dire le nombre d'AC constituant la chaîne de certification sous le certificat de l'ACR de l'IGC/A.

La PC des ACR gouvernementales et les PC des AC subalternes doivent limiter la délivrance de leurs certificats :

- à des AC sous la responsabilité d'une ou plusieurs autorités administratives ;
- à des personnes physiques, dans le domaine de compétence de l'autorité administrative ;
- à des machines pour l'authentification et le cachet-serveur qui sont sous la responsabilité exclusive d'une autorité administrative ;
- à des autorités administratives pour la signature de codes.

Les certificats délivrés par l'IGC/A peuvent être utilisés à des fins de validation de la chaîne de confiance constituée par l'ensemble des certificats des AC entre le certificat de l'ACR de l'IGC/A et le certificat d'un utilisateur final (de tout type à l'exception d'une AC). On s'assure ainsi que ne sont pas compromises les fonctions de sécurité (signature, authentification, chiffrement) pour lesquelles est utilisée la bi-clé associée au certificat de cet utilisateur final.

1.5.2 Limites de responsabilité

L'AA de l'IGC/A ne saurait être tenue pour responsable d'une mauvaise utilisation du certificat de l'ACR, ou de tout certificat émanant de l'IGC opérée par l'ACR (ou d'une IGC opérée par l'une de ses AC déléguées).

Les AA dont l'ACR a été certifiées par l'IGC/A portent seules la responsabilité de l'application de leurs propres politiques de certification dans leur organisation.

1.6 Gestion de la PC

1.6.1 Entité gérant la PC

La rédaction de la PC et de ses évolutions est confiée par l'ACR de l'IGC/A au bureau conseil de la DCSSI.

Les versions traduites en langues étrangères sont des traductions de courtoisie à l'amélioration desquelles les lecteurs peuvent contribuer en s'adressant au point de contact indiqué au paragraphe suivant.

1.6.2 Point de contact

Personnes à contacter concernant ce document :

SGDN/DCSSI/BCS

51 bd la Tour Maubourg

75700 PARIS – 07 SP

Courriel : igca@sgdn.gouv.fr.

1.6.3 Entité déterminant la conformité du corpus documentaire de l'IGC

Concernant l'IGC/A

L'ACR de l'IGC/A approuve la PC de l'IGC/A, sur la base d'une étude de conformité au [guide_audit_ACR] qu'elle confie à ses services compétents, et éventuellement d'un avis d'un cabinet externe.

La conformité de la DPC à la PC est définie de la même manière.

Concernant les ACR gouvernementales

L'ACR doit préciser dans sa PC qui définit la conformité de sa DPC avec sa PC.
La conformité du corpus documentaire de l'ACR avec les exigences de l'IGC/A est vérifiée par la DCSSI.

1.6.4 Procédures d'approbation de la conformité du corpus documentaire de l'IGC

Concernant l'IGC/A

La PC est présentée pour relecture et avis à la commission d'homologation de l'IGC/A. La commission d'homologation formalise son avis et en demande les corrections éventuelles. Lorsque la PC reçoit un avis favorable de la commission d'homologation, la PC est soumise à la validation de l'ACR de l'IGC/A. L'ACR peut demander des modifications avant d'approuver la PC et de lui attribuer une référence officielle.

Un contrôle de conformité du corpus documentaire est réalisé de manière systématique après chaque modification majeure de la PC, et régulièrement suivant la fréquence [F_CONFORM].

Concernant les ACR gouvernementales

L'IGC de l'ACR gouvernementale est soumise à un audit de conformité, mandaté par l'ACR de l'IGC/A, avant sa certification par l'IGC/A puis suivant la fréquence [F_CONFORM] à partir de la date de délivrance du certificat. Cet audit vérifie la conformité de la PC de l'ACR au [guide_audit_ACR] et à la présente PC. La cohérence de la DPC par rapport aux objectifs définis dans la PC est également vérifiée.

2 Responsabilités concernant la mise à disposition des informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

Les informations énumérées dans le §2.2 sont mises à disposition des différentes catégories de lecteurs par le service de publication (SP) de l'IGC/A.

L'AE de l'IGC/A peut être contactée pour des demandes spécifiques ou pour un complément d'information sur les documents publiés. En particulier l'AE est le point de contact pour la diffusion du certificat d'IGC/A via des media hors du contrôle de l'ACR de l'IGC/A.

Les certificats sont remis en mains propres aux représentants des ACR à l'issue des cérémonies de signature.

Enfin, les ACR ayant obtenu un certificat de l'IGC/A doivent publier mensuellement une copie de la liste de certificats d'autorités révoqués, au point de distribution mentionné dans leur certificat, avant le 5 de chaque mois.

2.2 Informations devant être publiées

Les informations suivantes concernant l'IGC/A sont publiées par le SP de l'IGC/A :

Information	Moyen de diffusion
la PC de l'IGC/A	Site www.ssi.gouv.fr/fr/sigelec/igca/politique_certification.html Remise au mandataire de l'ACR lors de la cérémonie de signature du certificat par l'IGC/A.
les formulaires de demande de certification	Site www.ssi.gouv.fr/fr/sigelec/igca/
les formulaires de demande de révocation	Site www.ssi.gouv.fr/fr/sigelec/igca/ Sur demande auprès du bureau conseil de la DCSSI. En cas de révocation d'urgence, auprès de la cellule de veille de la DCSSI.
les certificats de l'ACR de l'IGC/A et leurs empreintes SHA-1	Site www.ssi.gouv.fr/fr/sigelec/igca/ Dans certains navigateurs Internet. Publiés au Journal officiel de la République française[4].
les empreintes MD5 des certificats de l'ACR de l'IGC/A	Sur demande auprès de l'AE de l'IGC/A.
la notice des conditions et modalités d'intégration des certificats de l'IGC/A dans les produits de communication	Site www.ssi.gouv.fr/fr/sigelec/igca/

[4] Les certificats des clés RSA et DSA de l'IGC/A en cours de validité ont été publiées dans l'Avis relatif aux certificats électroniques de l'autorité de certification racine de l'administration française, dits « certificats IGC/A » - NOR : PRMX0710016V, Journal officiel de la République française n° 41 du 17 février 2007.

la feuille de route de l'IGC/A	Sur demande auprès de l'AE de l'IGC/A.
les certificats d'ACR signés par l'IGC/A	L'ACR peut publier ses certificats selon les moyens qui conviennent à ses besoins. Le SP de l'IGC/A publie les certificats délivrés aux ACR gouvernementales sur au moins l'un des sites de l'ACR de l'IGC/A, www.ssi.gouv.fr/fr/sigelec/igca/, sauf mention contraire des ACR concernées.
les LAR de l'IGC/A	Site www.ssi.gouv.fr/fr/sigelec/igca/revocation/ Le point de distribution de la LAR de l'IGC/A indiqué dans le certificat remis à l'ACR, sera le point de distribution mentionné par l'ACR dans sa demande de certification
L'information de la publication d'une nouvelle LAR émise d'urgence	Site www.ssi.gouv.fr/fr/sigelec/igca/revocation/ Par courriel aux points de contact indiqués dans les formulaires de demande de certification des ACR

2.3 Délais et fréquences de publication

Les informations énumérées dans le §2.1 sont disponibles dans les meilleurs délais via le SP.

En particulier les listes de révocation sont publiées au début de chaque mois, sauf nouvelle entrée dans la liste de révocation qui justifie d'une publication en urgence.

2.4 Contrôle d'accès aux informations publiées

L'accès aux informations définies au §2.2 est libre.

3 Identification et authentification

3.1 Nommage

3.1.1 Convention de noms

Dans chaque certificat, l'émetteur et le sujet sont identifiés par un nom distinctif (champ Distinguished Name ou DN).

Le DN de l'IGC/A est indiqué en ANNEXE 5 : Format des certificats et des LAR.

Le DN de l'ACR est par défaut celui contenu dans le certificat auto-signé produit par l'ACR en accompagnement de sa demande de certification. Son format doit correspondre à celui décrit en ANNEXE 5 : Format des certificats et des LAR.

3.1.2 Utilisation de noms explicites

L'identité des ACR portée dans les certificats délivrés par l'IGC/A doit permettre aux UC de les identifier sans ambiguïté.

Il est possible d'utiliser des acronymes dès lors qu'ils sont officiels et largement diffusés.

Pour les ACR gouvernementales, il est préconisé que le nom commun employé soit pérenne, du type « administration en charge de … ». De cette façon, quels que soient les changements de nom des ministères, le nom commun reste valide.

Le service de publication de l'IGC/A peut permettre aux UC de vérifier les informations constituant le nom distinctif d'une ACR gouvernementale ; à cette fin il peut par exemple publier un tableau de correspondance entre les acronymes et dénominations officiels des ministères et les certificats concernés.

Cette mesure permet de considérer comme valide un certificat délivré à une autorité administrative dont le nom distinctif comporte des noms d'organisations devenus obsolètes (suite à un remaniement ministériel par exemple) mais dont les activités et les engagements de responsabilités perdurent. Elle répond à un besoin de continuité de service et de maîtrise des dépenses publiques, en garantissant aux utilisateurs la confiance qui peut être accordée dans le certificat délivré.

3.1.3 Anonymisation ou pseudo-anonymisation des porteurs

L'identité utilisée pour les certificats de l'IGC/A et des ACR doit être explicite et ne peut en aucun cas être anonyme ou un pseudonyme.

3.1.4 Règles d'interprétation des différentes formes de nom

Les noms utilisés dans un certificat doivent être décrits selon le standard [X500].

3.1.5 Unicité des noms

L'AE de l'IGC/A veille à l'unicité des noms distinctifs des ACR objets des certificats délivrés par l'IGC/A.

Les acronymes étant autorisés, il peut y avoir des noms communs identiques pour des ACR différentes, mais il y a obligatoirement des champs du nom distinctif qui diffèrent, principalement ceux des organisations (O, OU). Si ce n'était pas le cas, l'ACR de l'IGC/A ne donnerait pas suite en l'état à la demande de certification qui soulève le problème.

Par ailleurs, une même ACR peut disposer de plusieurs certificats pour des bi-clés différentes, portant des noms différents identifiant sans ambiguïté l'ACR.

3.1.6 Identification, authentification et rôle des marques déposées

L'ACR de l'IGC/A peut refuser la délivrance d'un certificat à une ACR dont le nom ne serait pas conforme aux exigences de la présente PC ou utiliserait une marque déposée.

L'AE de l'IGC/A veille à ce que l'usage d'un acronyme par l'autorité demandeuse soit légitime ; en cas d'ambiguïté l'ACR de l'IGC/A peut proscrire l'usage de l'acronyme dans ce cas précis.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

L'ACR de l'IGC/A s'assure que l'ACR gouvernementale possède la clé privée correspondant à la clé publique à certifier lors de la demande de certification.

La preuve de la possession de la clé privée repose sur plusieurs mesures :

- la vérification de la signature numérique du certificat auto-signé ou de la requête de certification transmis par le demandeur ;
- l'indication par le demandeur, dans sa demande de certification, de l'empreinte numérique du certificat auto-signé, ou à défaut de la clé publique (au format précisé dans le formulaire de demande) ;
- la vérification par l'AE de l'IGC/A de l'identité du demandeur et de son habilitation, par une autorité administrative connue, à effectuer cette demande.

3.2.2 Validation de l'identité de l'autorité administrative

Une ACR faisant une demande de certification doit pouvoir être identifiée de façon unique et non ambiguë par l'AE de l'IGC/A.

Le formulaire de demande de certification doit être complété des renseignements permettant d'identifier l'AA dont dépend l'ACR (nom, adresse). L'AE de l'IGC/A vérifie que l'AA est bien une autorité administrative entrant dans le cadre d'application de cette PC. Si les informations transmises à l'AE sont incomplètes ou insuffisantes pour identifier l'AA, l'AE peut demander un complément d'information au demandeur (par exemple les références d'un décret précisant la mission de service public ou le ministère de tutelle de l'AA, l'annuaire de l'Administration française, etc.), ou contacter un tiers de confiance capable d'identifier l'AA (par exemple le HFD ou HFDS du ministère de tutelle).

Pour chaque catégorie d'AA définie au §1.1.1, la procédure de validation de l'identité doit être conforme aux décrets et arrêtés pris pour application de l'ordonnance [ORD05-1516].

3.2.3 Validation de l'identité de l'autorité de certification racine

Une ACR faisant une demande de certification doit pouvoir être identifiée de façon unique et non ambiguë par l'AE de l'IGC/A.

Le formulaire de demande de certification doit être complété des renseignements permettant d'identifier l'ACR (nom, adresse). L'AE de l'IGC/A vérifie que l'ACR est bien mandatée par l'AA qu'elle représente, au besoin en contactant l'AA ou un tiers de confiance capable d'identifier l'ACR (par exemple le HFD ou HFDS du ministère de tutelle).

3.2.4 Validation de l'identité du demandeur, du mandataire ou d'un témoin

L'identité d'un individu, chaque fois qu'elle doit être connue, doit être unique et non ambiguë.

Dans le cas d'une cérémonie, l'identification du mandataire et des témoins de l'ACR s'effectue par rapport facial auprès du responsable sécurité de l'IGC/A, en produisant un titre d'identité délivré ou reconnu par l'Administration française.

Dans le cas de l'identification du demandeur d'un certificat ou d'une révocation, l'AE de l'IGC/A, si elle ne connaît pas le demandeur, peut exiger de celui-ci de fournir, en complément de son dossier de demande, la copie d'un titre d'identité délivré ou reconnu par l'Administration française.

L'AE de l'IGC/A peut également contacter le FSSI de l'organisme, ou tout membre de la chaîne fonctionnelle de sécurité des systèmes d'information désigné par elle pour vérification.

En cas de crise justifiant la révocation d'urgence d'un certificat d'ACR, l'identification des individus impliqués dans la demande de révocation est réalisée selon les procédures du COSSI.

3.2.5 Informations non vérifiées de l'ACR porteuse du certificat

Les informations demandées sont vérifiées par l'AE de l'IGC/A.

3.2.6 Validation de l'autorité du demandeur

Le signataire d'une demande de certification ou de révocation doit être autorisé par l'AA qu'il représente à effectuer cette demande. Il doit apporter à l'AE de l'IGC/A toute information qu'elle jugerait nécessaire pour en être assurée.

Pour valider l'autorité du demandeur d'un certificat ou d'une révocation, l'AE de l'IGC/A peut exiger de celui-ci de fournir, en complément de son dossier de demande, la référence du Journal officiel de la République française publiant ses fonctions, ou tout autre justificatif officiel apte à identifier le demandeur et à établir sa compétence à faire la demande.

L'AE de l'IGC/A peut contacter le FSSI, le HFD ou le HFDS d'un ministère compétent pour s'assurer de l'autorité du demandeur auprès de l'AA concernée par la demande.

3.2.7 Critères d'interopérabilité

L'ACR de l'IGC/A doit être informée des accords de reconnaissance avec d'autres AC qu'une ACR a passés ou souhaiterait passer. Si ces accords sont de nature à perturber l'interopérabilité des ACR certifiées par l'IGC/A, ou à étendre l'usage des certificats à un domaine d'application interdit, l'ACR de l'IGC/A se réserve le droit de révoquer le ou les certificats délivrés à cette ACR, conformément au §4.8.3.

La demande de modification d'un certificat suit les mêmes conditions que celles portées au §4.1.

3.3 Identification et validation d'une demande de renouvellement d'une bi-clé

L'ACR de l'IGC/A ne délivre pas de bi-clé. Ce chapitre est donc sans objet.

3.4 Identification et validation d'une demande de révocation

Le formulaire de demande de révocation comporte des informations qui sont mises en corrélation avec la demande de certification initiale, et selon la cause de la révocation, avec le plan de crise de l'ACR qui a été communiqué à l'ACR de l'IGC/A. Ces informations sont connues d'un cercle restreint d'agents ayant besoin d'en connaître (demandeur, ACR, FSSI, AE de l'IGC/A et ses opérateurs, ACR de l'IGC/A, COSSI de la DCSSI) ; ceci réduit le risque d'une demande de révocation frauduleuse.

Si la demande de révocation est due à une compromission ou suspicion de compromission des clés privées, à la perte ou le vol d'éléments permettant sa reconstitution, alors la procédure d'identification suivie est celle décrite dans le plan de crise de l'ACR reprenant les préconisations du COSSI de la DCSSI. Ce dernier vérifie le respect de la procédure et rend compte à l'AE de l'IGC/A sur l'origine de la demande.

Dans le cas où la demande de révocation émane de l'ACR de l'IGC/A, alors cette demande est envoyée pour information à l'ACR concernée et pour action à l'AE de l'IGC/A.

Dans tous les cas c'est l'AE de l'IGC/A qui effectue l'identification du demandeur et valide la demande afin d'organiser une cérémonie de signature de listes de révocation dans les délais appropriés au regard de la cause de la révocation, cf §4.9.3.

4 Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande

Une demande de certificat n'est recevable par l'ACR de l'IGC/A que si toutes les conditions suivantes sont remplies :

- la demande concerne une ACR répondant aux caractéristiques définies au §1.4.3 ;
- elle est signée par une autorité pouvant justifier de sa compétence à effectuer cette demande, vérifiable par l'AE de l'IGC/A conformément au chapitre 3 ;
- le formulaire contient tous les renseignements techniques et administratifs demandés ;
- l'ACR concernée peut justifier que ses pratiques sont conformes aux exigences qui la concernent dans cette présente PC et dans le [guide_rédaction_ACR].

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

Les formulaires de demande sont disponibles sur le site de la DCSSI.

L'ACR doit renseigner sa demande en vérifiant sa conformité au §4.1.1.

