Secrétariat général
de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction Opérations
Bureau Conseil

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

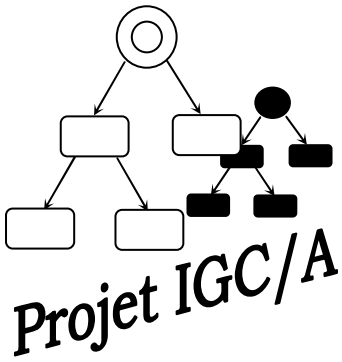
PREMIER MINISTRE

IGC/A

POLITIQUE DE CERTIFICATION

DE L'INFRASTRUCTURE DE GESTION DE LA CONFIANCE DE L'ADMINISTRATION

Version	:	1.1revA
Référence	:	N° 903/SGDN/DCSSI/SDO/BCS/
Date d'approbation	:	20/04/2007
Nombre de pages	:	56



Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Adresse postale :
51, boulevard de La Tour Maubourg
75700 PARIS - 07 SP

Historique des modifications

Version	Date	Objet de la modification	Auteur(s)	Statut
0.1	05/07/01	Création du document.	DCSSI/SDO/ BCS	Ébauche
1.1	16/07/02	OID officiel : 1.2.250.1.121.1.1.1	BCS	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	BCS	Validé par le Directeur central de la sécurité des systèmes d'information Le 20/04/2007

Sommaire

1 INTRODUCTION

1.1 Présentation générale

Cette politique de certification est utilisée dans le cadre de la certification des autorités de certification des administrations de l'Etat français par la direction centrale de la sécurité des systèmes d'information rattachée au secrétariat général de la défense nationale (notée par la suite SGDN/DCSSI). Elle définit les objectifs de sécurité pour le processus de certification à l'aide de l'Infrastructure de Gestion de la Confiance de l'Administration « IGC/A ». Elle concerne à la fois l'autorité responsable d'application de l'IGC/A et les autorités responsables d'application des administrations de l'État qui souhaitent faire certifier leurs autorités de certification racines par l'autorité de certification racine de l'IGC/A.

La politique de certification initiale (version 1.1) a été élaborée à partir :

- de l'étude IGC FEROS 1.1 dont elle incorpore les objectifs de sécurité,
- du document RFC 2527 qui a servi de canevas.

La version 1.1revA a intégré :

- certaines recommandations de la PRIS v2.0,
- les recommandations de l'étude des « impacts juridiques du déploiement par le SGDN/DCSSI de l'IGC/A phase 2 au profit de toutes les administrations » commandée en 2005 par la DCSSI.

Convention :

Dans la suite du document, le terme :

- « PC » remplace « politique de certification »,
- « DPC » remplace « déclaration de pratiques de certification ».

Par ailleurs, l'expression « autorités de certification étatiques » fait référence aux autorités de certification des administrations de l'Etat français certifiées par l'IGC/A ou demandant à l'être, appartenant au périmètre défini au § 1.3.2 Applications concernées.

1.2 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 1.2.250.1.121.1.1.1.

1.3 Acteurs de l'IGC/A et application de la politique

1.3.1 Les acteurs de l'IGC/A

Autorité Responsable d'Application ARA :

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

L'ARA de l'IGC/A est le secrétaire général de la défense nationale.
L'ARA d'une administration est généralement un membre de la chaîne fonctionnelle de la sécurité des systèmes d'information (fonctionnaire de sécurité des systèmes d'information, voire haut fonctionnaire de défense et de sécurité ou haut fonctionnaire de défense).

Autorité administrative AA :

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

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

Autorité de certification racine ACR :

L'ACR est l'autorité qui dispose d'une infrastructure de gestion de clés lui permettant d'enregistrer, de générer, d'émettre et de révoquer des certificats, principalement des certificats d'autorités de certification étatiques, conformément à la PC et à la DPC définies par son AA. L'ACR s'auto-certifie, c'est-à-dire qu'elle signe elle-même son propre certificat. L'ACR délègue à l'autorité d'enregistrement, l'enregistrement des AC, telles que définies au § 9.1, dont elle signe les certificats. De plus, dans le cas d'une ACR étatique, celle-ci peut, selon les conditions de la présente PC, être certifiée par l'ACR de l'IGC/A.

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

Autorité d'enregistrement AE de l'IGC/A :

L'AE de l'IGC/A est l'autorité qui vérifie les données propres aux ACR souhaitant faire certifier leurs bi-clés par l'IGC/A. L'AE de l'IGC/A publie un formulaire de demande de certification et un formulaire de demande de révocation pour l'IGC/A et pour les ACR souhaitant être certifiées par l'IGC/A.

L'AE de l'IGC/A est le chef du bureau conseil de la DCSSI.

Remarque :

Il n'est pas fait ici mention des utilisateurs finaux, tels que définis au § 9.1. En effet l'IGC/A ne délivre pas de certificats aux utilisateurs finaux.

1.3.2 Applications concernées

L'application concernée est la certification d'autorités de certification racines ministérielles ou interministérielles.

L'usage fait des certificats émis par ces AC racines étatiques n'entre pas dans le cadre de la présente PC.

1.4 Contacts

Personnes à contacter concernant ce document :

SGDN/DCSSI/BCS

51 bd la Tour Maubourg

75700 PARIS – 07 SP

email : igca@sgdn.pm.gouv.fr

Personnes habilitées à déterminer la conformité de la DPC avec la PC : les personnes habilitées à déterminer la conformité de la DPC avec la PC sont nommées par l'AA.

2 DISPOSITIONS GENERALES

2.1 Obligations

2.1.1 Obligations communes à tous les acteurs

- 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 ;
- respecter et appliquer la PC et sa ou ses DPC mises en œuvre ;
- respecter la convention ou l'acte réglementaire qui lie l'entité à l'ARA de l'IGC/A ;
- respecter le résultat d'un contrôle de conformité et remédier aux non-conformités qu'il révèle ;
- se conformer aux impératifs de sécurité définis dans le § 6.5.1. et § 6.5.2.

2.1.2 Obligations qui incombent à chacun des acteurs

Les obligations de l'ARA de l'IGC/A :

- l'ARA est responsable de l'ensemble des composantes de l'IGC/A (plate-forme d'enregistrement, plate-forme de certification, service de publication, ressources cryptographiques principalement) ;
- l'ARA prend la décision d'homologation de l'IGC/A avant sa mise en service, à partir du dossier d'homologation préparé par l'AA ;
- l'ARA décide la révocation de l'ACR de l'IGC/A et la révocation des certificats d'ACR étatique émis par l'IGC/A conformément au § 4.4.3 ;
- en cas de compromission de l'IGC/A, l'ARA prend la décision de la remise en service de l'ACR de l'IGC/A, à partir du dossier de contrôle de conformité préparé à cet effet par l'AA ;
- en cas de révocation du certificat d'une ACR étatique émis par l'IGC/A, l'ARA décide de l'attribution d'un nouveau certificat à cette ACR.

Les fonctions de l'ARA sont déléguées à l'ACR, ainsi qu'à l'AA et à l'AE de l'ACR, de la façon suivante :

Les obligations de l'AA 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 ;
- préparer l'homologation de l'IGC/A ;
- définir les exigences minimales devant figurer dans les PC des ACR étatiques souhaitant obtenir un certificat de l'IGC/A, sous la forme d'une PC-type ACR 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'ARA, lorsqu'un agent abuse de ses droits ou effectue une opération non conforme à ses attributions (Cf. § 5.3.6) ;
- arbitrer les litiges conformément aux § 3.1.5 et § 2.4.2. ;

- transmettre pour accord à l'ARA de l'IGC/A les demandes de révocation pour les cas identifiés au § 4.4.1 et pour action à l'ACR de l'IGC/A ;
- prononcer la décision de révocation de l'ACR de l'IGC/A ;
- déclarer la cessation d'activité de l'ACR de l'IGC/A.