Pour les ACR gouvernementales, la vérification de la conformité aux exigences de la présente PC et du [guide_rédaction_ACR] est réalisée par l'AE de l'IGC/A.

Si une demande est jugée irrecevable, le refus et son motif sont signifiés par l'AE de l'IGC/A ou l'organisme ayant effectué la vérification du dossier dans un délai maximum [T_MAX_ACR].

Si la demande est recevable, les conclusions de la vérification et les éléments techniques permettant la génération du certificat sont transmis à l'ACR de l'IGC/A. Celle-ci est libre d'accepter ou de refuser la demande de certificat au regard des éléments qui lui sont transmis, en particulier si les conclusions d'audit font apparaître des risques inacceptables pour l'ACR de l'IGC/A.

L'ACR de l'IGC/A peut accepter une demande de certificat sous réserve de la mise en œuvre de mesures contrant des risques identifiés comme non critiques. Dans ce cas l'ACR demandeuse et l'AA concernée sont responsables de l'application de mesures correctives, et des éventuels préjudices causés par la non application de ces mesures.

Les ACR demandeuses sont seules responsables de la gestion et de la protection de leurs clés puisque l'IGC/A ne délivre aucune bi-clé, mais seulement des certificats électroniques. Les signataires des dossiers de demande de certificats ont la responsabilité de l'exactitude des informations qui y sont portées.

Les informations et signatures requises pour constituer un dossier de demande ont pour objectif d'assurer à l'AA de l'IGC/A, que les autorités responsables de l'IGC concernées par la demande, et celles responsables de la sécurité des systèmes d'information de l'AA concernée, sont informées de la demande et des obligations qui incombent aux différentes parties dans la présente PC.

4.2 Traitement d'une demande

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

Processus adapté aux ACR gouvernementales

Les ACR gouvernementales adressent directement leur dossier de demande à l'AE de l'IGC/A.

L'AE de l'IGC/A accuse réception de l'envoi au demandeur indiqué dans le formulaire. Cet accusé de réception ne préjuge nullement de la recevabilité de la demande.

L'AE vérifie que la demande est complète et répond aux critères définis au §4.1.1 à l'exception de la conformité des pratiques aux exigences de l'IGC/A.

L'AE informe alors par messagerie électronique le demandeur de la prise en compte de sa demande, ou de son rejet en précisant le motif de rejet.

Si la demande est prise en compte, l'AE se met en rapport avec les points de contact techniques de l'ACR demandeuse afin de leur transmettre des certificats de tests et d'organiser l'audit de cette ACR.

L'ACR dispose d'un délai de [T_TESTS] pour réaliser ses simulations et faire part à l'AE d'éventuels problèmes rencontrés. Passé ce délai, sans remarque de la part de l'ACR, le format du certificat de test est considéré comme valide et sert de modèle au certificat final. L'ACR peut demander à l'AE de l'IGC/A la modification de ce délai.

Parallèlement, l'AE définit avec l'ACR les modalités de communication des informations nécessaires à l'audit et, si nécessaire, planifie une visite du site d'exploitation de l'IGC de l'ACR.

L'AE de l'IGC/A s'efforcera d'accuser réception des demandes dans un délai [T_MAX_AE].

4.2.2 Acceptation ou rejet de la demande

La demande est rejetée :

- si l'organisme faisant la demande n'entre pas dans le champ d'application de la présente PC ;
- si les signataires de la demande ne sont pas habilités à la faire ;
- si les éléments transmis sont incomplets concernant l'identification des points de contacts et les signatures d'autorités requises ;
- si l'ACR n'est pas conforme aux exigences de la présente PC et au [guide_rédaction_ACR].

Cette conformité est vérifiée :

- soit sur la base des conclusions et réserves du rapport d'audit de conformité à [guide_rédaction_ACR] selon le [guide_audit_ACR], réalisé dans un délai inférieur à [F_CONFORM] précédant la demande, par un organisme habilité ; si elle le juge utile, l'AE de l'IGC/A peut procéder à une visite de conformité complémentaire ;
- soit par un audit de conformité à [guide_rédaction_ACR] selon le [guide_audit_ACR] réalisé par l'AE de l'IGC/A ou l'organisme compétent chargé de la vérification de la recevabilité de la demande de certificat.

La demande peut être rejetée par l'AE de l'IGC/A s'il ne lui est pas possible de mener les travaux d'audit dans un délai de [T_Max_Audit]. Dans ce cas elle en informe l'ACR dans les meilleurs délais.

L'avis des auditeurs est transmis à l'ACR de l'IGC/A, qui décide d'accepter ou de refuser la demande au regard des conclusions du rapport. Il informe également l'AE de ses conclusions.

L'AE envoie alors au demandeur un courrier signé de l'ACR de l'IGC/A notifiant son refus ou son accord, avec, encas d'accord, la date retenue pour la cérémonie de signature du certificat.

4.2.3 Délai de traitement de la demande de certification

Le délai de traitement est variable car il dépend essentiellement du travail à réaliser pour vérifier la recevabilité de la demande, principalement l'audit et les tests préliminaires.

Le délai maximum est défini par :

T_MAX_DEMANDE = T_MAX_AE + MAX(T_MAX_AUDIT ;T_TESTS) + T_MAX_ACR

4.3 Délivrance du certificat

4.3.1 Actions de l'ACR de l'IGC/A

L'AE de l'IGC/A transmet à l'ACR de l'IGC/A les éléments techniques (certificat et script de cérémonie) nécessaires à la génération du certificat, selon un processus garantissant leur intégrité et leur origine et précisé dans la DPC.

L'ACR de l'IGC/A génère le certificat lors d'une cérémonie de signature en présence de l'ACR demandeuse ou d'une personne désignée par elle pour la représenter, appelée « mandataire », et de l'AE de l'IGC/A qui dispose du dossier de demande.

4.3.2 Actions de l'ACR demandeuse

L'ACR ou son mandataire doit vérifier la cohérence des informations portées dans la demande et celle portées dans le certificat généré pendant la cérémonie, et signaler toute anomalie constatée. A l'issue de la cérémonie, si aucune anomalie n'a été signalée sur le certificat, celui-ci est officiellement remis à l'ACR ou à son mandataire, sous la forme d'un fichier au format DER, sur un support amovible (cédérom ou clé USB).

4.4 Acceptation du certificat

4.4.1 Processus d'acceptation

L'AE de l'IGC/A transmet à l'ACR demandeuse des certificats de test avant la cérémonie de signature pour lui permettre de vérifier le format du certificat qui lui sera délivré, et d'en préparer le déploiement. Le format de certificat est considéré valide en l'absence d'indication contraire ou de demande de report de délai de la part de l'ACR avant l'expiration d'un délai de [T_TESTS].

L'ACR ou son mandataire acceptent formellement le certificat délivré lors de la cérémonie de signature en émargeant le registre de cérémonie. Aucune objection postérieure à la cérémonie ne pourra être reçue pour annuler l'acceptation du certificat.

4.4.2 Publication du certificat

Si l'ACR demandeuse n'a pas manifesté son opposition à la publication du certificat délivré par l'IGC/A, le SP de l'IGC/A publie ce nouveau certificat.

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

Dans le cas de la génération d'un nouveau certificat auto-signé de l'ACR de l'IGC/A, tous les services impliqués dans la réalisation des tests préliminaires, l'organisation des cérémonies, la publication, la maintenance des plates-formes sont informés.

Dans le cas de la génération d'un certificat d'ACR gouvernementale, le service de publication est le seul informé.

Une communication peut également être élaborée avec l'ACR de l'IGC/A pour informer les utilisateurs potentiels des certificats délivrés.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat de l'ACR de l'IGC/A

L'utilisation de la clé privée de l'ACR de IGC/A et du certificat associé est strictement limitée à la signature de certificats d'autorités de certification, à la signature de listes de certificats d'autorités révoqués, et à la non-répudiation (signature de fichiers échangés entre composantes de la plate-forme de certification IGC/A).

L'usage autorisé de la bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des clés (cf. annexe 5 : Format des certificats et des LAR).

Dès qu'une nouvelle clé privée est générée pour l'IGC/A, celle-ci peut être utilisée pour générer de nouveaux certificats d'ACR et des LAR avec une durée de vie maximale de [T_VALID_CERT].

La précédente clé privée peut servir encore à délivrer des certificats d'une durée de vite inférieure à [T_VALID_CERT] ; cet usage doit être motivé par une question d'interopérabilité ou une mesure d'urgence, et reste au choix de l'ACR de l'IGC/A qui tiendra compte de l'état de l'art en cryptologie.

Les certificats de l'ACR de l'IGC/A restent utilisables pour valider le chemin de certification des certificats signés des différentes clés privées de l'IGC/A, jusqu'à l'expiration de tous les certificats émis à l'aide de ces clés.

La responsabilité de l'AA de l'IGC/A ne peut être engagée qu'en cas de manquement à ses propres obligations ou à celles de l'ACR ou de l'AE de l'IGC/A.

La responsabilité de l'AA de l'IGC/A ne pourra valablement être mise en cause par une autre AA, si le préjudice subi par cette dernière résulte d'un manquement à l'une des obligations qui lui incombent dans la présente PC.

L'AA de l'IGC/A ne saurait être tenue pour responsable d'une mauvaise utilisation des certificats délivrés par l'IGC/A, ou de tout certificat délivré par une AC d'une chaîne de confiance certifiée par l'IGC/A.

4.5.2 Utilisation par une ACR de sa clé privée et du certificat délivré par l'IGC/A

L'utilisation de la clé privée de l'ACR doit être limitée à :

- la signature de certificats d'autorités de certification ;
- la signature de listes de certificats révoqués ;
- la signature de listes de certificats révoqués hors connexion.

Éventuellement, son usage pour la signature numérique ou la non-répudiation peut être autorisé, afin de sécuriser les échanges entre les composantes de l'IGC de l'ACR.

L'usage du certificat délivré par l'IGC/A est strictement limité par les règles définies au §1.5.

L'expiration ou la révocation d'un certificat délivré par l'IGC/A n'impose pas la fin de vie de la bi-clé de l'ACR.

Les AA dont dépendent les ACR certifiées par l'IGC/A sont seules responsables des préjudices causés par le non respect de leurs obligations telles que définies dans la présente PC. Elles portent seules la responsabilité de l'application de leurs propres politiques de certification dans leur organisation.

4.5.3 Utilisation de la clé publique et du certificat par l'UC

Les certificats délivrés par l'IGC/A ne peuvent être utilisés par un UC qu'à des fins de validation d'une chaîne de confiance entre le certificat de l'ACR de l'IGC/A et le certificat d'un utilisateur final ou d'une AC.

Il est de la seule responsabilité de l'UC de s'assurer de la validité des certificats délivrés par l'IGC/A, à l'aide des listes de certificats d'autorités révoquées publiées par le SP de l'IGC/A et diffusées par chacune des ACR certifiées.

4.6 Renouvellement d'un certificat

Nota :

La notion de « renouvellement de certificat » correspond à la délivrance d'un nouveau certificat pour lequel seuls les dates de validité et le numéro de série du certificat sont modifiés, toutes les autres informations restant identiques au certificat précédent, particulièrement la clé publique du porteur.

4.6.1 Causes possibles d'un renouvellement

La seule cause admise pour une demande de renouvellement est l'expiration du certificat délivré par l'IGC/A avant celle du certificat auto-signé de l'ACR gouvernementale.

Les certificats de l'ACR de l'IGC/A ne sont jamais renouvelés.

4.6.2 Origine d'une demande de renouvellement

L'origine d'une demande de renouvellement est la même que la demande initiale (cf. §4.1.1).

4.6.3 Procédure de traitement d'une demande de renouvellement

La procédure à suivre est identique à la procédure initiale de certification décrite aux §4.1, §4.2 et §4.3 ci-dessus. En particulier, l'audit préalable doit vérifier que la protection de la clé privée est toujours assurée, et que la même confiance peut lui être accordée malgré l'évolution de l'état de l'art en cryptographie.

4.6.4 Délivrance du nouveau certificat

La délivrance du nouveau certificat suit la démarche décrite au §4.3.

L'ACR de l'IGC/A n'a aucune obligation d'accepter la demande d'un nouveau certificat.

4.6.5 Acceptation du nouveau certificat

L'acceptation du nouveau certificat suit le processus décrit au §4.4.1.

4.6.6 Publication du nouveau certificat

La publication du nouveau certificat suit la démarche décrite au §4.4.2.

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

La notification du nouveau certificat suit la démarche décrite au §4.4.3.

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

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés doivent être renouvelées :

- pour suivre l'évolution de l'état de l'art en cryptographie, et en particulier les recommandations émises par la DCSSI ([R-ALGO] et [R-IGC]) afin de minimiser les possibilités d'attaques cryptographiques ;
- pour que l'ACR puisse continuer à délivrer des certificats d'AC d'une durée constante ;
- en cas de compromission, suspicion de compromission, vol ou perte des moyens de reconstitution de la clé privée de l'ACR.

Dans tous ces cas la délivrance d'un nouveau certificat par l'IGC/A est possible.

4.7.2 Origine d'une demande d'un nouveau certificat

La demande d'un nouveau certificat suit les mêmes conditions que celles portées au §4.1. Elle n'est pas obligatoire pour les ACR.

4.7.3 Traitement d'une demande

Le traitement d'une demande de certificat suite au changement d'une bi-clé est identique à celui décrit au §4.2.

4.7.4 Délivrance du nouveau certificat

La délivrance du nouveau certificat suit la démarche décrite au §4.3.

L'ACR de l'IGC/A n'a aucune obligation d'accepter la demande d'un nouveau certificat.

4.7.5 Acceptation du nouveau certificat

L'acceptation du nouveau certificat suit le processus décrit au §4.4.1.

4.7.6 Publication du nouveau certificat

La publication du nouveau certificat suit la démarche décrite au §4.4.2.

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

La notification du nouveau certificat suit la démarche décrite au §4.4.3.

4.8 Modification du certificat

Nota :

La modification d'un certificat correspond à la délivrance d'un nouveau certificat pour la même clé publique, consécutif à des modifications d'informations autres que uniquement les dates de validité et le numéro de série (dans le cas contraire il s'agit d'un renouvellement de certificat tel que décrit au §4.6).

4.8.1 Certificat de l'ACR de l'IGC/A

La modification des certificats de l'ACR de l'IGC/A est autorisée à condition qu'elle soit sans impact sur l'utilisation des certificats précédemment délivrés.

4.8.2 Causes possibles de la modification d'un certificat d'ACR

Une demande de modification d'un certificat peut être motivée par :

- le souci d'améliorer l'identification de l'ACR (changement de nom d'un ministère par exemple),
- le besoin d'une nouvelle information dans une extension répondant aux exigences de la [PRIS].

Le changement d'informations dans son nom distinctif (champ « DN ») ne contraint pas une ACR à demander la modification de son certificat dès lors que son identification est toujours possible sans ambiguïté.

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

La demande de modification d'un certificat suit les mêmes conditions que celles portées au §4.1.

4.8.4 Traitement d'une demande

Processus adapté aux ACR gouvernementales

Les ACR gouvernementales adressent directement leur dossier de demande à l'AE de l'IGC/A.

L'AE de l'IGC/A accuse réception de l'envoi au demandeur indiqué dans le formulaire. Cet accusé de réception ne préjuge nullement de la recevabilité de la demande.

L'AE vérifie que la demande est complète et répond aux critères définis au §4.1.1 à l'exception de la conformité des pratiques aux exigences de l'IGC/A.

L'AE informe alors par messagerie électronique le demandeur de la prise en compte de sa demande, ou de son rejet en précisant le motif de rejet.

Un rejet sera adressé si les modifications portées ne sont pas conformes aux règles concernant le format de certificat présentées au §7.1, et plus généralement aux exigences de la présente PC.

Si la demande est prise en compte, l'AE se met en rapport avec les points de contact techniques de l'ACR demandeuse afin de leur transmettre des certificats de tests.

L'ACR dispose d'un délai de [T_TESTS] pour réaliser ses simulations et faire part à l'AE d'éventuels problèmes rencontrés. Passé ce délai, sans remarque de la part de l'ACR, le format du certificat de test est considéré comme valide et sert de modèle au certificat final. L'ACR peut demander à l'AE de l'IGC/A la modification de ce délai.

L'AE de l'IGC/A s'efforcera d'accuser réception des demandes dans un délai [T_MAX_AE].

4.8.5 Délivrance du certificat modifié

La délivrance du certificat modifié suit la démarche décrite au §4.3.

L'ACR de l'IGC/A n'a aucune obligation d'accepter la demande de modification du certificat.

4.8.6 Acceptation du certificat modifié

L'acceptation du nouveau certificat suit le processus décrit au §4.4.1.

4.8.7 Publication du certificat modifié

La publication du nouveau certificat suit la démarche décrite au §4.4.2.

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

La notification du nouveau certificat suit la démarche décrite au §4.4.3.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

Pour l'ACR de l'IGC/A, les causes de révocation sont les suivantes :

- cessation d'activité de l'ACR ;
- fin anticipée de l'usage de la bi-clé ;
- compromission, suspicion de compromission, vol ou perte des moyens de reconstitution de la clé privée de l'ACR ;
- obsolescence d'informations d'identification contenues dans le certificat de l'ACR de l'IGC/A, dès lors que ces informations, si elles ne sont pas modifiées, empêchent l'identification de l'ACR.

Pour l'ACR gouvernementale, les causes de révocation sont les suivantes :

- cessation d'activité de l'ACR gouvernementale, ou modification de son statut incompatible avec les exigences du §1.4.3 ;
- fin anticipée de l'usage de la bi-clé ;
- compromission, suspicion de compromission, vol ou perte des moyens de reconstitution de la clé privée de l'ACR gouvernementale ;
- décision suite à une non-conformité révélée lors d'un contrôle de conformité ;
- non-respect de la PC de l'IGC/A par l'ACR gouvernementale – cette cause n'entraîne pas obligatoirement la révocation du certificat ;
- obsolescence d'informations d'identification contenues dans le certificat de l'ACR gouvernementale, dès lors que ces informations, si elles ne sont pas modifiées, empêchent l'identification de l'ACR.