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

- avertir l'AA de l'IGC/A de toute modification concernant sa partie dans la procédure de certification de la PC IGC/A ;
- respecter les conditions de la présente PC et de la DPC afférente ;
- respecter les rôles prévus au § 5.2.1. ;
- demander l'autorisation à l'AA conformément au § 6.6.2 pour toute évolution de son système ;
- utiliser ses clés publiques et privées, et ses certificats, aux seules fins pour lesquelles ils ont été émis et avec les outils spécifiés, conformément à la PC de l'IGC/A ;
- protéger sa clé privée et ses données d'activation en intégrité et en confidentialité ;
- assurer la disponibilité de sa clé publique et de son certificat ;
- veiller à l'unicité du nom utilisé dans le certificat de l'AC ;
- assurer l'unicité du numéro de série servant ensuite de base à l'unicité d'un certificat ;
- mettre à la disposition d'un utilisateur de certificat les informations communicables relatives aux obligations mises en œuvre dans l'opération de certification et lui permettant d'apprécier la confiance à accorder à un certificat ;
- déclarer à l'AA la révocation de sa clé privée en cas de compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'ACR de l'IGC/A (perte du secret principal, perte du code d'activation et perte de plus de deux secrets partagés) ;
- contrôler les accès physiques aux locaux hébergeant les composantes de l'IGC/A et les limiter aux personnels autorisés ;
- documenter les schémas de certification qu'elle entretient avec les ACR étatiques ou d'autres IGC ;
- soumettre à l'AA les demandes d'accords de certification avec des ACR étrangères au domaine de certification auquel elle appartient ;
- attester de la complémentarité des clés publique et privée d'une ACR étatique souhaitant être certifiées par l'IGC/A, conformément au § 3.1.7. ;
- générer le certificat d'une ACR étatique dès lors que les conditions de certification posées dans la PC IGC/A sont remplies par l'AC étatique ;
- renouveler le certificat d'une ACR étatique dès lors que les conditions de renouvellement du certificat posées dans la PC IGC/A sont remplies par l'ACR étatique ;
- obtenir confirmation de l'acceptation explicite du certificat par l'ACR étatique sous la forme d'un accord signé (papier ou électronique) ;
- révoquer le certificat d'une ACR étatique selon les conditions posées et dans le respect des procédures déterminées dans la présente PC ;
- révoquer son certificat suite à l'une des dites causes la concernant (cf. § 4.4.1) ;
- obtenir l'accord de l'ARA pour émettre une nouvelle bi-clé si sa clé privée a été compromise ;
- veiller à l'intégrité et la précision des dates utilisées dans la génération de certificats, de journaux d'événements, d'archives, etc ;
- enregistrer et archiver les informations conformément aux § 4.6. et § 4.5. ;

- respecter les impératifs des contrôles techniques définis au chapitre 6.1, 6.2 et 6.3 hormis le § 6.1.2. ;
- respecter, en fin de vie, les spécifications du § 4.9. ;
- respecter la procédure de modification définie au § 8.1. ;
- publier les informations listées au § 2.6.1en fonction du besoin d'en connaître des applications utilisatrices et des règles de confidentialité énoncées au § 2.8 ;
- respecter les conditions de disponibilité définies dans la présente PC et la DPC afférente ;
- publier des informations authentiques et intègres.

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

- avertir l'AA de toute modification concernant sa partie dans la procédure de certification ;
- respecter les rôles prévus au § 5.2.1 ;
- contrôler les accès physiques et les limiter aux personnels autorisés ;
- conserver et protéger en confidentialité et en intégrité les données d'identification transmises pour l'enregistrement ;
- publier un formulaire de demande de certification et de révocation pour les candidats à la certification ;
- enregistrer les demandes de certification des ACR étatiques acceptées par l'ARA de l'IGC/A et les transmettre à l'ACR de l'IGC/A pour action ;
- vérifier les données d'identification fournies lors de la procédure d'enregistrement des ACR étatiques ;
- fournir les données à l'ACR de l'IGC/A pour la certification, conformément au § 4.2. ;
- enregistrer les demandes de révocation des ACR étatiques acceptées par l'ARA de l'IGC/A et les transmettre à l'ACR de l'IGC/A pour action ;
- procéder à l'authentification d'une demande de renouvellement de certificat conformément au § 3.2. ;
- procéder à l'authentification d'une demande de révocation de certificat conformément au § 3.4. ;
- enregistrer et archiver ses informations conformément au § 4.6. et § 4.5..

Les obligations de l'ARA étatique sont :

- faire auditer l'IGC de son ACR par l'ARA de l'IGC/A ;
- respecter les exigences minimales définies par l'AA de l'IGC/A ;
- respecter ces exigences pendant, au minimum, la durée de validité du certificat ;
- authentifier les demandes de certification faites à l'AE de l'IGC/A pour la ou les ACR auxquelles elle confie la gestion de ses IGC ;
- s'assurer que la ou les ACR dont elle a la responsabilité n'utilisent ses clés publique et privée qu'aux fins pour lesquelles elles ont été émises (mentionnées dans leur certificat), et avec les outils spécifiés, en vertu de la PC ACR afférente ;
- 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 ;
- informer dans les plus brefs délais l'AA de l'IGC/A pour que cette dernière puisse remplir son obligation de demande de révocation conformément à l'article 4.4.2.

2.2 Responsabilités qui incombent à chaque acteur

A minima et sous réserve d'une convention ou d'un protocole d'accord particulier consenti entre les parties, les responsabilités des ARA IGC/A et ARA étatiques sont les suivantes :

Les responsabilités de l'ARA de l'IGC/A :

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

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

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

Les responsabilités des ARA étatiques :

L'ARA étatique (et les composantes auxquelles elle délègue) ayant fait certifier une ou plusieurs ACR par l'IGC/A est responsable des préjudices causés par le non respect de ses obligations telles que définies au chapitre 2.1 et des conditions d'homologation (conformité à la PC type ACR,…).

Le non respect des obligations des ARA étatiques définies au § 2.1 engage leur seule responsabilité et non celle de l'ARA de l'IGC/A ni celles des AA, ACR et AE de l'IGC/A.

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

2.3 Responsabilités financières

Sans objet.

2.3.1 Indemnisation par l'IGC

Sans objet.

2.3.2 Relations financières

Sans objet.

2.3.3 Processus administratifs

Un engagement contractuel pourra préciser, si nécessaire, les relations entre l'opérateur de l'une des composantes de l'IGC/A et l'ARA, dans le cas notamment de la sous-traitance.

2.4 Interprétation de la loi

2.4.1 Lois

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 décret nº96-67 du 29 janvier 1996 relatif aux compétences du secrétaire général de la défense nationale dans le domaine de la sécurité des systèmes d'information [DEC96-67] ;
- 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 [DEC01-693].

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.

2.4.2 Arbitrage des litiges

En priorité, un compromis est recherché par l'ARA de l'IGC/A en vue de résoudre les litiges qui pourraient exister entre elle et une ARA étatique, sur la base des responsabilités définies au 2.2.

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.

2.5 Barèmes des prix

Sans objet, les services de l'IGC/A n'étant pas facturés aux ARA responsables d'IGC étatiques.

2.5.1 Frais de génération ou de renouvellement de certificat

Sans objet.

2.5.2 Frais d'accès à un certificat

Sans objet.

2.5.3 Frais de révocation

Sans objet.

2.5.4 Frais pour d'autres services

Sans objet.

2.5.5 Politique de remboursement

Sans objet.

2.6 Publications et services associés

2.6.1 Publication d'informations concernant l'IGC/A

Les informations concernant l'IGC/A publiées sont les suivantes :

- la PC de l'IGC/A ;
- les formulaires de demande de certification ;
- les formulaires de demande de révocation ;
- les certificats de l'ACR de l'IGC/A ;
- les certificats d'ACR étatique signés par l'IGC/A, sous réserve du besoin d'en connaître.

Les informations ci-dessus, sont publiées conformément aux dispositions du § 2.8.1 et aux conditions fixées dans la DPC. Le moyen de publication de ces informations est précisé dans la DPC.

NB : La publication des LAR n'est pas assurée actuellement par le SP, mais est prévue dans une prochaine version de la PC.

2.6.2 Fréquence de publication

Les informations énumérées dans le § 2.6.1 sont disponibles dans les meilleurs délais via le SP.

Toute modification de l'une d'entre elles fera l'objet d'une mise à jour dans des délais définis dans la DPC, en fonction de la nature de l'information.

2.6.3 Contrôle d'accès

L'ACR est responsable de la mise en œuvre et de l'application de politiques de sécurité adaptées aux contrôles d'accès à ses publications.

2.6.4 Service de Publication

Le SP assure l'intégrité et l'authenticité des informations qu'il publie.

2.7 Contrôles de conformité

2.7.1 Fréquence du contrôle de conformité

Concernant l'IGC/A :

L'homologation par l'ARA de la ou des plates-formes utilisées par l'ACR et l'AE de l'IGC/A, en fonction des éléments fournis par l'AA, 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 VAR_TEMPS : :F_CONFORM relative aux composantes de l'IGC_A.

Concernant les ACR étatiques :

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

2.7.2 Identification et qualifications du contrôleur

Concernant l'IGC/A :

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

Concernant les ACR étatiques :

L'identification et les qualifications des contrôleurs seront précisées dans la convention liant l'ARA de l'IGC/A et l'ARA étatique.

2.7.3 Sujets couverts par le contrôle de conformité

Concernant l'IGC/A :

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

Concernant les ACR étatiques :

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

2.7.4 Mesures à prendre en cas de non-conformité

Concernant l'IGC/A :

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

Concernant les ACR étatiques :

Si le contrôle est l'audit initial pour la certification, une non-conformité entraîne le refus de la certification par l'IGC/A, dans l'attente d'une mise en conformité.

Dans le cas d'une visite de contrôle relevant une non-conformité, un délai de mise en conformité est indiqué au-delà duquel une demande de révocation de certificat sera effectuée par l'AA de l'IGC/A.

2.7.5 Communication des résultats

Concernant l'IGC/A :

Les éléments relatifs à l'homologation du système IGC/A sont communiqués par l'AA à l'ARA.

Concernant les ACR étatiques :

Les résultats des contrôles de conformité sont communiqués à l'ARA concernée, par l'ARA de l'IGC/A.