Un certificat peut également être révoqué s'il n'est plus utilisé par l'ACR gouvernementale.

4.9.2 Origine d'une demande de révocation

Pour les certificats de l'ACR de l'IGC/A, seule l'AA de l'IGC/A peut décider de leur révocation.

Pour les certificats délivrés par l'IGC/A à une ACR, l'autorité pouvant décider de la révocation dépendra du motif de cette révocation :

Motif	Autorité habilitée à établir la demande de révocation
Cessation d'activité de l'ACR ou modification de son statut	L'ACR elle-même, ou si elle est dans l'incapacité de le faire, l'ACR de l'IGC/A.
Fin anticipée de l'usage de la bi-clé	L'ACR.

Compromission, suspicion de compromission, vol ou perte des moyens de reconstitution de la clé privée de l'ACR	L'ACR et L'AA ou l'ACR de l'IGC/A.
Non-conformité révélée lors d'un contrôle de conformité	L'ACR elle-même, ou l'ACR de l'IGC/A après information de l'ACR en cas de non-conformité susceptible de nuire à la confiance accordée aux certificats délivrés par l'IGC/A.
Non-respect de la PC de l'IGC/A par l'ACR	L'ACR elle-même, ou l'ACR de l'IGC/A après information de l'ACR en cas de non-conformité susceptible de nuire à la confiance accordée aux certificats délivrés par l'IGC/A.
Obsolescence d'informations d'identification contenues dans le certificat de l'ACR	L'ACR elle-même, ou l'ACR de l'IGC/A après information de l'ACR en cas de non-conformité majeure susceptible de nuire à la confiance accordée aux certificats délivrés par l'IGC/A.
(Facultatif) Certificat non-employé	L'ACR.

4.9.3 Procédure de traitement d'une demande de révocation

Nota :

Les procédures détaillées de demande et traitement des révocations sont des informations sensibles qui ne sont divulguées qu'aux ACR auxquelles l'IGC/A délivre un ou plusieurs certificats.

Objectif de la procédure de révocation d'un certificat de l'ACR de l'IGC/A, motivée par une compromission ou suspicion de compromission des clés de l'ACR de l'IGC/A :

- Protéger : appliquer sans délais les mesures adaptées pour éviter toute nouvelle compromission des bi-clés (cf DPC).
- Alerter : informer le plus rapidement possible les utilisateurs impactés, pour leur permettre d'appliquer leur plan d'urgence sans délais.
- Secourir : limiter la propagation d'une compromission et son impact, en mettant en œuvre les parades le plus vite possible ; remettre en service une autre AC pour rétablir les services de l'IGC/A pour toutes les IGC des autorités administratives concernées.

Nota :

Une fois que le certificat est révoqué, il ne peut pas être réutilisé. La révocation est définitive, cependant si la cause de la révocation n'est pas une compromission, suspicion de compromission, vol ou perte des moyens de reconstitution de la clé privée de l'ACR de l'IGC/A, la même clé publique peut être de nouveau certifiée (exemple : révocation suite à un changement de l'identifiant de l'ACR de l'IGC/A). De plus, la révocation s'effectue sous un délai donné (cf. §4.4.4).

Après la révocation du certificat de l'IGC/A, la génération de nouvelles clés sera ou non obligatoire, selon la cause de la révocation, et sur décision de l'AA de l'IGC/A.

Objectif de la procédure de révocation d'un certificat d'ACR :

- Garder intègre le domaine de confiance de l'IGC/A.
- Accompagner l'ACR dans sa parade et la remise en service de son IGC.

Nota :

Une fois que le certificat est révoqué, il ne peut être réutilisé. La révocation est définitive, cependant en fonction des cas de révocation la même clé publique de l'AC peut être de nouveau certifiée (exemple : révocation suite à un changement de l'identifiant de l'AC).De plus la révocation s'effectue sous un délai donné (cf. §4.4.4).

Après la révocation du certificat d'une ACR gouvernementale, la génération de nouvelles clés sera ou non obligatoire, selon la cause de la révocation, et sur décision de l'ACR gouvernementale. L'ACR de l'IGC/A se réserve le droit de ne pas donner de suite favorable à la demande de certification pour cette nouvelle bi-clé, si les conditions de sécurité de l'IGC lui semblent être insuffisantes au regard de l'événement ayant entraîné la révocation.

4.9.4 Délai accordé pour formuler la demande de révocation

Dans le cas d'une compromission ou d'une suspicion de compromission de clé privée, une ACR gouvernementale, tout comme l'ACR de l'IGC/A s'il s'agit d'une de ses bi-clés, doit communiquer la demande dans un délai maximum de [T_INFO_CRISE] après la découverte de la compromission ou suspicion de compromission.

Dans les autres cas motivant une demande de révocation, qui ne justifient pas une publication urgente d'une nouvelle LAR, l'ACR gouvernementale doit communiquer cette information avec un préavis de [T_INFO_NU] avant le début du mois suivant.

4.9.5 Délai de traitement par l'ACR de l'IGC/A d'une demande de révocation

Les demandes de révocation devront être traitées à réception par l'AE de l'IGC/A.

Pour une LAR urgente, le temps pour traiter une révocation, c'est-à-dire le délai entre la prise en compte de la demande par l'AE de l'IGC/A et la publication de la LAR par le SP, sera défini par [T_REVOC].

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

Les ACR gouvernementales doivent publier au point de distribution de la liste de révocation indiqué dans le certificat qui leur a été délivré par l'IGC/A, une copie de la LAR publiée sur le site de publication des LAR de l'IGC/A, ou par messagerie, selon le moyen choisi par le SP de l'IGC/A pour les informations urgentes. L'ACR vérifie que cette copie est intègre, notamment en en vérifiant la signature apposée par l'IGC/A.

Les autres utilisateurs peuvent vérifier les statuts des certificats délivrés par l'IGC/A tant à l'aide de ces copies qu'à l'aide du SP de l'IGC/A. La [RFC5280] indique les mécanismes de vérification auxquels se conformer.

4.9.7 Fréquence d'établissement des LAR

Quoique soit très faible la probabilité de révoquer un certificat d'ACR gouvernementale compte tenu des fortes exigences de sécurité requises pour toute demande de certificat, l'IGC/A s'efforce de couvrir les objectifs de sécurité suivants pour l'établissement de ses LAR :

- La fréquence doit être assez rapprochée pour limiter le temps de latence pendant lequel les applications qui ont chargé la LAR précédente n'iront pas consulter la nouvelle LAR ([T_RECOUV_LAR]) ; en effet, selon la [RFC5280], les applications n'ont aucune obligation de vérifier la présence d'une nouvelle LAR avant la date de publication de la prochaine LAR indiquée dans la LAR en cours.
- La fréquence de publication doit faciliter la gestion manuelle des duplications et publications par les ACR ; la publication est donc mensuelle.
- Le SP de l'IGC/A dispose de trois jours au maximum pour publier la LAR valide au premier jour du mois.

- Les ACR doivent copier le LAR et en faire la mise en ligne dans leur système avant le 6ème jour du mois.
- Une défaillance dans le processus ne doit pas impacter de façon majeure le fonctionnement des IGC des ACR gouvernementales, et doit pouvoir être corrigée dans un délai Max([T_INFO_CRISE] ; [T_DISPO_PUB]).

Ces objectifs sont couverts par les exigences suivantes :

- La fréquence de mise à jour des listes de certificats révoqués est indiquée par [F_MAJ_LAR]. En cas de révocation en urgence, une nouvelle LAR sera publiée indépendamment de cette périodicité. Les ACR en seront averties par messagerie électronique via Internet, ou par un réseau sécurisé en cas d'indisponibilité.
- Les listes de révocation publiées doivent préciser la date de publication de la LAR suivante. La nouvelle LAR sera publiée au plus tard à cette date par les ACR. Les LAR ont une durée maximale de validité de [T_VALID_LAR].

4.9.8 Délai maximum de publication d'une LAR

Les LAR mensuelles sont signées par anticipation et par lots de douze LAR au maximum.

En cas de révocation urgente, la publication de la LAR sur le site de la DCSSI est faite dans les 24 heures.

Les ACR ont un délai maximum de [T_RECOUV_LAR] pour publier une copie de la LAR signée par l'ACR de l'IGC/A.

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

L'IGC/A ne met en œuvre aucun système de vérification en ligne de la révocation et de l'état des certificats, indépendamment de la publication sur Internet de LAR et certificats.

Les ACR peuvent mettre en place un tel système.

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

Sans objet.

4.9.11 Autres moyens disponibles d'information sur les révocations

Le cas échéant la DPC précisera les autres moyens à utiliser, dont seront informés les porteurs de certificats délivrés par l'IGC/A.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

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'ACR, et sur le site de la DCSSI.

4.9.13 Causes possibles d'une suspension

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

4.10 Service d'état des certificats

L'IGC/A met à la disposition des utilisateurs de certificats, sur le site de la DCSSI en libre consultation, des LAR format V2.

Les ACR ont pour obligation de dupliquer ces LAR sur leur propre infrastructure, dans un annuaire accessible en protocole LDAP V3.

La fonction d'information sur l'état des certificats doit être rendue disponible tant par l'ACR de l'IGC/A que par les ACR certifiées, avec une durée maximale d'indisponibilité par mois de 5 jours.

L'IGC/A n'offre pas de service de vérification automatique de l'état des certificats, tel qu'un serveur OCSP par exemple.

4.11 Fin de la relation entre l'ACR et l'ACR de l'IGC/A

En cas de fin de relation entre l'ACR et l'ACR de l'IGC/A avant la fin de validité du certificat, par exemple par suite de changement de statut de l'organisme auquel appartient l'ACR, le certificat délivré par l'IGC/A à cette dernière doit être révoqué.

4.12 Séquestre de clé et recouvrement

L'IGC/A ne délivrant pas de bi-clé aux ACR gouvernementales, le séquestre de clés n'est pas un service traité par la présente PC.

Les clés privées d'ACR ne doivent pas être séquestrées.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physiques

5.1.1 Situation géographique et construction des sites

Situation géographique

Les sites d'hébergement des composantes de l'IGC/A, et notamment du SP de l'IGC/A, doivent se trouver sur le territoire national.

Il en est de même pour les ACR demandant un certificat.

Protection contre les signaux parasites compromettants (S.P.C.)

L'implantation des dispositifs cryptographiques utilisés pour protéger les clés privées de l'ACR et des AC ne doit pas permettre l'interception, par un individu malveillant, des signaux parasites d'origine électromagnétique émis par les matériels (par conduction sur les câbles d'alimentation électrique ou les fils de masse ou par rayonnement en espace libre).

La capture de ces signaux, dits signaux parasites compromettants, dépend de la distance à l'équipement visé ou de la possibilité de se connecter aux câblages ou à tout autre conducteur passant à proximité de l'équipement (phénomène de couplage).

Une étude du contexte d'emploi et des équipements peut être demandée à la DCSSI pour définir les mesures de protection à mettre en œuvre.

Il est recommandé de suivre les instructions [IGI900] et [II300] pour la protection des clés privées des AC, c'est-à-dire de respecter l'une des conditions suivantes :

- soit, suite à l'évaluation du dispositif cryptographique, il est possible de définir une distance minimale entre les dispositifs cryptographiques et les locaux échappant au contrôle de l'AA (voie publique, voisinage) (par exemple 20 mètres dans toutes les directions (y compris verticalement), si les dispositifs sont de catégorie C) ;
- soit les dispositifs cryptographiques sont des matériels dits TEMPEST gérés selon les règles de l'instruction [II910] sur les articles contrôlés de la sécurité des systèmes d'information ;
- soit le local hébergeant les dispositifs cryptographiques est une enceinte faradisée.

Protection de l'IGC/A contre les S.P.C.

La plate-forme cryptographique de l'IGC/A doit toujours être opérée dans une cage de Faraday accueillant des personnes non hostiles.

5.1.2 Accès physique

La plate-forme de certification de l'IGC/A doit être stockée 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 physique aux dispositifs utilisés par les ACR pour protéger leurs clés privées ne doit être possible qu'aux seules personnes utilisant ces dispositifs.

5.1.3 Alimentation électrique et climatisation

La prévention physique contre des incidents matériels est effectuée conformément à la politique de sécurité de l'AA de l'IGC/A, et aux conditions contractuelles liant l'AA de l'IGC/A et les tiers hébergeant une ou plusieurs composantes de l'IGC/A.

La plate-forme de l'IGC/A est opérée dans un local climatisé et sur courant secouru. Des batteries permettent l'exploitation de la plate-forme en dépit d'une coupure d'alimentation électrique impromptue.

5.1.4 Vulnérabilité aux dégâts des eaux

La plate-forme de l'IGCA est stockée dans un local qui n'est pas sujet aux dégâts des eaux. Le risque d'inondation ne pouvant être écarté concernant le site hébergeant une ou plusieurs composantes de l'IGC/A, le plan anti-sinistre de l'IGC/A comporte une procédure de déménagement des composantes dans un local présentant les mêmes caractéristiques de protection des clés privées et des matériels qui ne soit pas menacé d'inondation.

5.1.5 Prévention et protection incendie

La prévention physique contre des incidents matériels est effectuée conformément à la politique de sécurité validée par l'AA de l'IGC/A, et aux conditions contractuelles liant l'AA de l'IGC/A et les tiers hébergeant une ou plusieurs composantes de l'IGC/A.

Les consignes de sécurité incendie doivent être vérifiées et connues des utilisateurs de la plate-forme de l'IGC/A.

5.1.6 Conservation des supports

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

5.1.7 Mise hors service des supports

La destruction des éléments ACSSI et des supports d'informations sensibles sera toujours réalisée conformément à la réglementation en vigueur pour les documents sensibles ou classifiés de défense.

5.1.8 Sauvegardes hors site

Le plan anti-sinistre définit la stratégie de sauvegardes et recouvrement.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

L'IGC/A réunit différents rôles de confiance pour opérer et contrôler ses services. Le §1.4 détaille ces différents acteurs.

On soulignera en particulier le rôle :

- du responsable sécurité de l'IGC/A ;
- de l'ACR et de l'AE de l'IGC/A ;
- des ingénieurs ;
- des opérateurs ;

- des évaluateurs et auditeurs ;
- des porteurs de parts de secrets.

5.2.2 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 opérations » de la DPC permet de définir un nombre d'exploitants minimum nécessaires par type d'opérations.

5.2.3 Identification et authentification pour chaque rôle

L'ACR doit faire vérifier l'identité et les autorisations de tout membre de son personnel avant de lui attribuer un rôle et les droits correspondants

Ces contrôles doivent être décrits dans la DPC de l'ACR et doivent être conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC doit être notifiée par écrit.

5.2.4 Rôles exigeant une séparation des attributions

Concernant les rôles de confiance, les cumuls suivants sont interdits au sein de l'IGC/A :

- (pendant une cérémonie) responsable de sécurité et tout autre rôle ;
- (pendant le développement et l'évaluation d'une même version du système) évaluateurs et ingénieurs ;
- (de façon générale) opérateurs et ingénieurs.

Les porteurs de secret ne doivent jamais détenir deux parts différentes d'un même secret.

Le responsable de sécurité de l'IGC/A ne peut pas être ingénieur système.

La DPC de l'IGC/A précisera les attributions de chacun des rôles définis dans cette PC.

Les ACR doivent définir les règles de séparation des rôles en fonction des risques encourus par le cumul de rôle pouvant compromettre la sécurité des fonctions mises en œuvre.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Les agents recrutés par l'AA de l'IGC/A sont soumis à leur devoir de réserve. Ils sont par ailleurs habilités au moins au niveau de confidentialité requis par la présente PC lorsqu'ils ont le besoin d'avoir accès à des documents classifiés (cf §5.3.8).

Les autorités de l'IGC/A doivent s'assurer que les personnels amenés à opérer les services dont elles ont la responsabilité, ont des attributions qui correspondent à leurs compétences professionnelles.

L'ACR de l'IGC/A doit informer toute personne intervenant dans des rôles de confiance de l'IGC/A :

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

5.3.2 Procédures de vérification des antécédents

Préalablement à l'affectation à un rôle de confiance, les agents recrutés par l'AA de l'IGC/A devront avoir été habilités au niveau CONFIDENTIEL DEFENSE. Leur habilitation sera revue régulièrement, au minimum une fois tous les 5 ans.

5.3.3 Exigences en matière de formation initiale

Les personnes intervenant dans les services de l'IGC/A, doivent être formées aux logiciels, matériels et procédures internes de fonctionnement des services opérés.

5.3.4 Exigences et fréquence en matière de formation continue

Tout nouvel opérateur 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 opérateur devra assister à une formation après toute évolution importante du système.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Aucune exigence spécifique concernant la fréquence de rotation n'est exprimée, à l'exception de la rotation des rôles de porteurs de secrets.

Les porteurs de secret peuvent déléguer, selon les règles de délégation des ACSSI, leur part à une personne qui ne peut en aucun cas recevoir en propre ou en délégation, une autre part de secret durant toute la vie de la bi-clé partagée.

5.3.6 Sanctions en cas d'actions non autorisées

L'ACR de l'IGC/A, en concertation avec l'AA, décide des sanctions à appliquer lorsqu'un agent abuse de ses droits ou effectue une opération non-conforme à ses attributions.

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

Les personnels contractants doivent respecter les mêmes conditions que celles énoncées dans les rubriques 5.3.1, 5.3.2, 5.3.3 et 5.3.4.