2.8 Politique de confidentialité de l'IGC/A

2.8.1 Types d'informations considérées comme confidentielles

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	Confidentiel défense
Les données d'identification d'un acteur de l'IGC/A	Diffusion restreinte
Le dossier d'enregistrement d'une ACR étatique	Diffusion restreinte
La DPC	Confidentiel défense
Le dossier d'homologation de l'IGC/A	Confidentiel défense
La décision d'homologation de l'IGC/A	Diffusion restreinte
La notification de la recevabilité d'une demande de certification	Diffusion restreinte

De la DPC peuvent être extraites certaines informations non classifiées, pour publication auprès des ARA étatiques, 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).

2.8.2 Types d'informations considérées comme non-confidentielles

Les informations concernant l'IGC/A, publiées par le SP et citées en 2.6.1 sont considérées comme non confidentielles.

2.8.3 Divulgation des causes de révocation et de suspension des certificats

Dans le cas d'une révocation à l'initiative d'une ACR étatique, celle-ci peut transmettre la cause de révocation à l'ARA de l'IGC/A.

Dans le cas d'une révocation du certificat d'une ACR étatique à l'initiative de l'ARA de l'IGC/A, celle-ci notifiera à l'ARA étatique la cause de la révocation.

Dans le cas d'une révocation du certificat de l'IGC/A, les causes de révocation sont transmises à l'ARA et à l'AE de l'IGC/A par l'ACR ou l'AA de l'IGC/A.

Dans tous les cas, la cause de révocation portée dans la LAR sera : " raison inconnue " (" Unknown ").

2.8.4 Délivrance aux autorités légales

L'ARA est responsable de la diffusion de l'information concernant l'IGC/A dans le cadre d'une commission rogatoire ou d'une autre obligation légale ou judiciaire.

2.8.5 Délivrance à la demande du propriétaire

Les informations relatives à l'ACR étatique et définies comme confidentielles en 2.8.1 ne peuvent être divulguées qu'aux AA et ARA concernées ou à un tiers habilité par elles.

2.8.6 Autres circonstances de délivrances possibles

D'autres circonstances pourront être définies dans le cadre de conventions ou engagement contractuel entre les parties.

2.9 Droits sur la propriété

Sans objet.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Enregistrement initial

3.1.1 Conventions de noms

Les noms utilisés dans un certificat sont décrits suivant [X500].

Dans chaque certificat conforme à [X509], le fournisseur et le porteur (subject) sont identifiés par un Nom distinctif (champ Distinguished Name ou DN).

Le DN de l'IGC/A est celui indiqué dans la DPC.

Le DN de l'ACR étatique est celui contenu dans le certificat (auto-signé).

3.1.2 Nécessité d'utilisation de noms explicites

Cf 3.1.1.

3.1.3 Interprétation des différentes formes de noms

Cf 3.1.1.

3.1.4 Unicité des noms

L'unicité d'un certificat est basée sur l'unicité de son numéro de série définie par l'ACR de l'IGC/A.

3.1.5 Résolution des litiges sur la revendication d'un nom

Si plusieurs directions au sein d'une même administration revendiquent la possession de l'ACR de 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'AE de l'IGC/A ne donnera de suite aux demandes de certification ou de révocation qu'après accord des parties.

3.1.6 Reconnaissance, authentification et rôle des noms de marques

Sans objet.

3.1.7 Preuve de la possession d'une clé privée

L'ACR de l'IGC/A s'assure que l'ACR étatique possède la clé privée correspondant à la clé publique à certifier par le biais du format de données utilisé par cette dernière pour transmettre la clé à certifier (certificat auto-signé).

3.1.8 Authentification de l'identité d'un organisme

L'authentification d'une ACR étatique doit l'identifier de façon unique et non ambiguë.

L'authentification peut être réalisée par l'intermédiaire d'une attestation de l'ARA ou de l'AA étatique dont dépend l'ACR, signée du représentant officiel de l'ARA ou de l'AA, ou directement auprès de l'AE de l'IGC/A par l'authentification de l'identité du représentant de l'ACR conformément au 3.1.9 qui doit

justifier de l'accord de son ARA. L'AE de l'IGC/A pourra contacter le HFD/HFDS de l'organisme, ou tout membre de la chaîne fonctionnelle de sécurité des systèmes d'information désigné par lui pour vérification.

3.1.9 Authentification de l'identité d'un individu

L'authentification de l'identité d'un individu doit permettre d'identifier l'individu de façon unique et non ambiguë.

Elle s'effectue par rapport facial auprès de l'AE de l'IGC/A, en produisant un titre d'identité reconnu par l'Administration française, et si nécessaire la référence du Journal officiel de la République française publiant les fonctions de l'individu.

3.2 Renouvellement de certificat après expiration

Le renouvellement de certificat après expiration requiert une authentification réalisée par la même procédure que lors de la première demande de certificat.

La période de validité d'un certificat émis par l'IGC/A est précisée par la variable VAR_TEMPS::T_VALID_CERT.

3.3 Génération de nouvelles clés après révocation

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'ARA de l'IGC/A.

Après la révocation du certificat d'une ACR étatique, la génération de nouvelles clés sera ou non obligatoire, selon la cause de la révocation, et sur décision de l'ARA étatique.

3.4 Authentification d'une demande de révocation

Si la demande de révocation est due à une compromission ou suspicion de compromission de clé, perte ou vol, l'authentification de la demande de révocation ne peut être effectuée avec la clé compromise. L'authentification doit être réalisée de préférence par un rapport facial d'un représentant de l'AA de l'ACR (étatique, ou de l'IGC/A) auprès de l'AE de l'IGC/A.

Si la demande de révocation est provoquée par une autre cause (modification d'informations contenues dans le certificat, révocation de l'AC, etc.), l'authentification de la demande de révocation peut être effectuée soit par :

- l'ACR en signant sa demande avec sa clé privée,
- l'AA de l'ACR par un rapport facial de son représentant auprès de l'AE de l'IGC/A, ou en utilisant la même procédure que lors d'un premier enregistrement.

Les demandes de révocation doivent être authentifiées et venir d'une source autorisée (cf. § 4.4.2). Dans le cas où la demande de révocation émane de l'AA, l'ACR ou de l'ARA alors cette demande est effectuée en liaison avec l'AE de l'IGC/A.

4 BESOINS OPERATIONNELS

4.1 Demande de certificat

L'ACR étatique adresse à l'AE de l'IGC/A une demande de certification, à l'aide du formulaire publié par le SP. Elle doit s'authentifier auprès de l'AE de l'IGC/A conformément au § 3.1.8. De ce fait :

- soit l'ACR étatique peut transmettre à l'AE de l'IGC/A un dossier d'enregistrement complet,
- soit il est nécessaire que l'identité du représentant de l'ACR soit authentifiée conformément au § 3.1.9, auquel cas l'AE de l'IGC/A et l'ACR étatique conviennent d'une date pour cette authentification qui est alors l'occasion de la remise de tous éléments du dossier d'enregistrement à l'AE de l'IGC/A.

L'AE de l'IGC/A contrôle et valide le dossier d'enregistrement, puis enregistre l'ensemble des pièces du dossier d'enregistrement.

En particulier l'AE vérifie que le format du certificat est compatible avec les formats acceptés par l'IGC/A, et au besoin transmet à l'ACR de l'IGC/A les éléments nécessaires à un test technique de conformité.

L'AE informe le demandeur de la recevabilité de sa demande, puis l'AE de l'IGC/A fournit les données pour la certification (cf. 4.1) à l'ACR de l'IGC/A de façon à en assurer l'intégrité et l'authenticité.

Le dossier d'enregistrement est composé a minima des pièces ci-dessous :

- les données permettant l'identification de l'ARA et de ses composantes conformément au § 3.1.8 ;
- les données permettant l'identification des représentants de l'ARA et de ses composantes conformément au § 3.1.9 ;
- l'identifiant de l'IGC ;
- la clé publique à certifier (cf. § 6.1.3) sur support papier ;
- la preuve de la possession de la clé privée (cf. § 3.1.7) ;
- la crypto-période du certificat demandé, de la clé publique et privée de l'ACR étatique ;
- les informations relatives à la PC de l'ACR étatique :
    - 3.1.1 Conventions de noms
    - 3.1.2 Nécessité d'utilisation de noms explicites
    - 3.1.3 Règles d'interprétation des différentes formes de noms
    - 3.1.4 Unicité des noms
    - 3.1.5 Procédures de résolution des litiges sur la revendication d'un nom
    - 3.1.7 Preuve de la possession d'une clé privée
    - 3.2 Nouvelle génération de certificat après expiration
    - 7.1 Profil du certificat
    - 7.1.1 Numéro de version
    - 7.1.4 Format de noms
    - 8.1 Procédures de modification de ces spécifications
    - 8.3 Procédures d'approbation des DPC

4.2 Génération de certificat

L'ACR de l'IGC/A génère le certificat de l'ACR étatique conformément à la DPC.

L'ACR de l'IGC/A remet à l'ACR de l'IGC étatique, le (ou les) nouveau(x) certificat(s) propre(s) à l'ACR étatique, et le (ou les) certificat(s) de la (ou des) bi-clé(s) de l'IGC/A utilisée(s) pour sa (ou leur) signature.