5.3.8 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/A ;
- DPC de l'IGC/A ;
- documentation technique des matériels et logiciels utilisés ;
- manuels de formations ;
- procédures internes de fonctionnement.

L'ACR et l'AE doivent veiller à ce que leur personnel respectif possède bien les documents identifiés ci-dessus en fonction de leur besoin d'en connaître comme le précise la DPC.

5.4 Procédures de constitution des données d'audit

5.4.1 Type d'événements à enregistrer

Informations minimales pour tout événement :

- date et heure de l'opération ;
- ACR concernée par l'opération ;
- nom de l'opérateur ;
- caractéristiques de l'événement.

Doivent être consignés ainsi dans le registre de cérémonies de l'IGC/A, les événements suivants :

- création de bi-clés IGC/A ;
- vérification des supports de parts de secrets IGC/A ;
- délivrance de certificats :
    - o génération de certificat d'une ACR gouvernementale (nouveau certificat, renouvellement, modification) ;
    - o génération de certificats propres à l'IGC/A ;
- révocation ;
- fin de vie de l'IGC.

Sont consignés également dans le registre de cérémonies de l'IGC/A les événements physiques dont la trace n'est pas fournie automatiquement par le système, comme :

- accès physiques aux plates-formes de cérémonie et cryptographiques de l'IGC/A ;
- déménagement du matériel ;
- sortie pour maintenance ;
- changement de configuration du système ;
- modifications de droits d'accès ;
- changements de mots de passe ;
- destruction de secrets.

Sont consignés dans d'autres registres, précisés dans la DPC, les événements tels que :

- accès physiques aux plates-formes ;
- changements concernant les personnes auxquelles un rôle de confiance est attribué (cf §5.2.1) ;
- communications avec le service de publication ;
- création et transmission de récépissés ;
- demandes d'ACR gouvernementales ;
- résultats d'audits.

Informations journalisées sur la plate-forme :

- démarrage et arrêt de l'application ;
- connexion d'un utilisateur ;
- modification de paramètres de configuration ;
- sauvegarde du journal d'audit ;
- messages d'alerte de l'application ou du système d'exploitation ;
- copie et suppression de fichiers ;
- création de nouveaux comptes.

Les ACR doivent mettre en place un système d'enregistrement d'événements analogues, qu'ils doivent indiquer dans leur PC.

5.4.2 Fréquence de traitement des journaux d'événements

L'analyse du contenu des journaux d'événements doit être effectuée de manière régulière par l'ACR de l'IGC/A, [F_JOURNX]. Un traitement particulier pour les alertes devra être mis en place et décrit dans la DPC.

5.4.3 Période de conservation des journaux d'événements

Les journaux sont archivés suivant la période [T_A _JOURNX].

5.4.4 Protection des journaux d'événements

Les journaux d'événements doivent être protégés en intégrité et confidentialité.

Les journaux d'événements ne peuvent être sauvegardés que par le responsable sécurité de l'IGC/A.

La DPC et la documentation système précise les moyens de protection employés.

5.4.5 Procédure de sauvegarde des journaux d'événements

Une copie de sauvegarde des journaux d'événements est réalisée après chaque cérémonie sur les plates-formes IGC/A.

Les ACR doivent mettre en place une procédure de sauvegarde adaptée à leur propre dispositif de protection des clés.

5.4.6 Système de collecte des journaux d'événements

Le système de collecte des journaux est décrit dans la DPC. Il peut être externe à la plate-forme de l'ACR ; il doit être intègre et respecter le même niveau de protection que les journaux originaux.

L'IGC/A dispose d'un système interne de collecte des journaux, régulièrement sauvegardés.

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

L'imputabilité d'une action revient à la personne, l'organisme ou le système l'ayant exécutée. Son nom est indiqué dans l'application s'il s'agit de l'opérateur, qui est informé avant sa prise de fonctions de l'enregistrement de ses actions dans les journaux des plates-formes IGC/A. Les acteurs intervenants sur les plates-formes sont nommés dans les procès verbaux d'opération qu'ils émargent en toute connaissance de cause.

5.4.8 Évaluation des vulnérabilités

Une procédure interne d'analyse du contenu des journaux d'événements doit permettre de détecter les vulnérabilités du système et prévenir les attaques potentielles sur le système. Cette procédure est détaillée dans la DPC.

5.5 Archivage des données

5.5.1 Types de données à archiver

Les procédures et les outils doivent permettre d'archiver les données suivantes :

- accords contractuels ou conventions ;
- certificats de l'IGC/A ;
- certificats des ACR gouvernementales délivrés par l'IGC/A, valides comme révoqués ;
- attribution des rôles de confiance ;
- constitution de la commission d'homologation ;
- dossiers d'homologation ;
- journaux d'événements
- logiciels et fichiers de configuration des différentes composantes ;
- déclaration de dépôt des codes sources ;
- ensembles des éléments utiles à l'enregistrement :
    - récépissés ;
    - dossiers d'enregistrement (demandes papier, données d'identification, requêtes ou certificats autosignés, etc.) ;
    - demandes de révocation et leurs résultats ;
    - courriers officiels de l'ACR ;
- rapports d'audits menés par la DCSSI ;
- registres de cérémonie ;
- scripts des cérémonies ;
- LAR.

5.5.2 Période de conservation des archives

Les durées d'archivage des données définies au §5.5.1 sont les suivantes :

accords contractuels ou conventions	pendant 10 ans
journaux d'événement	pendant une durée égale à [T_A_JOURNX]
certificats de l'ACR de l'IGC/A et des ACR certifiées	pendant [T_A_CERT]
toutes les autres données	pendant une durée de [T_ARCHIVES]

5.5.3 Protection des archives

Les archives doivent être protégées en intégrité et en confidentialité selon les mêmes règles de protection que les données avant leur archivage, sauf décision contraire de l'ACR de l'IGC/A.

Leur disponibilité doit être assurée selon un délai de restitution de [T_RECUP_ARCH].

5.5.4 Procédure de sauvegarde des archives

La procédure de sauvegarde des archives de l'IGC/A est détaillée dans la DPC de l'IGC/A.

Les ACR doivent indiquer dans leur DPC la procédure suivie pour leurs propres IGC.

5.5.5 Exigences d'horodatage des données

L'ACR définira dans la DPC la précision de l'horloge pour dater les événements enregistrés et archivés. Un soin particulier sera apporté à ce qu'il y ait une base de temps commune entre les composantes de l'IGC/A.

5.5.6 Système de collecte des archives

Le système de collecte des archives est celui du système d'information du SGDN. Il respecte les besoins de sécurité des informations archivées.

5.5.7 Procédures de récupération et de vérification des archives

Les archives sont sous la responsabilité de l'ACR de l'IGC/A. Le processus de récupération doit faire l'objet d'une procédure interne de fonctionnement mentionnée dans la DPC de l'IGC/A. La récupération doit être effectuée sous un délai maximal égal à [T_RECUP_ARCH].

5.6 Changement de clé d'AC

5.6.1 Clés de l'ACR de l'IGC/A

Lorsqu'une composante de l'IGC/A renouvelle ses clés, elle en informe ses utilisateurs ainsi que l'AA de l'IGC/A, sous une période minimale donnée égale à T_CHG_KEY. Selon la nature du changement (fin de période de validité de clés, renouvellement de clé suite à une révocation, etc.), les mesures prises doivent respecter les procédures de traitement énoncées dans les chapitres correspondants.

5.6.2 Clés d'ACR

L'IGC/A ne peut pas générer de certificats d'ACR dont la durée de vie dépasse la période de validité de son propre certificat. Aussi lorsqu'elle accède à une demande de certification, l'ACR de l'IGC/A fixe la durée de vie du certificat demandé de telle sorte qu'il ne soit jamais valable au-delà de la date de fin de validité du certificat de la bi-clé de l'IGC/A utilisée pour la signature.

Par ailleurs l'ACR de l'IGC/A n'attribue sa confiance à la clé d'une ACR gouvernementale qu'au plus pour une durée de [T_VALID_CERT], soit la durée de vie maximale des certificats délivrés par l'IGC/A.

La durée [T_VALID_CERT] est déterminée en tenant compte des recommandations cryptographiques de sécurité relatives aux longueurs de clés de la DCSSI [CRYPTO], et des besoins fonctionnels dictés par les produits du marché.

Une ACR gouvernementale peut toutefois générer des certificats auto-signés dont la durée de vie dépasse celle des certificats délivrés par l'IGC/A.

5.7 Reprise suite à compromission et sinistre

La référence au plan anti-sinistre, les modalités de déclenchement et les personnes responsables de ce plan doivent être nommées dans la DPC.

Ce plan doit être régulièrement testé, selon une fréquence F_TEST_PLAN.

L'IGC/A dispose d'un plan de reprise d'activité en cas de sinistre qui prend en compte les paramètres suivants :

- délai minimum de recouvrement de ses services ;
- politique de sécurité et de protection des secrets ;
- procédures de secours ;
- tests pratiques, formation et entraînement des personnels.

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

Les incidents ou compromissions détectées par le responsable sécurité de l'IGC/A, les ingénieurs système ou les évaluateurs, font l'objet d'une communication à l'ACR de l'IGC/A et au président de la commission d'homologation.

Les incidents ou compromissions détectés par les ACR gouvernementales doivent faire l'objet d'une information à l'ACR de l'IGC/A, qui en saisira au besoin la commission d'homologation de l'IGC/A.

La DPC précisera les mesures à appliquer dans un tel cas.

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

Cette procédure est détaillée dans la DPC et le plan de crise de l'IGC/A.

Les ACR doivent prévoir une telle procédure, qui doit inclure l'information de l'ACR de l'IGC/A.

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

Ces procédures doivent être décrites dans le plan de crise de l'IGC/A.

5.7.4 Capacités de continuité d'activités suite à un sinistre naturel ou autre

Cette rubrique doit être renseignée et apparaître dans le plan de crise de l'IGC/A.

5.8 Fin de vie de l'IGC

Toute ACR gouvernementale s'engage à ce qu'en fin de vie de l'IGC dont elle a la charge, elle se charge de :

- communiquer à l'ACR de l'IGC/A, dans le délai [T_FIN_VIE], son intention de cessation d'activité ;
- indiquer le moyen permettant d'accéder à ses archives, et la date de leur destruction programmée.

L'ACR de l'IGC/A procèdera alors à la révocation des certificats qui ont été délivrés à l'ACR gouvernementale, et en fera la publication suivant les procédures habituelles concernant la révocation. Il est dès lors considéré que les engagements pris entre l'ACR gouvernementale et l'ACR de l'IGC/A sont caduques.

En fin de vie de l'IGC/A :

- l'ACR doit s'assurer qu'aucun contractant ne peut agir pour son compte dans le processus de génération de certificat ;
- l'ACR doit alerter les utilisateurs de ses certificats de son intention de fin de vie dans le délai [T_FIN_VIE] ;
- l'ACR doit révoquer tous les certificats encore valides qu'elle a signés, y compris les siens ;
- les clés privées de l'ACR doivent être détruites conformément au §6.2.10 ;
- l'ACR doit préciser dans sa DPC qui elle doit prévenir et comment se déroule le transfert de ses obligations.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

Nota :

L'ACR de l'IGC/A ne génère pas de bi-clés pour les ACR. Par conséquent les paragraphes 6.1.1 et 6.1.2 suivants ne s'appliquent qu'aux bi-clés propres à l'ACR de l'IGC/A.

6.1.1 Génération des bi-clés

L'ACR de l'IGC/A génère plusieurs bi-clés de signature pour elle-même, afin de suivre l'évolution de l'état de l'art en cryptographie et les besoins opérationnels des ACR gouvernementales.

C'est lors d'une cérémonie de clés, en présence de l'ACR de l'IGC/A et des personnes identifiées au §5.2.1, que les nouvelles bi-clés sont générées, à l'aide d'une plate-forme cryptographique développée par la DCSSI et homologuée. Les clés et certificats générés font l'objet de plusieurs vérifications pour en assurer l'intégrité. La confidentialité des clés est assurée par des mesures techniques et organisationnelles détaillées dans la DPC.

6.1.2 Transmission de la clé privée à son propriétaire

Les clés privées de l'ACR de l'IGC/A lui sont transmises sous la forme de secrets partagés entre plusieurs porteurs sous les ordres de l'ACR de l'IGC/A. Les parts de secret ne peuvent pas être utilisées à l'insu de l'ACR de l'IGC/A.

Ces parts de secrets sont prises en compte formellement et nominativement et gérées suivant les procédures applicables aux ACSSI CD.

6.1.3 Transmission de la clé publique d'une ACR à l'ACR de l'IGC/A

Lors de sa transmission à l'IGC/A pour sa certification, la clé publique de l'ACR gouvernementale devra être protégée en intégrité et son origine devra en être authentifiée.

Les modes de transmission de la clé publique (certificat auto-signé, PKCS#10…), sont définis dans la procédure de demande de certificat indiquée au §4.2.

6.1.4 Transmission de la clé publique de l'ACR de l'IGC/A aux utilisateurs de certificats

L'ACR de l'IGC/A publie conjointement son certificat via son SP, et par une autre source utilisant de préférence un medium de communication différent (avis de publication au Journal officiel de la République française notamment).

Elle peut remettre également son certificat sur un support amovible directement aux témoins de l'ACR participant à une cérémonie de signature.

La transmission de la clé publique de l'IGC/A peut être faite également à l'attention des éditeurs de produits de communication selon un protocole à établir entre les parties, qui garantisse l'intégrité et l'origine de la clé publique.

6.1.5 Tailles des clés

Concernant l'IGC/A :

La taille de la clé de signature de l'ACR de l'IGC/A est d'au moins 2048 bits pour l'algorithme RSA.

La taille de la clé de signature de l'ACR de l'IGC/A est d'au moins 1024 bits pour l'algorithme DSA.

La fonction de hachage utilisée est SHA-1 ou SHA-2.

Les algorithmes de chiffrement symétrique, s'ils sont utilisés, doivent être l'AES ou le triple DES, ou un algorithme réputé plus robuste.

L'utilisation de courbes elliptiques est également autorisée.

Concernant les ACR :

La taille des clés des ACR doit suivre les mêmes exigences que celles de l'IGC/A.

L'algorithme utilisé doit être identique à celui de la clé IGC/A devant délivrer le certificat.

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

Concernant l'IGC/A :

La génération des paramètres des clés publiques et la vérification de leur qualité sont réalisées par la plate-forme cryptographique développée par la DCSSI selon les normes de sécurité propres à l'algorithme de chaque bi-clé.

Concernant les ACR :

L'équipement de génération de bi-clés doit utiliser des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

6.1.7 Objectifs d'usage de la clé

La clé privée de l'ACR de l'IGC/A sert pour les opérations de signatures des certificats des ACR et des LAR. Elle peut servir à la signature d'échanges entre composantes techniques de l'IGC/A.

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR et/ou de réponses OCSP, et à la sécurisation d'échanges entre composantes techniques de l'IGC.

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

Les clés de l'ACR de l'IGC/A sont générées à l'aide d'une ressource cryptographique matérielle isolée maîtrisée par les laboratoires de la sous-direction scientifique et technique de la DCSSI.

Les ACR demandant la délivrance d'un certificat par l'IGC/A, doivent disposer d'une ressource qui assure la protection des clés de l'ACR avec un niveau de sécurité jugé acceptable au regard des menaces pesant sur l'intégrité, la disponibilité et la confidentialité des bi-clés de l'AC racine et des AC déléguées.

Les clés de l'ACR ne doivent pas être stockées sur une ressource qui présente des vulnérabilités exploitables par un tiers non autorisé, et qui permettent de réaliser des opérations engageant l'ACR à son insu.

Une configuration conseillée est l'utilisation d'un boîtier de sécurité qualifié au niveau EAL4+ hors ligne.

Les générateurs d'aléas utilisés doivent être conformes à l'état de l'art, aux standards en vigueur ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Concernant l'IGC/A :

Le contrôle de la clé privée de l'ACR de l'IGC/A est réalisé par plusieurs personnes ; n exploitants parmi m sont nécessaires pour l'accès à la clé privée de l'ACR. Le système cryptographique utilisé garantit que la perte ou le vol de n éléments d'activation ne permet pas de compromettre la confidentialité de la clé. La clé privée de l'ACR de l'IGC/A ne peut être utilisée à l'insu de cette dernière.

La DPC précise les modalités de ce contrôle et les rôles de confiance impliqués.

Concernant les ACR :

Les clés de l'ACR ne doivent pas pouvoir être utilisées à son insu.

6.2.3 Séquestre de la clé privée

Concernant l'IGC/A :

Les clés privées de signature de l'ACR IGC/A ne sont pas séquestrées.

Les moyens mis en œuvre pour assurer la disponibilité et l'intégrité de la clé privée doivent permettre de faire face à la perte d'un des éléments utilisés pour activer la clé.

Concernant les ACR :

Le séquestre des clés des ACR n'est pas autorisé.

6.2.4 Copie de secours de la clé privée

Concernant l'IGC/A :

Aucune copie de secours des clés privées de l'ACR de l'IGC/A n'est effectuée. En revanche, des copies de secours des éléments permettant d'activer la clé sont réalisées. Elles répondent au besoin d'intégrité et de disponibilité de la plate-forme IGC/A, en permettant de se prémunir contre un sinistre majeur sur le site d'hébergement de la plate-forme, la perte ou le vol de l'un des éléments d'activation, et une défaillance du support d'enregistrement. Les conditions de génération, délivrance aux porteurs et stockage de ces copies, assurent le même niveau de protection de la confidentialité que celui des originaux.

Concernant les ACR :

Les conditions de génération, délivrance aux porteurs et stockage des copies des clés privées doivent assurer le même niveau de protection de la confidentialité que celui des originaux.