4.3 Acceptation d'un certificat

A la réception de son certificat, l'ACR étatique notifie à l'AE de l'IGC/A qu'elle accepte le certificat. Le moyen est précisé dans la DPC.

4.4 Suspension et révocation de certificat

4.4.1 Causes de révocations

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

1. cessation d'activité de l'ACR ;
2. compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'ACR ;
3. changement d'informations dans le certificat de l'ACR de l'IGC/A. Cette cause n'entraîne pas obligatoirement la révocation du certificat de l'ACR de l'IGC/A.

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

4. cessation d'activité de l'ACR de l'IGC/A ;
5. compromission, suspicion de compromission, vol ;
6. décision suite à une non-conformité révélée lors d'un contrôle de conformité ;
7. non-respect de la PC et/ou de la DPC de l'IGC/A. Cette cause n'entraîne pas obligatoirement la révocation du certificat ;
8. changement d'informations dans le certificat de la composante, dès lors que ces informations sont nécessaires à la vérification du statut du certificat.

Remarque :

Dans le cas de la compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'ACR de l'IGC/A, les certificats de toutes les composantes de l'IGC/A sont révoqués.

Pour l'ACR étatique :

9. cessation d'activité de l'ACR étatique ;
10. compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'ACR étatique ;
11. décision suite à une non-conformité révélée lors d'un contrôle de conformité ;
12. non-respect de la PC et/ou de la DPC de l'ACR étatique. Cette cause n'entraîne pas obligatoirement la révocation du certificat ;
13. changement d'informations dans le certificat de l'ACR étatique. Cette cause n'entraîne pas obligatoirement la révocation du certificat ;
14. non respect de la convention entre l'ACR étatique et l'IGC/A. Cette cause n'entraîne pas obligatoirement la révocation du certificat.

4.4.2 Qui peut demander une révocation ?

Autorité habilitée	*Causes*
L'ARA ou l'AA de l'IGC/A (cf. 4.4.1)	1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
L'ACR de l'IGC/A	2, 3, 6, 9
Toute composante de l'IGC/A	6, 9
L'ARA ou l'AA étatique	9, 10, 11, 12, 13, 14

4.4.3 Procédure de demande de révocation

Nota :

Les procédures suivantes sont données à titre indicatif, les LAR n'étant pas publiées pour le moment.

Procédure de révocation du certificat de l'ACR de l'IGC/A :

1. l'AA de l'IGC/A informe ses partenaires (les ARA des ministères) par les moyens de son choix, de ses intentions de révocation ;
2. l'ACR de l'IGC/A révoque les certificats valides qu'elle a signés ;
3. l'ACR de l'IGC/A met à jour la LAR ou génère une LAR en incluant l'identité du certificat à révoquer ;
4. l'ACR de l'IGC/A signe la LAR ;
5. selon la cause de révocation, les clés de l'ACR de l'IGC/A sont alors détruites suivant la procédure définie en § 6.2.9 ;
6. arrêt des services de la plate-forme, à l'exception du SP qui publie la LAR pendant la durée VAR_TEMPS : : T_REVOC_PUB ;
7. redémarrage des services de l'ACR sur décision de l'ARA de l'IGC/A, suite à la restauration de la plate-forme ;
8. l'ACR de l'IGC/A génère une nouvelle bi-clé et un certificat auto-signé selon la procédure définie en § 6.1.1.

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'ACR peut être de nouveau certifiée (exemple : révocation suite à un changement de l'identifiant de l'ACR).De plus, la révocation s'effectue sous un délai donné (cf. § 4.4.4).

Procédure de révocation du certificat de l'AE ou d'une composante de l'IGC/A :

La procédure de révocation du certificat de l'AE ou d'une autre composante de l'IGC/A est identique à celle de l'ACR de l'IGC/A, mise à part l'authentification de la demande de révocation qui est réalisée par l'AE ou l'AA de l'IGC/A.

Dans le cas de l'AE ses services sont interrompus jusqu'à ce qu'un nouveau certificat soit réémis. En cas de prolongement de l'interruption de service de l'AE, l'AA de l'IGC/A prend en charge les fonctions de l'AE. La révocation du certificat de l'AE n'empêche pas à priori la continuité des services de l'IGC/A.

Procédure de révocation pour une ACR étatique :

1. l'AE de l'IGC/A authentifie la demande de révocation de l'ACR étatique - conformément au § 3.4. - qui provient d'une personne autorisée - conformément au § 4.4.2., et en accuse réception à cette personne par le moyen de son choix ;
2. l'AE de l'IGC/A transmet à l'ACR de l'IGC/A la demande de révocation, par le moyen de son choix qui en garantit l'intégrité ;
3. l'ACR de l'IGC/A authentifie l'AE de l'IGC/A et vérifie l'intégrité de la demande ;
4. l'ACR de l'IGC/A met à jour la LAR ou génère une nouvelle LAR en incluant l'identité du certificat à révoquer ;
5. l'ACR de l'IGC/A signe la LAR et la transmet au SP ;
6. le SP publie la LAR à jour et en averti l'ACR par le moyen de son choix ;
7. l'ACR de l'IGC/A informe l'AE de la publication de la mise à jour de la LAR ;
8. l'AE informe l'émetteur de la demande de révocation de la publication de la mise à jour de la LAR.

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).

4.4.4 Temps de traitement d'une révocation

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

4.4.5 Causes possibles de suspension

Sans objet.

4.4.6 Qui peut demander une suspension ?

Sans objet.

4.4.7 Procédure de demande de suspension

Sans objet.

4.4.8 Limites d'une période de suspension

Sans objet.

4.4.9 Fréquence de la mise à jour de la liste des certificats révoqués

Nota :

Les procédures suivantes sont données à titre indicatif, les LAR n'étant pas publiées pour le moment.

Les fréquences de mise à jour des listes de certificats révoqués sont indiquées dans VAR_TEMPS: :F_MAJ_LAR.

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. La variable VAR_TEMPS: :T_NEXT_LAR donne une date informative sur la date d'émission de la prochaine LAR.

En cas de révocation, conformément au 4.4.4, une nouvelle LAR sera publiée indépendamment de cette périodicité.

La modification des informations de révocation nécessite un contrôle d'accès. L'information de révocation doit être protégée en intégrité et authentifiée ainsi que toutes les traces de modifications. Les LAR doivent être signées par l'ACR de l'IGC/A.

4.4.10 Exigences de contrôle des listes de certificats révoqués

Nota :

Les procédures suivantes sont données à titre indicatif, les LAR n'étant pas publiées pour le moment.

L'AE de l'IGC/A doit transmettre à l'ACR de l'IGC/A de façon intègre les informations à porter dans les LAR. L'ACR vérifie que les LAR qu'elle génère sont cohérentes avec les informations transmises par l'AE. Le mode opératoire est indiqué dans la DPD.

Les différentes composantes de l'IGC/A, ainsi que les ACR étatiques, doivent vérifier régulièrement le statut des certificats signés par l'IGC/A qui leur sont présentés (selon la fréquence VAR_TEMPS: :F_MAJ_LAR).

4.4.11 Publication des causes de révocation

Les causes de révocation ne sont pas publiées.

4.4.12 Contrôle en ligne des listes de certificats révoqués

Nota :

Les procédures suivantes sont données à titre indicatif, les LAR n'étant pas publiées pour le moment.

Dans le cas d'une défaillance matérielle ou autre, rendant le SP de l'IGC/A indisponible dans un temps supérieur à VAR_TEMPS : :T_DISPO_PUB. Le SP devra alors délivrer sur demande l'information de révocation par le moyen de son choix qui permette d'en garantir l'authenticité et l'intégrité.

4.4.13 Autres formes de publication des listes de certificats révoqués

Sans objet.

4.4.14 Contrôle en ligne des autres formes de listes de certificats révoqués

Sans objet.

4.4.15 Besoin spécifiques en cas de révocation pour compromission

Sans objet.

4.5 Journalisation d'événements

4.5.1 Types d'événements enregistrés

Les données enregistrées sont :

- informations minimales pour tout événement :
    - date et heure de l'opération
    - organisme destinataire de l'opération
    - nom de l'exécutant
    - nom des personnes présentes
    - nom du représentant de l'ARA ou de l'ACR étatique
    - résultat de l'événement
    - type de l'opération
    - cause de l'événement
    - événements physiques dont la trace n'est pas fournie automatiquement par le système
    - registre des accès physiques aux postes de travail de l'IGC/A
- autres registres dépendants de la configuration du site physique, à préciser dans la DPC tels que :
    - journaux des accès des personnes
    - changements concernant les personnes
    - changement de configuration du système
    - opérations menées sur les postes informatiques de l'IGC/A et relatives aux opérations rendues par l'IGC/A
- informations communes :
    - démarrage et arrêt de l'application
    - changements de mots de passe
    - création et transmission de récépissés
    - modification de paramètres de configuration de l'outil de certification
    - modifications de droits d'accès
    - remise à zéro du journal d'audit
    - suspension ou révocation de certificat
    - communications avec le service de publication
    - installation et désinstallation d'un logiciel ou périphérique matériel
    - messages d'alerte de l'application, du système d'exploitation ou du réseau
- enregistrement :
    - enregistrement d'un nouvel utilisateur (dans la base de données interne)
    - éventuellement demande de renouvellement
- génération de certificat :
    - destruction de secrets
    - génération de certificat d'une ACR
    - génération des certificats de l'AE et des composantes de l'IGC/A
    - génération des données de création et de vérification de l'AC
- révocation de certificat :
    - demande de révocation
    - apport de révocation
- si l'ACR génère les clés cryptographiques, alors elle enregistre les données propres à cette opération conformément aux PC d'applications utilisées, pour les aspects de demande de génération, de transmission et de destruction
- opérations menées sur les postes informatiques et matériels du réseau de l'ACR
- modification de paramètres de configuration
- copie et suppression de fichiers
- création de nouveaux comptes

4.5.2 Fréquence de traitement des journaux d'événement

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

4.5.3 Durée de rétention d'un journal d'événements

Les journaux sont archivés et répondent donc aux spécifications exprimées en 4.6.2.