Les clés privées peuvent faire l'objet de copies de secours soit dans un module cryptographique conforme aux exigences du §6.2.1 ci-dessus, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les opérations de chiffrement et de déchiffrement doivent être effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.

La longueur des clés symétriques de chiffrement utilisées sera de préférence au moins égale à 128 bits et en aucun cas inférieur à 100 bits (ex : AES, triple DES).

La taille des blocs utilisés devra être au minimum de 64 bits, et de préférence de 128 bits (triple DES=64 bits, AES=128 bits). Par ailleurs, le mode opératoire utilisé doit apporter une "bonne sécurité" et permettre de protéger la clé privée de l'AC en confidentialité mais aussi en intégrité. Pour ce faire, le mode opératoire CBC-MAC pourrait être utilisé.

Pour toute information complémentaire sur les algorithmes, il est recommandé de se référer au document sur les règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard de la DCSSI [R_ALGO].

6.2.5 Archivage de la clé privée

Aucune archive n'est effectuée de la clé privée de l'IGC/A.

Aucune archive ne doit être effectuée des clés privées des ACR.

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

Tout transfert de clé privée doit se faire sous forme chiffrée, conformément aux exigences du §6.2.4.

Les clés privées de l'ACR de l'IGC/A ne peuvent pas être transférées.

6.2.7 Stockage de la clé privée dans un module cryptographique

Il est recommandé de stocker les clés privées d'ACR dans un module cryptographique qualifié au niveau EAL4+ et utilisé hors ligne.

Cependant, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences du §6.2.4.

6.2.8 Méthode d'activation de la clé privée

L'activation des clés privées d'ACR dans un module cryptographique doit être contrôlée via des données d'activation et doit faire intervenir au moins deux personnes dans des rôles de confiance.

L'activation des clés privées de l'ACR de l'IGC/A est conforme à cette exigence ; la procédure d'activation est détaillée dans la DPC.

6.2.9 Méthode de désactivation de la clé privée

La désactivation des clés privées d'ACR dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

Une clé privée d'ACR peut également être désactivée après une certaine période d'inactivité.

La désactivation de la clé privée de l'ACR de l'IGC/A utilisée lors d'une cérémonie de signature ou de génération de bi-clé et de certificat, est réalisée immédiatement après l'utilisation de la clé.

6.2.10 Méthode de destruction des clés privées

En fin de vie d'une clé privée d'ACR, normale ou anticipée (révocation), cette clé doit être systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

La procédure de destruction doit assurer qu'aucune reconstitution totale ou partielle de la clé ne peut être réalisée pendant et après la destruction.

Les clés privées de l'IGC/A sont détruites suivant une procédure détaillée référencée dans la DPC.

6.2.11 Niveau d'évaluation sécurité du module cryptographique

L'ACR doit pouvoir justifier que la ressource qu'elle utilise pour protéger ses clés privées répond aux exigences définies au §6.2.1.

La sécurité de la ressource cryptographique de l'IGC/A a été évaluée par la DCSSI.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Concernant l'IGC/A :

Aucun archivage spécifique des clés publiques n'est réalisé en dehors de l'archivage des certificats.

Ces derniers sont archivés et conservés conformément au §5.5 Archivage des données.

Concernant les ACR :

Les clés publiques de l'ACR et des porteurs de certificats qu'elle délivre doivent être archivées dans le cadre de l'archivage des certificats correspondants ; aucun autre archivage n'est exigé.

6.3.2 Durées de vie des bi-clés et des certificats

Concernant l'IGC/A :

La durée de validité (crypto-période) de la bi-clé de l'ACR de l'IGC/A est [T_VALID_CERT]. Néanmoins cette durée peut être remise en cause par l'évolution de l'état de l'art en cryptologie.

Concernant les ACR :

La fin de validité d'un certificat autosigné d'ACR doit être postérieure à la fin de vie des certificats porteurs qu'elle émet. L'ACR doit préciser dans sa PC la durée de vie des clés de signature d'ACR et des certificats correspondants. Cette durée de vie doit être cohérente avec les caractéristiques de l'algorithme et la longueur de clé utilisés. Il est recommandé que la durée de vie des bi-clés respecte les règles [R_ALGO].

Aucune autre exigence particulière n'est prononcée pour la durée de validité des bi-clés des ACR.

En revanche les certificats sont délivrés aux ACR par l'IGC/A pour une durée définie.

Cette durée est la plus petite parmi :

- la durée de vie restante indiquée dans le certificat autosigné de l'ACR ;
- la durée de vie restante du certificat de la bi-clé IGC/A utilisée pour la signature ;
- la durée de vie maximale des certificats délivrés, indiquée par la variable [T_Valid_Cert].

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

La génération et l'installation des données d'activation d'un module cryptographique ou d'un dispositif conforme au §6.2.1doivent se faire lors de la phase d'initialisation et de personnalisation de ce module ou dispositif. Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles doivent leur être transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne doivent être connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués.

Les données d'activation des bi-clés de l'ACR de l'IGC/A sont générées et installées conformément à cette exigence.

Si l'ACR génère la clé privée du porteur, elle a pour obligation de transmettre au porteur les données d'activation correspondantes par le biais d'un chemin garantissant la protection en intégrité et en confidentialité des données. Notamment, la remise de la donnée d'activation doit être séparée dans le temps ou dans l'espace de la remise de la clé privée.

L'ACR de l'IGC/A ne génère aucune donnée d'activation pour les ACR.

6.4.2 Protection des données d'activation

La protection en intégrité et en confidentialité des données d'activation générées par l'ACR de l'IGC/A pour sa plate-forme cryptographique relève de sa responsabilité jusqu'à la remise au destinataire. Une fois ces données transmises, il appartient au destinataire d'en assurer la confidentialité, l'intégrité et la disponibilité. Sa responsabilité pourra donc être engagée en cas d'utilisation de ces données par une personne non autorisée.

6.4.3 Autres aspects liés aux données d'activation

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

Ce chapitre est sans objet pour l'ACR de l'IGC/A.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Pour la plate-forme de l'IGC/A, SP inclus, les besoins de sécurité sont les suivants :

- journalisation (imputabilité et nature des actions effectuées) des événements en fonction des rôles et des opérations ;
- gestion des sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapides des droits d'accès ;
- identification et authentification des utilisateurs du poste de travail ;
- protection contre les virus informatiques et toutes formes de logiciels compromettant ou non-autorisé et mise à jour des logiciels ;
- protection des supports d'informations contre les dommages, le vol et la compromission même par réutilisation et l'usurpation ;
- les supports amovibles utilisés lors de l'initialisation de la plate-forme de certification doivent être protégés en écriture et clairement identifiés ;
- filtrage des entrées et sorties du réseau ;
- gestion de la configuration du système d'information ;
- fonctions d'audits (non-répudiation et nature des actions effectuées).

Les ACR doivent respecter ces mêmes objectifs ainsi que les objectifs suivants si le dispositif dans lequel sont activées les clés de l'ACR est connecté à un réseau ouvert de façon permanente ou temporaire :

- 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.

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Le niveau d'évaluation est défini par la commission d'homologation de l'IGC/A.

Il est recommandé que les systèmes informatiques de l'IGC mettant en œuvre le module cryptographique fassent l'objet d'une qualification au niveau standard [QUALIF_STD].

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC doit être documentée et doit respecter dans la mesure du possible des normes de modélisation et d'implémentation.

La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau doivent être documentées et contrôlées.

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'ACR doit mener.

Les objectifs suivants ont été définis pour l'IGC/A :

- chaque évolution de la plate-forme de l'IGC/A doit faire l'objet d'une vérification de bon fonctionnement ;
- la configuration, les procédures d'installation et de maintenance doivent être documentées, testées et validées ;
- le développement d'un système permettant de mettre en œuvre les entités de l'IGC/A doit utiliser une méthode éprouvée ;
- une analyse de risque doit être menée avant tout développement de système de façon à prendre en considération les objectifs de sécurité dès la phase des spécifications ;
- l'IGC/A doit utiliser des systèmes et des produits de confiance sécurisés et protégés contre toute modification non autorisée ;
- l'ACR de l'IGC/A s'assure que chacune de ses entités satisfait aux exigences de sécurité correspondantes en utilisant, par exemple, des systèmes et/ou des matériels conformes à un ou plusieurs profils de protection appropriés, définis dans le cadre de la norme ISO 15408 ou une norme équivalente.

6.6.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC doit être signalée à l'ACR pour validation. Elle doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

Concernant l'IGC/A :

Toute évolution du système doit :

- être communiquée à la commission d'homologation de l'IGC/A
- être autorisée par l'ACR de l'IGC/A ;
- être documentée ;
- apparaître dans les procédures de fonctionnement internes à l'IGC/A ;
- être conforme au schéma de maintenance de l'assurance dans les produits évalués.

L'ACR de l'IGC/A s'assure :

- que des procédures de contrôle portant sur les modifications (mise à jour, correction, patch,…) existent ;
- que la sécurité de la ressource cryptographique n'est pas altérée par un tiers ou de toute autre manière pendant la durée de son transport, de son utilisation ou de sa conservation éventuelle ;
- que la ressource cryptographique fonctionne correctement ;
- que la capacité de traitements et de stockage répond au besoin ;
- que le maintien en conditions opérationnelles est assuré.

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

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

La commission d'homologation de l'IGC/A détermine ce niveau pour chaque version majeure des composantes de l'IGC/A.

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

De plus, les échanges entre composantes au sein de l'IGC peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

Une analyse de risque relative à l'interconnexion devra avoir été menée afin d'établir les objectifs et les solutions de sécurité adaptées. A défaut le dispositif cryptographique dans lequel les clés de l'ACR sont activées doit être isolé.

Concernant l'IGC/A :

Les plates-formes de signature et cryptographiques ne sont pas connectées en réseau. Les fichiers non confidentiels qui doivent être échangés entre services de l'IGC/A, pourront s'effectuer via des réseaux différents dès lors que leur intégrité, et l'intégrité des supports d'échanges de fichiers, est vérifiée et garantie par des moyens et procédures décrits dans la DPC.

6.8 Horodatage

Plusieurs exigences de la présente PC nécessitent la datation par les différentes composantes de l'IGC d'événements liés aux activités de l'IGC.

Pour dater ces événements, les différentes composantes de l'IGC peuvent recourir :

- soit à une autorité d'horodatage, interne ou externe à l'IGC, conforme à la politique d'horodatage de la [PRIS] ;
- soit en utilisant l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près.

L'IGC/A ne propose pas de service d'horodatage.

L'IGC/A utilise l'heure système de l'IGC ; les procédures d'exploitation imposent la vérification et la synchronisation systématique des composantes de l'IGC/A lors des cérémonies.

7 Profils des certificats et des LAR

7.1 Profil des certificats

7.1.1 Numéro de version

Les certificats utilisés sont les certificats X.509 v3 spécifiés dans le standard [RFC5280].

Les champs de base utilisés sont définis dans l'annexe 5 «Format des Certificats et des LAR».

7.1.2 Extensions du certificat

Les extensions critiques sont définies dans l'annexe 5 «Format des Certificats et des LAR».

7.1.3 OID des algorithmes

Les identificateurs d'algorithmes doivent être inscrits auprès d'un registre (par exemple un registre international tel que celui de l'ISO).

7.1.4 Forme des noms

Se reporter à l'annexe 5 «Format des Certificats et des LAR».

7.1.5 Contraintes sur les noms

Se reporter à l'annexe 5 «Format des Certificats et des LAR».

7.1.6 OID de PC

L'identificateur (OID) de la PC de l'IGC/A est indiqué en page de couverture et au §1.3.

Les certificats des ACR gouvernementales doivent respecter le format défini en ANNEXE 5 : Format des certificats et des LAR.

7.1.7 Utilisation de l'extension « contraintes de politique »

Se reporter à l'ANNEXE 5 : Format des certificats et des LAR.

7.1.8 Sémantique et syntaxe des qualifiants de politique

Se reporter à l'ANNEXE 5 : Format des certificats et des LAR.

7.1.9 Sémantiques de traitement des extensions critiques de la PC

Se reporter à l'ANNEXE 5 : Format des certificats et des LAR.

7.2 Profil des LAR

7.2.1 Numéro de version

La version 2 du format des listes des autorités révoquées (LAR) est utilisée. Elle est définie dans le standard [RFC5280].

7.2.2 Extensions de LAR et d'entrées de LAR

Les LAR incluent les champs de base de la version 2 de la norme sur les LAR, ainsi que les extensions :

- AuthorityKeyIdentifier (non critique),
- CRLNumber (non critique et optionnel).

7.3 Profil OSCP

Le protocole OCSP, qui permet à un client d'adresser une requête sur la validité d'un certificat à un serveur qui effectue lui-même cette analyse, n'est pas utilisé par l'IGC/A.

Ceci n'exclue pas qu'une ACR utilise ce protocole. Elle devra alors se conformer aux exigences portée dans les chapitres correspondants de la [PRIS].

8 Audit de conformité et autres évaluations

8.1 Fréquences et / ou circonstances des évaluations

Concernant l'IGC/A :

L'homologation par l'AA de la ou des plates-formes utilisées par l'ACR et l'AE de l'IGC/A, en fonction des éléments fournis par l'ACR DE L'IGC/A, doit précéder la première mise en service de l'IGC/A.

Un contrôle de conformité est réalisé de manière systématique après chaque modification majeure de la DPC, et régulièrement suivant la fréquence [F_CONFORM] relative aux composantes de l'IGC_A.

Concernant les ACR gouvernementales :

L'IGC de l'ACR gouvernementale est soumise à un audit de conformité, mandaté par l'ACR de l'IGC/A, avant sa certification par l'IGC/A. Puis suivant la fréquence [F_CONFORM] relative aux ACR gouvernementales, à partir de la date de délivrance du certificat, elle est soumise à une visite de contrôle.

8.2 Identités / qualifications des évaluateurs

Concernant l'IGC/A :

Les éléments relatifs à l'homologation du système IGC/A sont décrits dans le document d'homologation.

Concernant les ACR gouvernementales :

L'identification et les qualifications des contrôleurs seront précisées dans la demande de certification par l'ACR gouvernementale, ou dans la réponse à cette demande par l'AE de l'IGC/A.

8.3 Relations entre évaluateurs et entités évaluées

Les auditeurs en charge de l'audit de conformité des ACR gouvernementales sont soit :

- le service d'audit de la DCSSI ;
- un laboratoire d'audit agréé par la DCSSI.

L'ACR de l'IGC/A n'a en aucun cas obligation de prendre en compte un rapport d'audit mené par un autre organisme.

Les auditeurs en charge de l'audit de conformité de l'ACR de l'IGC/A sont des membres des services de la DCSSI qui respectent la règle de séparation des rôles définie au §5.2.4.

8.4 Sujets couverts par les évaluations

Concernant l'IGC/A :

Les éléments relatifs à l'homologation du système IGC/A sont décrits dans le document d'homologation.

Concernant les ACR gouvernementales :

Les éléments relatifs au contrôle de conformité (audit initial pour la certification, ou visite de contrôle) des ACR gouvernementales sont décrits dans le référentiel d'audit de l'IGC/A ([guide_audit_ACR] et [guide_rédaction_ACR]).

8.5 Actions prises suite aux conclusions des évaluations

Concernant l'IGC/A :

Les éléments relatifs à l'homologation du système IGC/A sont décrits dans le document d'homologation.

Concernant les ACR gouvernementales :

Pour chaque non-conformité observée, l'auditeur estimera le risque résiduel mineur, majeur ou critique pour la sécurité des ressources de l'ACR gouvernementale et de ses AC subordonnées auditées. Si des risques critiques sont constatés la demande de délivrance de certificat est refusée. Selon les non-conformités observées, l'ACR de l'IGC/A peut accepter la délivrance du certificat sous réserve de l'engagement de l'ACR gouvernementale à corriger les non-conformités dans le délai prescrit par l'auditeur.

Si lors d'une visite de contrôle, les non-conformités indiquées comme devant être corrigées persistent au-delà des délais prescrits, l'ACR de l'IGC/A peut prendre la décision de révoquer le certificat émis pour cette ACR gouvernementale.

8.6 Communication des résultats

Concernant l'IGC/A :

L'ACR de l'IGC/A prononce l'homologation par une note officielle. Ce document peut être diffusé aux ACR gouvernementales.

Concernant les ACR gouvernementales :

Les résultats des contrôles de conformité sont communiqués par l'ACR de l'IGC/A au correspondant nommément désigné dans la demande de l'ACR gouvernementale, à l'AA, à l'ACR et au HFDS ou FSSI ayant appuyé la demande.

9 Autres problématiques métiers et légales

9.1 Tarifs

La délivrance de certificats pour les ACR gouvernementales ne fait pas l'objet d'une facturation.

9.2 Responsabilité financière

L'AA de l'IGC/A s'engage à respecter la présente PC. Toute condition supplémentaire non portée dans ce document ne pourra être valablement considérée comme une obligation de l'AA de l'IGC/A.