4.5.4 Protection d'un journal d'événements

Les journaux d'événements doivent être protégés en intégrité et confidentialité conformément au 2.8.1

4.5.5 Copie de sauvegarde des journaux d'événements

Si une copie de sauvegarde des journaux d'événements est réalisée, elle devra être protégée au même niveau que les originaux (cf. § 4.5.4).

4.5.6 Système de collecte des journaux (interne ou externe)

Le système de collecte des journaux peut être interne ou externe à l'ACR de l'IGC/A (idem pour l'AE).

4.5.7 Imputabilité

L'imputabilité d'une action revient à la personne, l'organisme ou le système l'ayant exécutée. Son nom figure dans le champ " nom de l'exécutant " du journal d'événements, ou à défaut dans les procès verbaux d'opération, ou sur tout autre support précisé dans la DPC Cette imputabilité est mise en œuvre par des mesures organisationnelles.

4.5.8 Analyse 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 doit figurer dans la DPC.

4.6 Archives

4.6.1 Types de données à archiver

Mettre en place les procédures et les outils permettant d'archiver les données suivantes :

- accords contractuels ou conventions
- certificats des composantes de l'IGC/A et des ACR étatiques signées par l'IGC/A
- LAR
- demandes de révocation et leurs résultats
- données d'identification personnelles
- dossiers d'enregistrement
- journaux d'événements

- logiciels et fichiers de configuration des différentes composantes
- récépissés
- ensembles des éléments utiles à l'enregistrement
- procès verbaux de cérémonies de clés

4.6.2 Période de rétention des archives

Les durées d'archivage des données du 4.6.1 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 sont conservés	pendant T_A_CERT
toutes les autres données	pendant une durée de T_ARCHIVES

4.6.3 Protection des archives

Les archives doivent être protégées en intégrité et en disponibilité (la disponibilité doit permettre de réaliser la condition T_RECUP_ARCH).

La définition de la sensibilité des journaux d'événements (sensible ou classifié) dépend de la nature des informations traitées et du métier. Elle doit être définie au cas par cas. Elle peut causer un besoin de protection en confidentialité.

4.6.4 Procédure de copie des archives

Cf DPC.

4.6.5 Besoin d'horodatage des enregistrements

L'ACR définira dans la DPC la précision de l'horloge pour dater les évènements enregistrés et archivés (Cf. § 4.5.1 et § 4.6.1). Un soin particulier sera apporté à ce qu'il y ait une base de temps commune entre les composantes de l'IGC/A.

4.6.6 Système de collecte des archives

Cf DPC.

4.6.7 Procédure de récupération des archives

Une composante ne peut récupérer et consulter que ses propres archives. Le processus de récupération doit faire l'objet d'une procédure interne de fonctionnement ou doit figurer dans la DPC de l'IGC/A. La récupération doit être effectuée sous un délai minimal égal à T_RECUP_ARCH.

4.7 Changement de clé d'une composante

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.

4.8 Compromission et plan anti-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 ces services
- politique de sécurité et de protection des secrets
- procédures de secours
- tests pratiques, formation et entraînement des personnels

4.8.1 En cas de corruption des ressources informatiques et/ou logicielles

En cas de corruption des ressources informatiques, logicielles et/ou données se référer au plan anti-sinistre (cf. 4.8).

4.8.2 En cas de révocation de la clé publique d'une composante de l'IGC/A

En cas de révocation du certificat de l'ACR de l'IGC/A ou d'une de ses composantes les procédures suivies sont celles décrites au 4.4.3.

4.8.3 En cas de compromission de clé d'une composante de l'IGC/A

En cas de compromission de clé de l'ACR, d'une de ses composantes :

1. les certificats sont révoqués conformément au 4.4.3. ;
2. les clés sont alors détruites suivant la procédure définie en 6.2.9 ;
3. les opérations sécurisées à l'aide des certificats à partir de la date de compromission sont annulées ;
4. les services concernés par la révocation sont arrêtés jusqu'à l'autorisation par l'ARA de l'IGC/A de la remise en service.

4.8.4 Mesures de sécurité en cas de sinistre

Cette rubrique doit être renseignée et apparaître dans le plan anti-sinistre de l'IGC/A (cf. 4.8).

4.9 Fin de vie d'une composante

En fin de vie une composante s'engage à :

- communiquer avant une date donnée son intention de cessation d'activité VAR_TEMPS : :T_FIN_VIE ;
- en informer ses partenaires (AA et ARA de l'IGC/A, autres composantes, autres IGC, etc.) de ses intentions de fin d'activité ;
- remettre ses archives à l'AA de l'IGC/A.

De plus, pour la fin de vie de l'ACR de l'IGC/A :

- l'ACR doit révoquer les certificats valides qu'elle a signés ;

- l'ACR doit s'assurer qu'aucun contractant ne peut agir pour son compte dans le processus de génération de certificat ;
- les clés privées de l'ACR doivent être détruites conformément au 6.2.9 ;
- l'ACR doit préciser dans sa DPC qui elle doit prévenir, comment se déroule le transfert des obligations (archives et logs à une autre entité, et comment seront traités les certificats encore valides qui seraient amenés à être révoqués après la date de sa fin de vie).

Nota :

La fin de vie d'une ACR étatique est une cause de révocation (cf 4.4.1) dont la procédure est décrite au 4.4.3..

5 CONTROLES DE SECURITE PHYSIQUE, DES PROCEDURES ET DU PERSONNEL

5.1 Contrôles physiques

5.1.1 Situation géographique et construction des sites

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.

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.

5.1.3 Électricité et air conditionné

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

En particulier, la plate-forme de l'IGC/A doit être protégée contre les signaux parasites compromettants lors de la mise en œuvre des fonctions et informations dont le besoin de confidentialité est élevé.

5.1.4 Exposition à l'eau

La plate-forme de l'IGCA doit être stockée dans un local qui n'est pas sujet aux dégâts des eaux.

5.1.5 Prévention et protection contre le feu

La prévention physique contre des incidents matériels est effectuée conformément à la politique de sécurité de l'ARA de l'IGC/A, et aux conditions contractuelles liant l'ARA 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 médias

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

5.1.7 Traitement des déchets

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

5.1.8 Site de recouvrement

Le plan anti-sinistre, décrit en 4.8 définit la stratégie de recouvrement.

5.2 Contrôle des procédures

5.2.1 Rôles de confiances

L'annexe « Rôles » de la DPC précise comment et sous quelles conditions ces rôles peuvent être cumulés par un même exploitant. Afin de veiller à la séparation des tâches critiques, on distingue quatre rôles au sein des composantes de l'IGC/A. Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où cela ne dégrade pas la sécurité des services offerts. L'annexe « rôle par opération » précise comment et sous quelles conditions ces rôles peuvent être cumulés par un même exploitant.

Afin de veiller à la séparation des tâches critiques, on distingue six rôles au sein de l'ACR de l'IGC/A :

- Administrateur d'ACR :
    - mise en route (initialisation cryptographique) de la composante ;
    - responsabilité des services délivrés ;
    - supervision des actions des opérateurs ;
    - mise en œuvre des PC et DPC ;
    - configuration des journaux d'événements (de l'IGC) ;
    - remontée des incidents au responsable de sécurité.
- Opérateur d'ACR :
    - exploitation des services délivrés ;
    - exécution des fonctions cryptographiques ;
    - remontée des incidents de sécurité à l'administrateur.
- Responsables de sécurité d'ACR :
    - contrôle de la sécurité physique et fonctionnelle (gestion des contrôles d'accès physique, etc.) ;
    - mise en oeuvre la politique de sécurité ;
    - analyse des journaux d'événements ;
    - remontée des incidents à l'AA de l'IGC/A.
- Détenteur de secret partagé :
    - détient un élément de reconstitution de la clef privée.
- Détenteur de secret principal :
    - détient la partie indispensable de reconstitution de la clé privée.
- Maître de cérémonie.
    - veille au bon déroulement de la procédure de la Key Ceremony ;
    - il valide les données publiques lors de l'établissement du certificat.

Afin de veiller à la séparation des tâches critiques, on distingue trois rôles au sein de l'AE de l'IGC/A :

- Administrateur d'AE :
    - mise en route (initialisation cryptographique) de la composante ;
    - responsabilité des services délivrés ;
    - supervision des actions des opérateurs ;
    - mise en oeuvre des politiques de certification et déclarations des pratiques de certification ;
    - configuration des journaux d'événements (de l'IGC) ;
    - remontée des incidents au responsable de sécurité.
- Opérateur d'AE :

  - responsabilité des opérations ;
  - exploitation des services délivrés ;
  - remontée des incidents de sécurité à l'administrateur.
- Responsable de sécurité d'AE :
  - contrôle de la sécurité physique et fonctionnelle (gestion des contrôles d'accès physique, etc.) ;
  - mise en oeuvre la politique de sécurité ;
  - analyse des journaux d'événements ;
  - remontée des incidents à l'AA compétente.

Les personnes ayant un rôle de confiance doivent être habilitées. Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

5.2.2 Nombre de personnes nécessaires à chaque tâche

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 des rôles

L'identification et l'authentification des personnes commandant une action en fonction d'un rôle ayant trait à la gestion d'un certificat s'appuient sur des mesures organisationnelles. Chaque composante met en place une gestion des droits d'accès selon les besoins et les autorisations définies par la présente PC qui respecte la séparation des rôles.

5.3 Contrôle du personnel

5.3.1 Compétences, qualification et antécédents requis

Le nom et la fonction de tous les personnels amenés à travailler au sein de composantes de l'IGC/A doivent être explicitement précisés dans la DPC.

Ils doivent être soumis à une clause de confidentialité vis-à-vis de leur employeur. Dans le cas des agents d'autorités administratives, ceux-ci sont soumis à leur devoir de réserve.

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

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

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

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

Chaque entité opérant une composante de l'IGC/A doit mettre en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante.

5.3.2 Procédures préalables de contrôle

Préalablement à l'affectation à un rôle de confiance, les vérifications suivantes doivent être menées :

- les personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions ; ils devront remettre à leur employeur une copie du bulletin n°3 de leur casier judiciaire ;
- les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces informations seront revues régulièrement, au minimum une fois tous les 5 ans.

5.3.3 Exigences de formation initiale

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

5.3.4 Exigences et fréquences des formations

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

5.3.5 Gestion des métiers

En termes de gestion de carrière pour un exploitant donné, les règles à appliquer sont celles pratiquées par l'organisme employeur.

5.3.6 Sanctions pour des actions non-autorisées

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

5.3.7 Contrôle du personnel contractant

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
- documents constructeurs des matériels et logiciels utilisés
- procédures internes de fonctionnement

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

6 CONTROLES TECHNIQUES DE SECURITE

6.1 Génération et installation de bi-clé

6.1.1 Génération de bi-clé

L'ACR de l'IGC/A peut générer une ou deux bi-clés de signature (RSA et DSA Cf. au § 6.1.5).

L'ACR de l'IGC/A génère et utilise ses bi-clés de signature à l'aide de la ressource cryptographique définie au § 6.1.8, en respectant les exigences de protection physique et logique et les spécifications sur les rôles à mettre en œuvre pour l'initialisation de l'ACR de l'IGC/A (Cf. § 5.2.1). Cette étape constitue la cérémonie des clés qui est sous le contrôle du maître de cérémonie et fait intervenir les détenteurs de secret.

6.1.2 Transmission de la clé privée à un utilisateur final

Sans objet.

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

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

Les modes de transmission de la clé publique (PKCS#10, certificat auto-signé…), sont définis dans la DPC.

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

L'ACR de l'IGC/A publie son certificat par le SP.

Elle peut remettre également son certificat aux représentants de l'ACR étatique à l'issue de la certification de cette dernière, par un moyen en garantissant l'intégrité et l'authenticité.

6.1.5 Taille des clés

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

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

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

La taille de la clé de signature des composantes est d'au moins 2048 bits pour les algorithmes RSA et DSA.

Les algorithmes de chiffrement symétrique sont au minimum l'AES et le triple DES.

6.1.6 Génération des paramètres de clé publique

L'entité qui génère une bi-clé génère également les paramètres de clé publique. Aucune trace des paramètres de génération n'est conservée.

6.1.7 Contrôle de la qualité des paramètres

L'entité qui génère des clés s'assure qu'elles remplissent les conditions énoncées au § 6.2.1.

6.1.8 Mode de génération de clé (matériel ou logiciel)

Les clés de l'ACR de l'IGC/A sont générées à l'aide d'une ressource cryptographique matérielle isolée.

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

6.1.9 Usages de la clé

La clé privée de l'ACR de l'IGC/A sert pour les opérations de signatures des certificats de ses composantes (principalement le SP), des ACR étatiques et des LAR.

6.2 Protection de clé privée

6.2.1 Module de cryptographie utilisant des normes

Les algorithmes utilisés devront être conformes aux standards en vigueurs ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés.

6.2.2 Contrôle de clé privée par plusieurs personnes

Le contrôle de la clé privée de l'ACR de l'IGC/A est réalisé par plusieurs personnes (systèmes où n exploitants parmi m sont nécessaires pour l'accès à la clé privée de l'ACR). L'accès et la mise en œuvre de ces données requiert au minimum cinq rôles de confiance conformément aux spécifications de l'annexe "Rôles par opérations" sur le nombre de personnes devant approuver une action.

En cas de perte d'un secret partagé, il sera possible de reconstituer ce dernier sans revenir à la clé privée. Au maximum cette fonction n'est possible que pour la perte simultanée de deux secrets partagés au plus.

6.2.3 Séquestre de clé privée

La clé privée de signature de l'ACR de l'IGC/A n'est pas séquestrée.

6.2.4 Copie de secours de clé privée

Aucune copie de secours de la clé privée de l'ACR de l'IGC/A n'est effectuée.

6.2.5 Archivage de clé privée

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

6.2.6 Mise à la clé du module cryptographique

La clé privée est reconstituée par le module cryptographique lors de chaque processus de signature.

6.2.7 Méthode d'activation de clé privée

L'activation de la ressource cryptographique de l'ACR de l'IGC/A s'effectue conformément aux spécifications du chapitre "Rôles par opérations" de la DPC sur le nombre de personnes devant approuver une action.

6.2.8 Méthode de désactivation de clé privée

La désactivation de la clé privée s'effectue à l'issu du processus de signature. Après sa désactivation, la ressource cryptographique doit être conservée dans un lieu protégé.

6.2.9 Méthode de destruction de clé privée

La destruction de la clé privée de l'ACR de l'IGC/A requiert la destruction des secrets répartis.

La méthode de destruction des données de l'ACR de l'IGC/A est conforme à leur niveau de classification et à la PSSI de l'ARA de l'IGC/A.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

On ne procède pas à un archivage spécifique des clés publiques en dehors de l'archivage des certificats.

Ces derniers sont archivés et conservés conformément au 4.6.2.

6.3.2 Durée de vie des clés publiques et privées

La durée de validité (cryptopériode) de la bi-clé de l'ACR de l'IGC/A est de : VAR_TEMPS : :T_UTIL_KPRIV, VAR_TEMPS : :T_VALID_KPUB

La durée de validité du certificat est inférieure ou égale à la cryptopériode de l'IGC/A : VAR_TEMPS : :T_VALID _CERT

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Sans objet.

6.4.2 Protection des données d'activation

Sans objet.

6.4.3 Autres aspects sur les données d'activation

Sans objet.

6.5 Contrôle de la sécurité des postes de travail

6.5.1 Besoins de sécurité spécifiques sur les postes de travail:

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 évènements 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/sorties réseau ;
- mise en gestion de la configuration du système d'information.

6.5.2 Niveau de sécurité du poste de travail

Les postes de travail de l'ACR de l'IGC/A utilisés pour la génération des clés, des certificats et LAR sont déconnectés de tout réseau et sont classifiés « confidentiel défense ». Ils doivent être opérés dans une zone protégée.

6.6 Contrôle physique du système durant son cycle de vie

6.6.1 Contrôles des développements des systèmes

La plate-forme de l'IGC/A doit faire l'objet d'une vérification de bon fonctionnement conformément au § 2.7.3.

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'AA 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 Contrôles de la gestion de la sécurité

Toute évolution du système doit :

- être autorisée par l'AA ;
- 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'AA 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 ;
- de la montée en charge et du maintien du système à niveau.

6.7 Contrôles de sécurité réseau

Sans objet.

6.8 Contrôles techniques des modules de cryptographie

cf. § 6.2 et § 6.1.8.

7 PROFILS DES CERTIFICATS ET LISTES DE CERTIFICATS REVOQUES

7.1 Profil du certificat

Les certificats utilisés sont les certificats X.509 v3 spécifiés dans le standard [RFC3280].

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

7.1.1 Numéro de version

Les certificats utilisés doivent respecter le standard [RFC3280] (format X509 v3).

7.1.2 Extensions de certificat

Les extensions critiques sont définies au chapitre 13 (ANNEXE 5 : Format des certificats et des LAR).

7.1.3 Identificateurs d'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 Format de noms

Les noms doivent respecter les règles édictées au § 3.1.1.

7.1.5 Contrainte de noms

Cf chapitre 13 (ANNEXE 5 : Format des certificats et des LAR).