En particulier, les pertes d'exploitations dues à la révocation d'un certificat à l'initiative de l'AA ou de l'ACR de l'IGC/A, à un retard dans le renouvellement d'un certificat non imputable à l'AA de l'IGC/A, un délai de traitement respectant les engagements décrits dans les présentes conditions, ne sauraient être retenues contre l'AA de l'IGC/A.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations classifiées

Information	Mentions de Protection ou de Classification
Les archives de journaux d'événements	Diffusion restreinte
La clé privée reconstituée propre à l'ACR	Confidentiel défense
Les secrets partagés, le secret principal et leurs supports physiques	ACSSI CD
Les données d'identification d'un acteur de l'IGC/A	Diffusion restreinte
Le dossier d'enregistrement d'une ACR gouvernementale	Diffusion restreinte
La DPC	Confidentiel défense
Le dossier d'homologation de l'IGC/A	Confidentiel défense
Les spécifications des plates-formes de cérémonie et cryptographique	Diffusion restreinte
La décision d'homologation de l'IGC/A	Diffusion restreinte
La cause de révocation d'un certificat	Diffusion restreinte
Le plan de crise de l'IGC/A et conditions particulières concernant les ACR gouvernementales en cas de crise	Confidentiel défense
Les résultats des audits des ACR gouvernementales	Diffusion restreinte

De la DPC peuvent être extraites certaines informations non classifiées, pour publication auprès des AA gouvernementales, ou d'un public plus large. C'est le cas notamment :

- des moyens utilisés pour la publication des informations non classifiées de défense,
- de la procédure de demande de certificats,
- et d'autres informations mentionnées explicitement comme telles dans la DPC ou faisant l'objet d'une dé-classification ponctuelle par l'ACR de l'IGC/A.

Les supports amovibles de la plate-forme de certification doivent recevoir la mention « ACSSI » et être traités conformément à [II910] et [DIR911] (notamment les aspects relatifs à la conservation, la maintenance et la destruction)

9.3.2 Informations hors du périmètre des informations confidentielles

La présente PC ainsi que les autres informations concernant l'IGC/A publiées par le SP et citées au chapitre 2, sont considérées comme non confidentielles.

9.3.3 Responsabilités en terme de protection des informations confidentielles

Les agents ayant connaissance de données confidentielles dans le cadre de leurs fonctions devront respecter le secret professionnel. S'ils ont à traiter des informations classifiées de défense, ils devront être habilités au niveau adéquat et justifier d'un besoin d'accès à ces données. En cas de manquement à ces obligations, des poursuites pénales pourront être engagées contre eux sur le fondement des articles 226-13 et 413-10 du code pénal.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

Il est entendu que toutes collectes et tout usage de données à caractère personnel qui seraient effectués par l'ACR de l'IGC/A seront réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL] (Cf. §9.15).

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles peuvent se trouver principalement dans :

- le dossier d'enregistrement d'une demande d'ACR (s'il comporte la copie de la carte d'identité notamment).

La DPC précisera les informations à caractère personnel qui seraient nécessaires dans d'autres cas, par exemple dans des procédures définies pour gérer une crise touchant l'ACR gouvernementale.

9.4.3 Responsabilité en termes de protection des données personnelles

L'ACR de l'IGC/A et l'ACR gouvernementale devront respecter les dispositions de la loi [CNIL]. A défaut, le responsable du traitement pourrait voir sa responsabilité pénale engagée et ce notamment quant aux formalités préalables à respecter et aux mesures de protection à adopter (articles 226-16 à 226-24 du code pénal).

9.4.4 Notification et consentement d'utilisation des données personnelles

Le consentement d'utilisation des données personnelles est exprimé par le demandeur qui appose sa signature sur le document présentant des données à caractère personnel, dans le cadre d'utilisation décrite dans la présente PC qu'il peut librement consulter au préalable.

L'ACR gouvernementale dispose d'un droit d'accès et de rectification des données collectées par l'AE de l'IGC/A pour l'émission du certificat ACR et la gestion de son cycle de vie. Ce droit peut s'exercer auprès de l'AE.

Aucune des données à caractère personnel fournies par un porteur ne sera utilisée par l'ACR IGC/A pour une autre utilisation autre que celle définie dans le cadre de la présente PC, sans le consentement du porteur.

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

L'AA de l'IGC/A respecte la législation et la réglementation en vigueur sur le territoire français.

Les informations à caractère personnel communiquées par l'ACR gouvernementale à l'ACR de l'IGC/A ne peuvent être divulguées qu'aux acteurs des services de l'IGC/A ayant besoin d'en connaître.

9.4.6 Autres circonstances de divulgation d'informations personnelles

S'il est nécessaire à l'ACR de l'IGC/A, de divulguer dans d'autres circonstances des informations à caractère personnel, ceci doit se faire avec l'accord exprès de l'ACR gouvernementale concernée.

9.5 Droits sur la propriété intellectuelle et industrielle

Le [CODE_PI] réglemente les droits sur la propriété intellectuelle et industrielle.

Des clauses particulières concernant la propriété des logiciels et matériels utilisés pour l'exécution des services de l'IGC/A sont mentionnées dans la DPC.

Les logos et productions graphiques créées par l'AA de l'IGC/A pour la communication et l'exécution des services de l'IGC/A sont la propriété industrielle de l'AA de l'IGC/A.

Les contributions personnelles des agents aux réalisations graphiques restent leur propriété intellectuelle mais ils cèdent leur droit d'usage à l'AA de l'IGC/A.

Les productions documentaires sont la propriété de l'AA de l'IGC/A.

En cas de modification de la structure de l'AA de l'IGC/A, tous ces droits pourront être transférés à l'entité reprenant les activités de l'AA et de l'ACR de l'IGC/A.

9.6 Interprétations contractuelles et garanties

L'AA de l'IGC/A, du fait du statut du SGDN et des missions de la DCSSI, est responsable de la coordination de la sécurité des systèmes d'information des administrations d'État. Mais chaque ministère reste responsable de la sécurité de ses propres systèmes d'information.

Ainsi, la cohérence et la coordination des différents documents adoptés dans le cadre de l'IGC/A devront être garanties par l'AA de l'IGC/A. Mais l'effectivité de leur mise en place relève de la responsabilité de chaque ministère.

Chaque composante de l'IGC/A est responsable du respect et de l'application des parties de la PC et de la DPC lui incombant, étant noté que l'ACR de l'IGC/A doit avoir communiqué ces informations à la composante concernée. Cependant, il ne s'agit en réalité que d'une distinction fonctionnelle car seule la responsabilité juridique de l'ACR de l'IGC/A pourra être mise en cause par les porteurs et les utilisateurs de certificats.

C'est pourquoi ne sont présentées par la suite que les obligations de l'AA et de l'ACR de l'IGC/A, la DPC précisant les obligations de chacune des composantes (AE, SP, etc.).

L'ACR de l'IGC/A est responsable de toute faute ou négligence, d'elle-même ou de l'une de ses composantes, qui aurait pour conséquence la lecture, l'altération ou le détournement des données à caractère personnel des porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'IGC/A.

L'ACR de l'IGC/A a également un devoir général de surveillance quant à la sécurité et l'intégrité des certificats qu'elle délivre.

En revanche, l'ACR gouvernementale – le porteur du certificat – est responsable de la protection de sa clé privée, de ses données d'activation et de l'accès à sa base de certificats. Il doit informer l'ACR de l'IGC/A de toute modification concernant les informations contenues dans son certificat.

9.6.1 Obligations communes aux ACR gouvernementales et à l'ACR de l'IGC/A

Les obligations communes aux ACR gouvernementales et à l'ACR de l'IGC/A consistent à respecter et appliquer la présente PC, ce qui implique notamment de :

- documenter ses procédures internes de fonctionnement et les tenir à jour ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles l'entité concernée s'engage ;
- accepter les contrôles de conformité effectués par l'équipe d'audit mandatée (cf. chapitre 8), suivre leurs recommandations et remédier aux non-conformités qu'ils révèleraient ;
- 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'ACR et les documents qui en découlent ;
- respecter et appliquer leur DPC respective ;
- apporter les mesures nécessaires et suffisantes à la correction des non-conformités détectées dans les audits, dans les délais préconisés par les auditeurs.

9.6.2 Les obligations de l'AA

Dans le contexte défini au §1.4, les obligations de l'AA de l'IGC/A sont assumées pour la plupart par l'ACR de l'IGC/A. Les obligations spécifiques à l'AA de l'IGC/A sont alors :

- assumer la responsabilité de l'ensemble des composantes de l'IGC/A (ressources matérielles et logicielles et services de l'IGC/A) ;
- décider la révocation du certificat de l'ACR de l'IGC/A et la révocation des certificats d'ACR gouvernementales émis par l'IGC/A conformément au §4.8.3 ;
- prendre la décision de la remise en service de l'IGC/A après un sinistre ou une crise majeure.

9.6.3 Les obligations de l'ACR de l'IGC/A

Les obligations de l'ACR de l'IGC/A sont :

- élaborer et approuver la PC de l'IGC/A ;
- élaborer la DPC de l'IGC/A en conformité avec la présente PC, et l'approuver ;
- faire appliquer dans ses services les règles édictées dans la PC et la DPC, dans les instructions techniques particulières auxquelles la DPC renvoie ;
- constituer la commission l'homologation de l'IGC/A ;

- prononcer la décision d'homologation de l'IGC/A avant sa mise en service, sur l'avis de la commission d'homologation se prononçant au vu du dossier d'homologation préparé par les services concernés de l'IGC/A ;
- définir les exigences minimales devant figurer dans les PC des ACR gouvernementales souhaitant obtenir un certificat de l'IGC/A, sous la forme d'une PC-type ou d'un corpus documentaire couvrant ce besoin ;
- déterminer les qualités et le nombre de personnes affectées à une opération ainsi que la répartition des rôles ;
- décider des sanctions à appliquer, en concertation avec l'AA, lorsqu'un agent abuse de ses droits ou effectue une opération non-conforme à ses attributions ;
- arbitrer les litiges ;
- accepter ou refuser les demandes de certification ;
- accepter ou refuser les demandes de révocation pour les cas identifiés au §4.8.3. ;
- en cas de révocation du certificat d'une ACR gouvernementale émis par l'IGC/A, décider de l'attribution d'un nouveau certificat à cette ACR ;
- participer aux cérémonies de signature et de génération de clés et certificats ;
- prononcer la révocation de l'ACR de l'IGC/A sur décision de l'AA de l'IGC/A ;
- déclarer la cessation d'activité de l'ACR de l'IGC/A.

9.6.4 Les obligations de l'ACR gouvernementale

Les obligations d'une ACR gouvernementale sont :

- faire auditer son IGC selon les exigences définies dans cette PC ;
- respecter les exigences minimales définies par l'ACR de l'IGC/A, pendant, au minimum, la durée de validité du certificat ;
- se conformer aux procédures et instructions particulières publiées par l'ACR de l'IGC/A pour lui adresser ses demandes de certification, de révocation, ou toute autre demande à l'attention de l'IGC/A ;
- assurer l'authenticité, l'exactitude et la complétude des informations transmises à l'AE de l'IGC/A par elle-même et par les autorités auxquelles elle délègue ;
- assurer l'information des autorités et agents auxquelles elle délègue, concernant leurs rôles et responsabilités, et le traitement des informations à caractère personnel ou confidentielles, conformément à la présente PC ;
- publier les LAR de l'IGC/A dans les délais impartis ;
- informer dans les plus brefs délais l'ACR de l'IGC/A de tout événement modifiant ou susceptible de modifier les conditions d'application de la présente PC, notamment pour une cause motivant une révocation, pour que l'ACR de l'IGC/A puisse remplir ses obligations en la matière.

9.7 Limite de garantie

Aucune garantie ne peut-être exigée de l'IGC/A par les ACR gouvernementales ou les utilisateurs de certificats.

9.8 Limite de responsabilité

Une convention ou un protocole d'accord particulier consenti entre les parties (ACR gouvernementale et ACR de l'IGC/A), peut préciser certaines responsabilités complémentaires aux responsabilités exposées ci-après.

A minima, les responsabilités des AA de l'IGC/A et AA gouvernementales sont limitées comme indiqué ci-après.

9.8.1 L'ACR et l'AA de l'IGC/A

La responsabilité de l'AA de l'IGC/A ne peut être engagée qu'en cas de manquement à ses propres obligations ou à celles de l'ACR de l'IGC/A.

La responsabilité de l'AA ou de l'ACR de l'IGC/A, ne pourra valablement être mise en cause par l'ACR gouvernementale, si le préjudice subi par cette dernière résulte d'un manquement à l'une des obligations qui lui incombent dans la présente PC.

L'AA de l'IGC/A ne saurait être tenue pour responsable d'une mauvaise utilisation du certificat de l'ACR gouvernementale ou de tout certificat émanant de l'IGC opérée par l'ACR gouvernementale (ou d'une IGC opérée par l'une de ses AC déléguées).

9.8.2 Les ACR gouvernementales

L'ACR gouvernementale est responsable des préjudices causés par le non respect des obligations lui incombant mentionnées dans la présente PC.

Le non respect de ses obligations engage sa seule responsabilité et non celle de l'AA de l'IGC/A ni celle de l'ACR de l'IGC/A.

Les ACR gouvernementales portent seules la responsabilité de l'application de leurs propres politiques de certification dans leur organisation.

9.9 Indemnités

Sans objet.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

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

La durée de validité de la DPC associée peut être indépendante de la durée de vie de la PC, si la DPC a pris en compte les exigences de plusieurs PC ; dans ce cas elle reste valide jusqu'à la fin de validité des derniers certificats émis selon les PC auxquelles elle se rapporte.

9.10.2 Fin anticipée de validité

L'évolution de la présente PC n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel exigé par l'évolution de l'état de l'art en cryptologie.

9.10.3 Effets de la fin de validité et clauses restant applicables

Les clauses restant applicables au-delà de la fin d'utilisation de la PC, sont celles concernant l'archivage des données. Toutes les autres obligations deviennent caduques et sont remplacées par celles décrites dans la ou les PC encore en vigueur.

9.11 Notifications individuelles et communications entre les participants

Pas d'exigences spécifiques.

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

L'ACR de l'IGC/A révise sa PC et sa DPC à chaque évolution du système et chaque fois qu'une évolution remarquable de l'état de l'art le justifie.

Les corrections typographiques, orthographiques ou grammaticales, ou les modifications de présentation, sont autorisées sans avoir à être notifiées.

Les modifications mineures du texte font l'objet de révisions dont le contenu est porté dans l'historique du document. Seules les modifications majeures font l'objet d'un changement de version. Les modifications sont majeures si elles modifient le niveau de sécurité ou le domaine de confiance, ou les engagements, obligations et responsabilités des acteurs de l'IGC/A.

9.12.2 Mécanisme et période d'information sur les amendements

Les révisions sont signalées par le SP qui publie la PC.

Les nouvelles versions peuvent faire l'objet d'une publicité ciblée auprès des ACR gouvernementales, avant ou après leur publication, et éventuellement d'une plus large publicité par tout moyen jugé pertinent par l'ACR de l'IGC/A en fonction des lecteurs concernés.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

Une nouvelle version majeure de la PC motive l'attribution d'un nouvel identifiant d'objet (OID).

9.13 Dispositions concernant la résolution de litiges

9.13.1 Résolution des litiges sur la revendication d'un nom

Si plusieurs directions au sein d'une même administration revendiquent l'attribution d'un certificat d'ACR pour cette administration, la certification par l'IGC/A ne sera accordée qu'à celle présentant l'accord du membre de la chaîne fonctionnelle de la sécurité des systèmes d'information de plus haut niveau.

Pour tout autre litige portant sur la revendication d'un nom, l'ACR de l'IGC/A ne donnera de suite aux demandes de certification ou de révocation qu'après accord des parties intéressées. Si le litige survient après l'attribution d'un certificat sur la base d'une demande validée par une autorité légitime, le certificat attribué ne pourra être révoqué, si nécessaire, qu'à la demande de l'ACR gouvernementale concernée.

9.13.2 Résolution des litiges autres

En priorité, un compromis est recherché par l'AA de l'IGC/A en vue de résoudre les litiges qui pourraient exister entre elle et une AA, sur la base des responsabilités définies au §9.6.

Les modalités de règlement des litiges intervenant dans le cadre de la sous-traitance d'un ou plusieurs services de l'IGC/A seront définies dans le marché public liant les parties.

9.14 Juridictions compétentes

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

9.15 Conformité aux législations et réglementations

L'environnement législatif pour la mise en œuvre de l'ACR IGC/A est constitué des textes de lois et règlements mentionnés dans l'ANNEXE 2 : Références bibliographiques, principalement les suivants :

- l'article 1316 du Code Civil relatif à la signature électronique [CC1316] ;
- la loi n° 2004-575 du 21 juin 2004 modifiée, pour la confiance dans l'économie numérique [LCEN] ;
- la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés [LCNIL] ;
- l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives [ORD05-1516] ;
- le décret n° 2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique [DEC01-272] ;
- le titre III / chapitre 2 / section 1 du code de la défense, relatif aux compétences du secrétaire général de la défense nationale dans le domaine de la sécurité des systèmes d'information ;
- le décret n° 2001-693 du 31 juillet 2001 créant au secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information [DEC2001-693], consolidé le 4 mai 2007.

Les instructions générales interministérielles, les instructions interministérielles, les directives et recommandations citées à l'ANNEXE 2 : Références bibliographiques, précisent les contraintes et mesures associées à ce contexte.

9.16 Dispositions diverses

9.16.1 Accord global

Les éventuels accords passés avec les partenaires doivent être validés par l'AA de l'IGC/A, ou l'ACR de l'IGC/A si elle en reçoit l'accord de l'AA de l'IGC/A.

9.16.2 Transfert d'activités

Se référer au §5.8.

9.16.3 Conséquences d'une clause non valide

Les conséquences, le cas échéant, seront traitées en fonction de la législation en vigueur.

9.16.4 Application et renonciation

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

9.16.5 Force majeure

Sont considérés comme cas de force majeure les cas habituellement retenus par les tribunaux français, respectant la définition suivante : événement irrésistible et imprévisible qui, provenant d'une cause extérieure au débiteur d'une obligation ou à l'auteur d'un dommage, le libère de son obligation ou l'exonère de sa responsabilité (cf. [Vocab_jurid]).

9.17 Autres dispositions

La présente PC ne formule pas d'exigence spécifique supplémentaire.

ANNEXE 1 : Glossaire

Termes juridiques :

Autorité – (selon [Vocab_jurid]) 1 – pouvoir de commander appartenant aux gouvernants et à certains agents publics ; 2 – organe investi de ce pouvoir.

Termes techniques généralement employés dans le cadre d'une infrastructure de gestion de clés :

Autorité d'horodatage – Autorité responsable de la gestion d'un service d'horodatage.

Autorité administrative (AA) – voir paragraphe 1.4 Acteurs et utilisateurs concernés par l'IGC/A.

Autorité de certification (AC) -. Autorité chargée de créer et d'attribuer les certificats.

Autorité de certification racine (ACR) – voir paragraphe 1.4 Acteurs et utilisateurs concernés par l'IGC/A.

Autorité d'enregistrement (AE) – voir paragraphe 1.4 Acteurs et utilisateurs concernés par l'IGC/A.

Bi-clé – Une bi-clé est un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptologie basée sur des algorithmes asymétriques. Quatre types de bi-clés interviennent dans une infrastructure de gestion de clés (signature, certification, d'échange de clés ou de transport de clés et confidentialité).

Certificat électronique – Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente PC Type, le terme « certificat électronique » désigne uniquement un certificat délivré à une personne physique et portant sur une bi-clé d'authentification, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

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

Contrôle de conformité – Action qui consiste à réaliser un examen le plus exhaustif possible afin de vérifier l'application stricte des procédures et de la réglementation au sein d'un organisme.

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, en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Domaine de certification : chemin constitué d'une chaîne de certificats d'AC (la signature du certificat d'une AC est vérifiée en utilisant le certificat de l'AC signataire et ainsi de suite). Un domaine de certification peut être contraint par des restrictions liées au nommage, aux politiques de certification ou à la longueur maximale du chemin.

Données d'activation : données privées associées à un utilisateur final permettant de mettre en œuvre sa clé privée.

Données d'identification : données privées permettant d'identifier un porteur de certificat et d'attester de son habilitation à représenter l'utilisateur final de ce certificat.

Enregistrement – Action qui consiste pour une autorité d'enregistrement à éditer le profil d'un demandeur de certificat, conformément à une PC.

Génération d'un certificat – Action réalisée par une AC et qui consiste à signer le gabarit d'un certificat édité par une AE, après avoir vérifié la signature de l'AE

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 plate-forme de certification, d'une plate-forme d'enregistrement centralisée et/ou locale, d'un service d'archivage, d'un service de publication, etc.

Journalisation : Fait d'enregistrer dans un fichier dédié à cet effet certains types d'événements provenant d'une application ou du système d'exploitation d'un poste informatique. Le fichier résultant rend possible la traçabilité et l'imputabilité des opérations effectuées.

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 porteurs et les utilisateurs de certificats.

Porteur de certificat : individu qui possède, en propre ou pour le compte d'une personne morale, une bi-clé et son certificat associé, ainsi que les moyens d'activer la bi-clé.

Prestataire de services de certification électronique (PSCE) – Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (ACRs / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ « issuer » du certificat.

Produit de sécurité – Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Publication d'un certificat – Fait de mettre un certificat à disposition d'utilisateurs susceptibles d'avoir à vérifier une signature ou à chiffrer des informations.

Qualification des produits de sécurité – Acte par lequel la DCSSI atteste du niveau de sécurité d'un produit de sécurité en s'appuyant sur le schéma français d'évaluation et de certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, schéma défini par le décret [DEC02-535].

Renouvellement de certificat – Action effectuée à la demande d'un utilisateur final ou en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour un porteur. La re-génération de certificat après révocation n'est pas un renouvellement.

Révocation de certificat – Action demandée par une AC, une AE, une TPC, le porteur de certificat ou son autorité de sécurité, et dont le résultat est la suppression de la caution de l'AC sur un certificat donné, avant la fin de sa période de validité. Cette action peut être la conséquence de différents types d'événements tels que la compromission d'une clé, le changement d'informations contenues dans un certificat, etc. L'action de révocation peut consister soit à publier une liste des certificats révoqués, soit à mettre à la disposition des utilisateurs un serveur pouvant indiquer l'état révoqué ou non d'un certificat.

Service de Publication – Le service de publication (SP) rend disponible les certificats de clés publiques émis par une AC, à l'ensemble des utilisateurs potentiels de ces certificats. Il publie une liste de certificats reconnus comme valides et une liste de certificats révoqués (LCR) et/ou une liste des certificats d'AC Révoqués (LAR). Ce service peut être rendu par un annuaire (par exemple, de type X500), un serveur d'information (Web), une délivrance de la main à la main, une application de messagerie, etc.

ANNEXE 2 : Références bibliographiques

1.1 Réglementation

[CC1316]	Code Civil – article 1316 relatif à la signature électronique
[LCEN]	Loi n°2004-575 du 21 juin 2004 modifiée, pour la confiance dans l'économie numérique
[LCNIL]	Loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés
[ORD05-1516]	Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
[DEC01-272]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique
[DEC07-584]	Décret n°2007-584 du 23 avril 2007 relatif à certaines dispositions réglementaires de la première partie du code de la défense (Décrets en conseil des ministres)
[DEC01-693]	Décret n°2001-693 du 31 juillet 2001 créant au secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information
[DEC02-535]	Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information
[IGI1300]	Instruction générale interministérielle sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'État n°1300 / SGDN / SSD du 25 août 2003
[IGI900]	Instruction générale interministérielle sur la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées n°900/SGDN/SSD/DR ou n°900/DISSI/SCSSI/DR du 20 juillet 1993
[II910]	Instruction interministérielle sur les articles contrôlés de la sécurité des systèmes d'information n°910/SGDN/SSD/DR – n°910/DISSI/SCSSI/DR du 19 décembre 1994
[II300]	Instruction interministérielle sur la protection contre les signaux parasites compromettants n°300 / SGDN / TTS / SSI / DR du 21 juin 1997
[DIR911]	la directive relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), n°911 / DISSI / SCSSI / DR du 20 juin 1995
[R901]	Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense n°901/DISSI/SCSSI du 2 mars 1994

1.2 Documents techniques

[PRIS]	Politique de référencement intersectorielle de sécurité version 2.0
[PP_AC]	Profil de protection AC (PPnc/0006) Cf. www.ssi.gouv.fr

[PP_AE]	Profil de protection AE (PPnc/0005) Cf. www.ssi.gouv.fr
[R-ALGO]	Mécanismes cryptographiques – Règles et recommandations – version 1.10 du 19 décembre 2006
[R-IGC]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard ou renforcé – version 1.0 du 13 mars 2006
[QUALIF_STD]	Processus de qualification standard, DCSSI, version 1.0 du 28/07/2003 n° 1591/SGDNDCSSI/SDR
[X509]	Information Technology – Open Systems Interconnection – The Directory : Public-key and attribute certificate frameworks, Recommendation X.509, version de mars 2000 (complétée par les correctifs techniques n°1 d'octobre 2001, n°2 d'avril 2002 et n°3 d'avril 2004) de l'ITU (International Telecommunication Union)
[X500]	Information Technology – Open Systems Interconnection – The Directory : Overview of concepts, models and services, Recommandation X500 de février 2001 de l'ITU
[RFC2247]	Using Domains in LDAP/X.500 Distinguished Names – utilisation des noms de domaines Internet pour les noms disctinctifs de type annuaire LDAP
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework – Modèle de politique de certification et de déclaration des pratiques de certification
[RFC3739]	IETF - Internet X.509 Public Key Infrastructure, Qualified Certificates Profile, RFC 3726 03/2004 – profils des certificats qualifiés.
[RFC5280]	IETF – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – profils de certificats et de listes de certificats révoqués d'infrastructure de clés publiques, RFC 5280 de mai 2008
[7498-2]	ISO/IEC 7498-2 (1989) - « Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2 : Architecture de sécurité »
[guide_audit_ACR]	Guide d'audit des autorités de certification racine de la DCSSI – OID :
[guide_rédaction_ACR]	Guide de rédaction des politiques de sécurité et déclarations des pratiques de certification des autorités de certification racine, de la DCSSI – OID :

1.3 Documents Divers

[Vocab_jurid]	Vocabulaire juridique – publié sous la direction de Gérard Cornu, association Henri Capitant, 7ème édition mise à jour « Quadrige » de juin 2005, Presses Universitaires de France.

ANNEXE 3 : Règles de répartition des rôles

Les détenteurs de secret sont des personnels habilités de l'ACR de l'IGC/A.

Un détenteur de secret ne peut pas être ingénieur système, ni auditeur.

Un auditeur ne peut pas être également un ingénieur système.

Un responsable de sécurité ne peut pas être opérateur de signature.

Un responsable de sécurité ne peut être opérateur d'AE ni AE.

Le maître de cérémonie peut être un opérateur d'AE ou l'AE, un ingénieur système ou un auditeur. Il peut aussi être un porteur, qui de préférence n'intervient alors pas pendant la cérémonie comme porteur de secret.

ANNEXE 4 : Définition des variables de temps Var_Temps

Variable	Description	Entité concernée	Durée / fréquence
F_CLE	Fréquence moyenne de publication d'une nouvelle bi-clé par l'IGC/A.	ACR de l'IGC/A	6 ans (ou valeur de la formule indiquée au §5.6.1)
F_CONFORM	Fréquence des contrôles de conformité.	ACR et composantes de l'IGC/A ACR gouvernementale	1 an 3 ans
F_JOURNX	Fréquence de contrôle des journaux d'événements.	ACR de l'IGC/A SP	A chaque certification Au moins une fois par semaine
F_MAJ_LAR	Fréquence de mise à jour des listes de certificats d'autorités révoqués = temps séparant les dates de début de validité de deux LAR non urgentes successives.	ACR et SP de l'IGC/A	1 mois
F_TEST_PLAN	Fréquence des tests du plan anti-sinistre.	ACR et composantes de l'IGC/A	3 ans
T_A _JOURNX	Durée de conservation des archives de journaux d'événements.	ACR et composantes de l'IGC/A	1 mois sur le site jusqu'à la fin de vie de l'IGC/A sur le site de rétention des archives
T_A_CERT	Durée de conservation des archives de certificats.	ACR de l'IGC/A	Jusqu'à la fin de vie de l'IGC/A sur le site de rétention des archives
T_ARCHIVES	Période de rétention des archives (autres que les certificats et les journaux d'événements).	ACR et composantes de l'IGC/A	Jusqu'à la fin de vie de l'IGC/A sur le site de rétention des archives
T_CHG_KEY	Période avant laquelle une entité annonce le renouvellement de sa bi-clé.	ACR et composantes de l'IGC/A	3 mois
T_DISPO_PUB	Temps représentant les conditions de disponibilité du service de publication.	SP de l'IGC/A	Cf. DPC

Variable	Description	Entité concernée	Durée / fréquence
F_CLE	Fréquence moyenne de publication d'une nouvelle bi-clé par l'IGC/A.	ACR de l'IGC/A	6 ans (ou valeur de la formule indiquée au §5.6.1)
T_INFO_CRISE	Délai maximum accepté pour déclarer tout événement grave affectant une IGC et motivant une révocation	ACR de l'IGC/A ACR gouvernementale	24 heures
T_INFO_NU	Délai maximum accepté pour déclarer un événement motivant une révocation non urgente avant la publication de la LAR suivante	ACR de l'IGC/A ACR gouvernementale	15 jours
T_MAX_ACR	Délai maximum pris par l'ACR pour notifier l'acceptation ou le rejet d'une demande à l'appui des justificatifs nécessaires transmis par ses services	ACR de l'IGC/A	6 mois
T_MAX_AE	Délai maximum pris par l'AE pour la transmission des accusés de réception des demandes et la saisine des services IGC/A concernés	AE	2 semaines
T_MAX_AUDIT	Délai maximum de rédaction des conclusions d'audit, mesuré entre la date d'accusé de réception de la demande de certification, et la transmission officielle du rapport d'audit à l'ACR de l'IGC/A.	Service Audit	6 mois
T_PUB_LAR	Délai de publication d'une nouvelle LAR depuis sa date de début de validité	SP de l'IGC/A	3 jours
T_RECOUV_LAR	Délai de recouvrement entre la date de début de validité d'une LAR et la date de fin de validité de la LAR précédente	SP de l'IGC/A ACR gouvernementales	5 jours
T_REVOC_PUB	Délai de fonctionnement du service de publication après la révocation de l'ACR de l'IGC/A.	SP de l'IGC/A	6 mois
T_FIN_VIE	Délai minimum entre l'annonce de la fin de l'activité d'une composante d'IGC et sa fin de vie effective.	ACR et composantes de l'IGC/A ACR gouvernementale	3 mois 3 mois

Variable	Description	Entité concernée	Durée / fréquence
F_CLE	Fréquence moyenne de publication d'une nouvelle bi-clé par l'IGC/A.	ACR de l'IGC/A	6 ans (ou valeur de la formule indiquée au §5.6.1)
T_INVALID	Date à laquelle la clé privée est susceptible d'avoir été compromise (elle peut être différente de la date de révocation).	ACR	Selon le cas
T_PUBLI	Temps mis par une AC pour transmettre au service de publication un certificat émis.	ACR de l'IGC/A	Cf. DPC
T_RECUP_ARCH	Durée nécessaire à la récupération des archives, suite à une demande.	ACR et composantes de l'IGC/A	Cf. DPC
T_TESTS	Délais minimum alloué à l'ACR pour effectuer ses tests de fonctionnement avec les certificats de tests qui lui sont transmis par l'AE de l'IGC/A, et pour signaler à cette dernière tout problème rencontré. Sans nouvelles de l'ACR à la fin de ce délai, les tests sont considérés probants.	ACR gouvernementale	3 semaines à défaut d'une mention particulière de l'ACR gouvernementale
T_VALID_CERT	Période de validité d'un certificat délivré par l'IGC/A.	ACR de l'IGC/A ACR gouvernementale	18 ans max 12 ans
T_VALID_CLE PRIVEE	Période d'utilisation de la clé privée pour signer des certificats	ACR de l'IGC/A	9 ans
T_VALID_LAR	Durée de validité d'une LAR	LAR à publication programmée LAR à publication urgente	[F_MAJ_LAR] + 5 jours [F_MAJ_LAR] - [début de validité de la LAR] + 5 jours

ANNEXE 5 : Format des certificats et des LAR

a. Format des certificats auto-signés de l'ACR de l'IGC/A

Les certificats de l'IGC/A certifiant les clés RSA-2048 et DSA-1024 sont de la forme :

Identification des champs de base du certificat IGC/A	**Champs de bases des certificats RSA-2048 et DSA-1024 de l'IGC/A**
Bloc des données à signer	
Version	« 2 » (pour Version 3)
Numéro de série	Unicité garantie par l'IGC/A.
Algorithme de signature	SHA-1 RSA ou SHA-1 DSA
Émetteur	E = igca@sgdn.pm.gouv.fr CN = IGC/A OU = DCSSI O = PM/SGDN L = Paris S = France C = FR
Valide à partir du	Champ « validity/notBefore » au format UTCTime YYMMDDHHMMZ
Valide jusqu'au	Champ « validity/notAfter » au format UTCTime YYMMDDHHMMZ
Objet	E = igca@sgdn.pm.gouv.fr CN = IGC/A OU = DCSSI O = PM/SGDN L = Paris S = France C = FR
Clé publique	Champ « algorithm » indiquant l'OID de l'algorithme auquel est dédiée la clé publique du porteur (RSA 2048 ou DSA 1024). Champ « subjectPublicKey » contenant la valeur de la clé publique au format BIT STRING. Les champs « issuerUniqueIdentifier » et « subjectUniqueIdentifier » ne sont pas utilisés.
Identification des extensions du certificat IGC/A	**Contenu des extensions du certificat de l'IGC/A**
Utilisation de la clé publique	Non-répudiation, Signature du certificat, Signature de la liste de révocation de certificats hors connexion, Signature de la liste de révocation de certificats.

	Extension non critique.
Stratégie de certificat / Politiques de certification	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.121.1.1.1
Identificateur de la clé du sujet	Par exemple : A3 05 2F 18 60 50 C2 89 0A DD 2B 21 4F FF 8E 4E A8 30 31 36
Identificateur de la clé de l'autorité	Le même que l'identificateur de la clé du sujet. Dans cet exemple : ID de la clé=A3 05 2F 18 60 50 C2 89 0A DD 2B 21 4F FF 8E 4E A8 30 31 36
Contraintes de base	Extension critique : Type d'objet=Autorité de certification Contrainte de longueur de chemin d'accès=Aucun(e)
Fin du bloc de données à signer	
Algorithme de signature	Algorithme utilisant la clé publique du porteur. Champ « algorithm » : sha1 Le champ « parameters » n'est pas utilisé
Valeur de la signature	Champ « signatureValue » : contient une signature numérique calculée à partir du codage ASN.1DER de la structure tobeSigned (bloc des données à signer) Le code ASN.1 DER de cette structure est utilisé comme une entrée de la fonction de signature. La valeur de cette signature est ensuite encodée en ASN.1 comme un « BIT STRING » et incluse dans le champ de signature du certificat.

Les certificats de l'IGC/A certifiant des clés RSA-4096 doivent être de la forme :

Identification des champs de base du certificat IGC/A	**Champs de bases des certificats RSA-4096 de l'IGC/A**
Bloc des données à signer	
Version	« 2 » (pour Version 3)
Numéro de série	Unicité garantie par l'IGC/A.
Algorithme de signature	SHA-256 RSA
Émetteur	Nom distinctif de l'ACR de l'IGC/A, conforme aux règles applicables aux ACR
Valide à partir du	Champ « validity/notBefore » au format UTCTime YYMMDDHHMMZ
Valide jusqu'au	Champ « validity/notAfter » au format UTCTime YYMMDDHHMMZ
Objet	Nom distinctif de l'ACR de l'IGC/A, conforme aux règles applicables aux ACR
Clé publique	Champ « algorithm » indiquant l'OID de l'algorithme auquel est dédiée la clé publique du porteur (RSA 4096).