7.1.6 Identificateur de Politique de Certification

L'identificateur (OID) de la PC de l'IGC/A est indiqué au § 1.2.

Les certificats des ACR étatiques doivent respecter le format défini au chapitre 13 (ANNEXE 5 : Format des certificats et des LAR).

7.1.7 Utilisation d'extension de contraintes sur les politiques

Cf chapitre 13 (ANNEXE 5 : Format des certificats et des LAR).

7.1.8 Syntaxes et sémantiques des qualificateurs de politiques

Cf chapitre 13 (ANNEXE 5 : Format des certificats et des LAR).

7.1.9 Règles de traitement de l'extension critique "Politique de Certification"

L'extension « politique de certification » est traitée comme une extension non critique dans les certificats racines de l'IGC/A, conformément au standard [RFC3280].

7.2 Profil des Listes de certificats révoqués

7.2.1 Numéro de version de liste de certificats révoqués

La version 2 du format des listes des autorités révoquées (LAR) est utilisée. Elle est définie dans le standard [RFC3280].

7.2.2 LAR et extension des 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).

8 ADMINISTRATION DES SPECIFICATIONS

8.1 Procédure de modification de ces spécifications

L'AA de l'IGC/A doit prévenir les autorités de l'IGC/A et les utilisateurs des certificats de l'IGC/A, notamment les ARA des IGC des ACR étatiques certifiées, des modifications qu'elle entend mener sur sa PC et sa DPC, dès lors que ces modifications peuvent affecter des accords particuliers ou le niveau de sécurité offert par l'IGC/A.

8.2 Politiques de publication et de notification

L'ACR de l'IGC/A s'appuie sur le SP pour publier toutes documentations pertinentes, en fonction du besoin d'en connaître défini au 2.8.1.

8.3 Procédures d'approbation des DPC

L'approbation d'une DPC de l'IGC/A est confiée à l'AA de l'IGC/A qui vérifie l'adéquation de la DPC de l'IGC/A avec la PC de l'IGC/A.

9 ANNEXE 1 : GLOSSAIRE

9.1 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 1.3.1 Les acteurs de l'IGC/A.

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

Autorité de certification racine (ACR) - voir paragraphe 1.3.1 Les acteurs de l'IGC/A.

Autorité d'enregistrement (AE) - voir paragraphe 1.3.1 Les acteurs de l'IGC/A.

Autorité Responsable d'application (ARA) - voir paragraphe 1.3.1 Les acteurs de 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

Haché - Résultat d'une fonction de hachage, c'est-à-dire d'une fonction calculant le condensat d'un message de telle sorte qu'une modification même infime du message entraîne la modification du haché.

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.

Service de publication (SP) de l'IGC/A - Le SP rend publiques certaines informations, notamment les certificats de l'ACR de l'IGC/A, conformément à la PC et la DPC de l'IGC/A.

Actuellement, le SP ne publie pas de liste de certificats d'autorités révoqués (LAR). Cette fonction étant en cours de développement, la présente PC indique néanmoins à titre indicatif, les mesures et contraintes relatives à la génération, signature et publication des LAR, qui prendront effet lors de la mise en œuvre de la fonction et feront l'objet d'une modification de la présente PC.

Signature numérique - Données ajoutées à une unité de données ou transformation cryptographique d'une unité de données permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple) [7498-2].

Suspension 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 suspension de la validité d'un certificat pour une période donnée. Cette action peut être la conséquence de l'absence temporaire d'un porteur de certificat.

Utilisateur de Certificat – Toute personne physique ou tout système informatique utilisant un certificat de clé publique à des fins de vérification de signature numérique.

Utilisateur Final (UF) – En règle générale, l'utilisateur final 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'AC de l'IGC.

Validation de certificat - La procédure de vérification d'un certificat consiste en un ensemble d'opérations destinées à s'assurer que les informations contenues dans le certificat ont été validées par une autorité de confiance. La validation d'un certificat inclut entre autres la vérification de sa période validité, de son état (révoqué ou non), et la vérification de la signature de l'AC génératrice. Elle inclut également la validation du certificat de l'AC génératrice.

Vérification de signature - La vérification d'une signature consiste à déchiffrer la signature d'un message, en mettant en œuvre la clé publique de l'émetteur. Si le message clair obtenu est identique au haché calculé à partir du message reçu, alors il est garanti que le message est intègre et qu'il a été signé par le porteur de la clé privée correspondant à la clé publique utilisée pour la vérification.

10 ANNEXE 2 : REFERENCES BIBLIOGRAPHIQUES

10.1 Réglementation

[CC1316]	Code Civil – article 1316 relatif à la signature électronique
[LCEN]	Loi n°2004-575 du 21 juin 2004 modifiée, po ur la confiance dans l'économie numérique
[LCNIL]	Loi n°78-17 du 6 janvier 1978 modifiée, re lative 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
[DEC96-67]	Décret nº 96-67 du 29 janvier 1996 relatif aux compétences du secrétaire général de la défense nationale dans le domaine de la sécurité des systèmes d'information
[DEC01-693]	Décret n°2001-693 du 31 juillet 2001 c réant 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 rel atif 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 j uillet 1993
[II910]	Instruction interministérielle sur les articles contrôlés de la sécurité des systèmes d'information n°910/SGDN/SSD/DR - n°910/DISSI/SCS SI/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 199 5
[R901]	Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense n°901/DISSI/S CSSI du 2 mars 1994

10.2 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'oct obre 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
[RFC3280]	IETF - Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 3280 04/2002
[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 »

11 ANNEXE 3 : REGLES DE REPARTITION DES ROLES

11.1 Règles pour l'ACR de l'IGC/A

Les détenteurs de secret partagé et principal sont des personnels habilités du SGDN.

Un détenteur de secret ne peut être opérateur d'enregistrement.

Un détenteur de secret ne peut être administrateur d'enregistrement.

Le détenteur de secret principal est l'AA de l'IGC/A.

11.2 Règles pour l'AE de l'IGC/A

Un opérateur d'AE ne peut être opérateur d'ACR.

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

Un responsable de sécurité ne peut être administrateur d'AE.

Un responsable de sécurité ne peut être opérateur d'ACR.

Un responsable de sécurité ne peut être administrateur d'ACR.

Un opérateur peut être administrateur.

12 ANNEXE 4 : DEFINITION DES VARIABLES DE TEMPS VAR_TEMPS

Variable	Description	Entité concernée	Durée / fréquence
F_CONFORM	Fréquence des contrôles de conformité	ACR et composantes de l'IGC/A ACR étatique	2 ans 3 ans
F_JOURNX	Fréquence de contrôle des journaux d'événements	ACR et composantes de l'IGC/A SP	A chaque certification Au moins une fois par semaine
F_MAJ_LISTE	Fréquence de mise à jour des listes de certificats	ACR et SP de l'IGC/A	A chaque certification
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
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 étatique	3 mois 3 mois
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_UTIL_KPRIV	Période d'utilisation d'une clé privée	ACR de l'IGC/A	9 ans
T_VALID_CERT	Période de validité d'un certificat	ACR de l'IGC/A ACR étatique	18 ans max 9 ans
T_VALID_KPUB	Période de validité d'une clé publique	ACR de l'IGC/A ACR étatique	18 ans max 9 ans

13 ANNEXE 5 : FORMAT DES CERTIFICATS ET DES LAR

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

Les certificats de l'IGC/A seront de la forme :

Identification des champs de base du certificat IGC/A	Contenu des champs de bases du certificat de l'IGC/A
Bloc des données à signer	
Version	« 2 » (pour Version 3)
Numéro de série	Unicité garantie par l'IGC/A. Du type : 3911 4510 94
Algorithme de signature	sha1RSA
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). Champ « subjectPublicKey » contenant la valeur de la clé publique au format BIT STRING, par exemple : 3082 010A 0282 0101 00B2 1FD1 D062 C533 3BC0 0486 88B3 DCF8 88F7 FDDF 43DF 7A8D 9A49 5CF6 4EAA CC1C B9A1 EB27 89F2 46E9 3B4A 71D5 1D8E 2DCF E6AD AB63 50C7 540B 6E12 C990 36C6 D82F DA91 AA68 C572 FE17 0AB2 177E 79B5 3288 70CA 70C0 964A 8EE4 55CD 1D27 94BF CE72 2AEC 5CF9 7320 FEBD F72E 8967 B8BB 4773 12F7 D135 693A F20A B9AE FF46 4246 A2BF A185 1AF9 BFE4 FF49 85F7 A370 8632 1C5D 9F60

	F7A9 ADA5 FFCF D134 F97D 5B17 C6DC D60E 286B C2DD F1F5 3368 9D4E FC87 7C36 12D6 A380 E843 0D55 6194 EA64 3747 EA77 CAD0 B258 05C3 5D7E B1A8 4690 3156 CE70 2A96 B230 B877 E679 C0BD 293B FD94 774C BD20 CD41 25E0 2EC7 1BBB EEA4 0441 D25D AD12 6A8A 9B47 FBC9 DD46 40E1 9D3C 33D0 B502 0301 0001 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	[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	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.