	Champ « subjectPublicKey » contenant la valeur de la clé publique au format BIT STRING. Les champs « issuerUniqueIdentifier » et « subjectUniqueIdentifier » ne sont pas utilisés.
Identification des extensions du certificat IGC/A	**Contenu des extensions des certificats RSA-4096 de l'IGC/A**
Utilisation de la clé publique	Non-répudiation, Signature du certificat, Signature de la liste de révocation de certificats hors connexion, Signature de la liste de révocation de certificats. Extension non critique.
Stratégie de certificat / Politiques de certification	[1]Stratégie du certificat : identifiant d'objet (OID) de la PC de l'IGC/A régissant l'émission du certificat et son utilisation. Par exemple : Identificateur de stratégie=1.2.250.1.121.1.1.2 Non critique. Les qualificateurs optionnels « CPS pointer » et « user Notice » ne doivent pas être renseignés.
Identificateur de la clé du sujet	Par exemple : A3 05 2F 18 60 50 C2 89 0A DD 2B 21 4F FF 8E 4E A8 30 31 36
Identificateur de la clé de l'autorité	Le même que l'identificateur de la clé du sujet. Dans cet exemple : ID de la clé=A3 05 2F 18 60 50 C2 89 0A DD 2B 21 4F FF 8E 4E A8 30 31 36
Contraintes de base	Extension critique : Type d'objet=Autorité de certification Contrainte de longueur de chemin d'accès=Aucun(e)
Point de distribution des listes de certificats révoqués	Pas de point de distribution indiqué. Le nom de fichier de la LAR publiée par l'IGC/A est « igca.crl ».
Fin du bloc de données à signer	
Algorithme de signature	Algorithme utilisant la clé publique du porteur. Champ « algorithm » : SHA-256 Le champ « parameters » n'est pas utilisé
Valeur de la signature	Champ « signatureValue » : contient une signature numérique calculée à partir du codage ASN.1DER de la structure tobeSigned (bloc des données à signer) Le code ASN.1 DER de cette structure est utilisé comme une entrée de la fonction de signature. La valeur de cette signature est ensuite encodée en ASN.1 comme un « BIT STRING » et incluse dans le champ de signature du certificat.

Les certificats de l'IGC/A utilisant des courbes elliptiques pourront comporter d'autres extensions, qui seront indiquées dans une révision de la présente PC.

b. Format des certificats des ACR gouvernementales

Les certificats auto-signés ou les requêtes de certification des ACR gouvernementales transmis à l'ACR de l'IGC/A doivent avoir un format conforme à [X509] et [RFC5280].

Le format des certificats délivrés en retour par l'IGC/A inclut les champs de base et extensions obligatoires ci-après ; il tiendra compte également des extensions contenues dans la requête ou le certificat auto-signé, mais n'attribuera de statut critique qu'à celles mentionnées dans le gabarit suivant :

Champs de base *(nom du champ précisé en anglais)*		
Champ	**Valeur**	**Indications pour renseigner ce champ**
Version *(Version)*	2	La valeur 2 correspond à la version 3 de la norme [X509].
Numéro de série *(Serial number)*	Attribué par l'IGC/A.	Le numéro de série du certificat est une valeur entière. Il identifie de manière unique les certificats émis par l'IGC/A.
Algorithme de signature utilisé par l'AC avec sa bi-clé *(Algorithm)*	DSA 1024 avec SHA-1 RSA 2048 avec SHA-1 RSA 4096 avec SHA-256	Cette structure, composée de la structure algorithmIdentifier, donne des informations sur l'algorithme de signature et la fonction de hachage utilisés par l'ACR de l'IGC/A pour signer le certificat.
Sujet / Objet *(Subject)*	Le nom distinctif contenu dans le certificat auto-signé ou la requête de certification de l'ACR.	Il est primordial que le nom distinctif soit le même que celui employé par l'ACR dans le champ nom distinctif de l'émetteur des certificats qu'elle délivre. Le nom distinctif doit vérifier les conditions décrites ci-après.
Emetteur *(Issuer)*	Attribué par l'IGC/A	Ce champ contient le nom distinctif de l'ACR de l'IGC/A, tel que mentionné dans le certificat de la clé publique de l'IGC/A utilisée pour la signature du présent certificat.
Valide à partir du **Valide jusqu'à** *(Validity)*	Dates de validité au format UTCTime.	Cette structure est composée des champs notBefore et notAfter. Elle précise la période de validité du certificat. La date de début de validité est la date du jour de la cérémonie de signature du certificat. La date de fin est déterminée par la valeur la plus petite entre : [Date de fin de validité du certificat autosigné ou de la requête de certification de l'ACR gouvernementale] et [Date de début de validité du certificat de l'ACR de l'IGC/A + [T_UTIL_KPRIV] de l'ACR de l'IGC/A].

Clé publique *(Subject Public Key Info)*	Les valeurs actuellement possibles sont : DSA 1024 RSA 2048 RSA 4096	Cette structure est composée des champs de la structure algorithmIdentifier (« algorithm », « parameters »), qui spécifie l'algorithme qui utilise la clé publique du porteur, et «subjectPublicKey » qui contient le train de bits de la clé publique.
Identificateur unique de l'émetteur *(Issuer Unique Identifier)*	Ne doit pas être utilisé.	La [RFC5280] déconseille l'utilisation de ce champ.
Identificateur unique du sujet *(Subject Unique Identifier)*	Ne doit pas être utilisé.	La [RFC5280] déconseille l'utilisation de ce champ.

Extensions obligatoires *(nom du champ précisé en anglais)*			
Champ	**Valeur**	**Criticité**	**Indications**
Utilisations de la clé *(Key usage)*	La valeur présente dans le certificat ou la requête de certification de l'ACR. Au minimum l'usage « Signature du certificat » doit être mentionné.	Critique	Les deux valeurs suivantes ne devraient être mentionnées que si la clé publique de l'ACR est utilisée pour la vérification de la signature d'autres objets que les certificats et listes de certificats révoqués : digitalSignature : pour vérifier les signatures numériques dont les buts sont autres que la non-répudiation, la signature de certificats ou de LAR. nonRepudiation : pour vérifier les signatures numériques utilisées afin de fournir un service de non-répudiation qui protège contre le fait qu'un signataire puisse nier avoir commis une action (dans un contexte autre que la signature de certificats ou de LAR).
Identifiant de clé d'autorité *(Authority Key Identifier)*	valeur du champ « SubjectKeyIdentifier » du certificat de l'ACR de l'IGC/A.	Non critique	Seul le champ « keyIdentifier » sera utilisé, avec la valeur du champ « SubjectKIdentifier » du certificat de l'ACR de l'IGC/A.
Identifiant de la clé du sujet *(Subject Key Identifier)*	valeur du champ « identifiant de la clé du sujet » du certificat auto-signé ou de la requête de certification de l'ACR objet du certificat.	Non critique	Valeur unique dérivée de la clé publique ou d'une méthode de génération de valeur unique.
Politiques de certification / stratégies de certificat *(Certificate policies)*	Identificateur de politique = toutes les politiques (AnyPolicy).	Non critique	Cette séquence, donne une liste de politiques de certification qui s'appliquent au certificat. Ces politiques sont reconnues par l'autorité de certification.

Contraintes de base *(Basic Constraints)*	CA = 1 (type d'objet = Autorité de certification) Pour les ACR gouvernementales : pathLenConstraint = Contrainte de longueur de chemin d'accès = aucune	Critique	CA : booléen indiquant si ce certificat peut être utilisé pour vérifier des signatures de certificat, autrement dit si le porteur de certificat peut se comporter comme une AC ou non. pathLenConstraint : Ce champ donne le nombre maximal de certificats d'AC qui peuvent suivre ce certificat dans un chemin de certification. Lorsque ce nombre vaut 0, cela signifie que l'AC ne peut générer de certificats que pour des utilisateurs finaux.
Point de distribution des listes de certificats révoqués *(CRL Distribution Point)*	Chemin de téléchargement des LAR communiqué par l'ACR dans sa demande.	Non critique	Le nom de fichier de la LAR est imposé : « igca.crl » (attention au respect des minuscules).

Fin du bloc de données à signer		
Champ	**Valeur**	**Indications pour renseigner ce champ**
Algorithme d'empreinte numérique *(AlgorithmIdentifier)*	Algorithm : OID de l'algorithme utilisé pour signer le certificat. Parameters : non utilisé, dans la mesure où les paramètres de l'algorithme utilisé pour signer le certificat ont déjà été mentionnés plus haut.	Cette séquence est composée des champs « algorithm » et « parameters ». Elle spécifie l'algorithme qui utilise la clé publique du porteur. A ce niveau, les informations sur l'algorithme utilisé pour signer le certificat ne sont pas protégées, contrairement aux informations sur l'algorithme définies plus haut qui, elles, sont signées. Aucune vérification n'est requise pour vérifier la cohérence de l'information non protégée et l'information protégée. Pour vérifier un certificat, le système de vérification doit utiliser l'algorithme mentionné dans le bloc de données à signer.
Empreinte numérique *(signatureValue)*		Ce champ contient une signature numérique calculée à partir du codage ASN.1 DER de la structure tobeSigned (bloc de données à signer). Le code ASN.1 DER de la structure tobeSigned est utilisé comme une entrée pour la fonction de signature. La valeur de cette signature est ensuite encodée en ASN.1 comme un « BIT STRING » et incluse dans le champ de signature du certificat.

Traitement des autres extensions

Si d'autres extensions sont présentes dans la requête de certification ou le certificat auto-signé de l'ACR, elles seront reprises dans le certificat délivré par l'IGC/A, à condition de respecter les indications portées dans le tableau suivant.

Autres extensions	
Utilisation de clé étendue *(Extended Key usage)*	Valeur présente dans la requête de certification ou le certificat auto-signé de l'ACR. Non critique.
Durée d'utilisation de clé privée *(Private Key usage period)*	Usage déconseillé. Valeur présente dans la requête de certification ou le certificat auto-signé de l'ACR. Non critique.
Mappage de politiques *(Policy mappings)*	Ne doit pas être utilisé.
Autre nom de sujet *(Subject Alternative Name)*	Valeur présente dans la requête de certification ou le certificat auto-signé de l'ACR. Non critique.
Autre nom d'émetteur *(Issuer Alternative Name)*	Ne doit pas être utilisé.
Attributs d'annuaire du sujet *(Subject Directory Attributes)*	Valeur présente dans la requête de certification ou le certificat auto-signé de l'ACR. Non critique.
Contraintes de nom *(Name Constraints)*	Valeur présente dans la requête de certification ou le certificat auto-signé de l'ACR. Non critique. NameConstraintsSyntax : Ce champ, qui ne peut être utilisé que dans les certificats d'AC, indique un espace de noms auquel doivent appartenir tous les noms de sujet figurant dans les certificats suivants d'un chemin de certification. permittedSubtrees : Définit le sous-arbre d'une hiérarchie de nommage à l'intérieur duquel l'AC a le droit d'émettre des certificats. GeneralSubtree : base - Précise le type de nom utilisé comme repère pour la hiérarchisation du domaine de certification. ExcludedSubtrees : Définit le sous-arbre d'une hiérarchie de noms à exclure.
Contraintes de politique *(Policy Constraints)*	Ne doit pas être utilisé. Ce champ requiert l'identification d'une politique de certificat explicite, et/ou inhibe la possibilité d'utiliser le croisement de politique dans un chemin de certification.
Inhibition de la valeur spéciale "toute politique" *(Inhibit Any policy)*	Ne doit pas être utilisé.

Liste CRL la plus récente *(Freshest CRL)*	Ne doit pas être utilisé.
Autres extensions possibles	Selon spécificités de l'ACR, et au choix de l'ACR de l'IGC/A. Non critique par principe.

c. Règles concernant le nom distinctif (DN)

Le DN qui se trouve dans le champ « Objet » d'un certificat d'ACR doit être conforme aux exigences des chapitres 3.1.1 de [RFC3739], ainsi qu'aux exigences supplémentaires suivantes, qui ne s'appliquent que sur les nouveaux certificats (nouvelles ACR et renouvellement de certificats d'ACR existantes). Ces exigences n'exigent pas le renouvellement anticipé des certificats d'ACR générés préalablement à la publication de la présente PC qui seraient non conformes.

Le DN doit comporter un sous-ensemble des attributs suivants, dont certains obligatoires :

Nom des attributs	Contrainte d'utilisation	Commentaires / Informations normatives
domainComponent	Facultatif	Se conformer au standard [RFC2247]
countryName	Obligatoire	FR pour France
stateOrProvinceName	Facultatif	N'est pas utilisé pour les ACR gouvernementales.
organizationName	Obligatoire	Doit contenir le nom officiel complet – à la date d'émission du certificat - de l'AA pour le compte de laquelle œuvre l'ACR. Pour les administrations de l'État, ce nom peut être : • soit le nom du ministère au service duquel l'AA est attachée, tel que défini au journal officiel de la République française, • soit le nom commun de l'AA, qui peut être abrégé au secteur d'activité de l'AA (ex. : « O=Gendarmerie nationale » pour la direction générale de la gendarmerie nationale). Il est recommandé de ne pas utiliser d'acronyme, sauf s'ils sont officiels et que la chaîne de caractères du nom officiel complet dépasse 40 caractères.
organizationalUnitName	Recommandé	Doit contenir l'identification de l'AA structurée conformément à la norme ISO 6523 : du type ICD du numéro SIREN / SIRET (0002), suivi d'un espace et de 9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET. Si d'autres instances de l'attribut organizationalUnitName sont présentes, elles ne doivent pas commencer par 4 chiffres.
localityName	Facultatif	
SerialNumber	Facultatif	
CommonName	Recommandé	Doit contenir le nom commun de l'ACR.

EmailName	Déconseillé	En raison du caractère éphémère des adresses de messagerie, il est déconseillé d'utiliser cette extension.

d. Format des listes d'autorités révoquées émises par l'IGC/A

Les listes d'autorités révoquées (LAR) émises par l'IGC/A doivent avoir un format conforme au standard [RFC5280].

Nom des Champs	Valeur	Commentaires / Informations normatives
Bloc des données à signer		
Version	« 1 » indiquant la version 2.	
Émetteur	DN du certificat de l'IGC/A certifiant la clé signataire des certificats d'autorités révoqués dans cette LAR.	
Date d'effet		
Prochaine mise à jour	Date d'effet + [F_MAJ_LAR]	
Algorithme de signature	RSA-SHA1	
Identificateur de la clé de l'autorité	Champ identique à celui du certificat de l'IGC/A certifiant la clé signataire des certificats d'autorités révoqués dans cette LAR	
Certificats révoqués	Liste de couples de valeurs : « Numéro de série du certificat » et « date de révocation par l'AC »	La date de révocation ne peut être qu'antérieure ou identique à la date de la signature de la liste. Elle n'a de sens que si elle est antérieure à la fin de validité initialement indiquée dans le certificat.
Numéro de série		Indique le numéro de la LAR.
Code de la cause de la révocation	NON UTILISE.	

ANNEXE 6 : modalités de vérification des certificats de l'IGC/A et conditions de leur intégration dans les produits de communication

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Paris, le 22 janvier 2007

MODALITÉS DE VÉRIFICATION DES CERTIFICATS DE L'IGC/A ET CONDITIONS DE LEUR INTÉGRATION DANS LES PRODUITS DE COMMUNICATION

Les certificats de l'IGC/A sont publics ; ils peuvent être intégrés par tout éditeur d'outil de communication électronique ou par tout responsable ou usager de téléservices de l'administration, sous réserve de l'acceptation des dispositions suivantes :

- la personne qui télécharge les certificats de l'IGC/A s'engage à respecter la finalité de ces certificats, à savoir la vérification de la validité des « certificats racines » de la chaîne de certification dans les échanges avec les administrations ;
- la personne reconnaît télécharger et intégrer les certificats de l'IGC/A sous sa seule et exclusive responsabilité ;
- le SGDN décline toute responsabilité en cas de défaut de téléchargement ou d'intégration de ces certificats, ainsi que d'une mauvaise utilisation des certificats intégrés.

La diffusion des certificats de l'IGC/A sur des sources de références officielles multiples et utilisant des technologies différentes permet aux éditeurs et aux usagers de contrôler le contenu des certificats qu'ils utilisent, en comparant les diverses sources disponibles :

- l'avis publié au Journal officiel de la République française, édition n°41 du 17 février 2007, sous le numéro NOR : PRMX0710016V, consultable sur le site du J.O. électronique authentifié ou sur le site http://www.legifrance.gouv.fr/;
- le site Internet de la direction centrale de la sécurité des systèmes d'information : http://www.ssi.gouv.fr/fr/igca/accueil_igca.html.

Lorsqu'il intègre le certificat de l'IGC/A dans un produit de télécommunication, tout éditeur engage sa responsabilité s'il n'a pas contrôlé la conformité et l'intégrité de ce certificat par les moyens mis en œuvre par le SGDN. Il sera dans ce cas seul responsable des dommages à ses clients qui pourraient survenir du fait de l'intégration d'un certificat erroné.

Pour tout renseignement complémentaire, contacter la DCSSI aux coordonnées suivantes :

Direction centrale de la sécurité des systèmes d'information
Bureau Conseil
51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP
Télécopie : 01.71.75.84.20 - Courriel : igca@sgdn.gouv.fr