13.2 Format des certificats des ACR étatiques

Les certificats des ACR étatiques transmis à l'ACR de l'IGC/A doivent avoir un format conforme à celui défini dans la PC-Type ACR.

Le format des certificats délivrés en retour par l'IGC/A sera le suivant :

Nom des Champs définis par la norme X509 v3		Commentaires / Informations normatives
Bloc des données à signer (Structure Certificate\tobeSigned)		
Version	2.	Les certificats utilisés dans le cadre des politiques de certification définies dans PC2 respecteront la recommandation X.509v3. La valeur « 2 » correspond à la version 3.
Numéro de série (Serial number)	Attribué par l'IGC/A.	Le numéro de série du certificat est une valeur entière, unique pour une AC (dont le nom est donné en 4.9. Il identifie de manière unique un certificat émis par une AC donnée.
Algorithme de signature (Signature / algorithmIdentifier / algorithm /parameters)	Selon l'usage possible de la clé à certifier, l'algorithme peut différer. Ce champ est donc lié à l'extension keyUsage. Valeurs conseillées : RSA : 2048 DSA : 1024 minimum SHA-1	Cette structure, composée de la structure algorithmIdentifier, donne des informations sur l'algorithme de signature et la fonction de hachage utilisés par l'AC pour signer le certificat. La structure algorithmIdentifier est composée des champs « algorithm » et « parameters »
Émetteur (Issuer)	E = igca@sgdn.pm.gouv.fr CN = IGC/A OU = DCSSI O = PM/SGDN L = Paris S = France C = FR	Ce champ contient le nom du fournisseur du certificat de d'autorité de certification qui signe le certificat courant.
Valide à partir du Valide jusqu'à (Validity)	Le format UTCTime est utilisé.	Cette structure est composée des champs notBefore et notAfter. Elle précise la période de validité du certificat.
Objet (Subject (X500 name))	Le DN contenu dans le certificat auto-signé.	Ce champ contient le nom du porteur de certificat, c'est-à-dire le propriétaire de la clé publique à certifier. La norme précise qu'une AC ne doit pas générer de certificats pour deux utilisateurs différents et ayant le même nom contenu dans le champ subject.
Clé publique	Selon l'usage possible de la clé à certifier, l'algorithme peut	Cette structure est composée des champs de la structure algorithmIdentifier (« algorithm »,

(Subject Public Key Info)	différer. Ce champ est donc lié à l'extension keyUsage. Valeurs conseillées : RSA : 2048 DSA : 1024 minimum SHA-1	« parameters »), qui spécifie l'algoritme qui utilise la clé publique du porteur, et «subjectPublicKey » qui contient le train de bits de clé publique.
Identificateur unique de l'émetteur ***(Issuer Unique Identifier)***	N'EST PAS UTILISE.	Ce composant est utilisé pour identifier sans ambiguïté un émetteur en cas de réutilisation d'un nom.
Identificateur unique du sujet ***(Subject Unique Identifier)***	N'EST PAS UTILISE.	Ce composant est utilisé pour identifier sans ambiguïté un sujet en cas de réutilisation d'un nom.
Extensions		
Identificateur de clé d'autorité ***(Authority Key Identifier)***	Obligatoire=Oui ; Critique=Non ; Seul le « keyIdentifier » sera utilisé, avec la valeur du champ « SubjectKIdentifier » du certificat de l'ACR de l'IGC/A.	Cette séquence identifie la clé publique à utiliser pour vérifier la signature d'un certificat. Elle permet de distinguer des clés différentes utilisées par une même AC (par exemple en cas de renouvellement de clé). La clé peut être identifiée soit par un identificateur de clé explicite (champ « keyIdentifier ») soit par l'association d'un numéro de certificat avec le nom de l'autorité de certification du certificat de cette clé publique (« AuthorityCerIssuer »+ « AuthorityCertSerialNumber »).
Identificateur de clé de sujet ***(Subject Key Identifier)***	Obligatoire=Oui ; Critique=Non ; SubjectKIdentifier=valeur unique dérivée de la clé publique ou d'une méthode de génération de valeur unique. Valeur reprise du certificat auto-signé de l'AC racine étatique.	Ce champ identifie la clé publique objet de la certification par l'IGC/A. Il permet de distinguer plusieurs clés utilisées par un même porteur de certificat (par exemple, en cas de renouvellement de clé). Cet identificateur doit identifier de manière unique une clé parmi celles utilisées par un porteur de certificat.
Utilisation de la clé ***(Key usage)***	Obligatoire=Oui ; Critique=Non ; Valeur : Signature du certificat, Signature de la liste de révocation de certificats hors connexion, Signature de la liste de révocation de certificats (06).	digitalSignature : pour vérifier les signatures numériques dont les buts sont autres que nonRepudiation, keyCertSign et CRLSign. 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 (cet usage ne peut pas être utilisé pour la signature de certificats ou de LAR.) keyEncipherment : pour chiffrer des clés ou d'autres informations de sécurité, comme par exemple une clé de transport. dataEncipherment : pour chiffrer des données utilisateurs, autres que les clés ou d'autres informations de sécurité. keyAgreement : pour utiliser comme clé publique

		de négociation de clé. keyCertSign : pour vérifier la signature d'une AC sur un certificat. cRLSign : pour vérifier la signature d'une AC sur une LAR. encipherOnly : clé publique de négociation de clé seulement pour une utilisation de chiffrement de données quand le champ keyAgreement est aussi positionné à 1 (ce qui signifie qu'avec un autre usage de clé que keyAgreement, le positionnement de ce champ à 1 est indéfini). decipherOnly : clé publique de négociation de clé seulement pour une utilisation de déchiffrement quand le champ keyAgreement est positionné à 1 (ce qui signifie qu'avec un autre usage de clé que le keyAgreement, le positionnement de champ à 1 est indéfini).
Utilisation de clé étendue (Extended Key usage)	Obligatoire=Non ; Critique=Non.	
Durée d'utilisation de clé privée (Private Key usage period)	Obligatoire=Non ; Critique=Non.	Ne doit jamais être critique.
Politiques de certificat (Certificate policies)	Obligatoire=Non ; Critique=Non. 1]Politique du certificat : Identificateur de politique = OID de la PC de l'IGC/A régissant l'émission du certificat.	Cette séquence, composée de structures du type de celle de « policyInformation » suivante, donne une liste de politiques de certification qui s'appliquent au certificat. Ces politiques sont reconnues par l'autorité de certification. Structure « policyInformation » : policyIdentifier : Ce champ contient l'identificateur de la PC utilisée pour émettre le certificat. CertPolicyId policyQualifiers
Mappage de politiques (Policy mappings)	Obligatoire=Non ; Critique=Non.	
Autre nom de sujet (Subject Alternative Name)	Obligatoire=Non ; Critique=Non.	
Autre nom d'émetteur (Issuer Alternative Name)	Obligatoire=Non ; Critique=Non.	
Attributs d'annuaire du sujet (Subject Directory Attributes)	Obligatoire=Non ; Critique=Non.	
Contraintes de base (Basic Constraints)	Obligatoire = Oui ; Critique=Non. CA = 1 (type d'objet = Autorité	CA : booléen indiquant si ce certificat peut être utilisé pour vérifier des signatures de certificat, autrement dit si le porteur de certificat peut se

	de certification) pathLenConstraint = Doit être rempli (valeur de 0 à max). La plupart du temps Contrainte de longueur de chemin d'accès = aucune	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 le porteur de ce certificat ne peut générer de certificats que pour des utilisateurs finaux. Ce champ ne doit être rempli que lorsqu'il s'agit du certificat d'une AC. Remarque : si le système utilisateur de certificat ne reconnaît pas cette extension, le certificat ne pourra pas être utilisé pour vérifier la signature des certificats délivrés par l'AC.
Contraintes de nom (Name Constraints)	Obligatoire=Non ; Critique=Non.	NameConstraintsSyntax : Ce champ, qui ne peut être utilisé que dans les certificats d'AC, indique un espace de noms auxquel 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 porteur de certificat 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)	Obligatoire=Non ; Critique=Non.	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)	Obligatoire=Non ; Critique=Oui seulement si utilisé.	
Point de répartition de liste CRL (CRL Distribution Point)	N'EST PAS UTILISE.	Cette extension identifie le point de distribution des LAR de l'IGC/A. Reasons : ce champ indique les raisons de la révocation couvertes par cette LAR. SI ce champ est absent, le point de distribution de LAR correspondant doit publier tous les certificats révoqués, indépendamment de leurs motifs de révocation. cRLIssuer : Ce champ indique le nom du générateur et signataire de la LAR. Si ce champ est inutilisé, aucun nom n'est précisé dans ce champ, il est positionné par défaut au nom de l'AC génératrice du certificat courant..
Liste CRL la plus récente	N'EST PAS UTILISE.	

(Freshest CRL)		
autres extensions possibles	Selon spécificités de l'ACR étatique certifiée.	Non critique par principe
Fin du bloc de données à signer		
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.

13.3 Format des listes d'autorités révoquées émises par l'IGC/A (LAR IGC/A)

Les listes d'autorités révoquées émises par l'IGC/A auront un format conforme au standard [RFC3280].