Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

SECRETARIAT GENERAL DE LA DEFENSE ET DE LA SÉCURITÉ NATIONALE

Agence nationale de la sécurité des systèmes d'information

IGC/A 4096

Demande de certificat

pour une

autorité de certification racine

d'une Administration de l'État

Renseignements techniques et administratifs

Autorité administrative concernée :

Nom	
Adresse	

Autorité de certification racine (ACR) faisant l'objet de la demande de certificat :

Nom	
Adresse	
Adresse(s) de publication de ses politiques de certification	
Adresse de publication de son certificat auto-signé	
Adresse de messagerie électronique	

Autorité effectuant la demande :

Nom		**Prénom**	
Fonction au sein de l'Administration			
Rôle au sein de l'IGC			
Coordonnées			
Adresse de messagerie électronique			

☐ Joindre la photocopie d'une pièce d'identité à la présente demande.

N.B. : Conformément à la PC de l'IGC/A, ces informations à caractère personnel sont exclusivement utilisées par l'autorité d'enregistrement de l'IGC/A, pour s'assurer de l'identité du signataire du présent document ; renseigner ce formulaire vaut acceptation de l'utilisation de ces données dans ce but.

Contexte de la demande :

Un audit de conformité des AC subordonnées et certificats terminaux au RGS a-t-il été mené ?	
OUI ☐ Date de l'audit : Référence du rapport d'audit :	NON ☐

Des écarts ont-ils été constatés ?	
OUI, des écarts mineurs ☐ OUI, des écarts majeurs ☐	NON ☐

Un audit de conformité à la PC de l'IGC/A a-t-il été mené ?	
OUI ☐ Date de l'audit : Référence du rapport d'audit :	NON ☐

Des écarts ont-ils été constatés ?	
OUI, des écarts mineurs ☐ OUI, des écarts majeurs ☐	NON ☐

Motif de la demande (indiquer ci-dessous les principaux bénéfices attendus de l'obtention du certificat demandé)

Dates souhaitées pour la cérémonie de signature du certificat :

Merci de préciser le mois, ou quelques dates par ordre décroissant de préférence, auquel vous souhaiteriez obtenir le certificat demandé :

Rang de préférence	**Jours**	**Mois**

N.B. : Ces dates sont données à titre indicatif. La date de la cérémonie sera fixée précisément dès lors que l'autorité de certification racine de l'IGC/A aura accepté la présente demande, en tenant compte de l'avis remis par l'autorité d'enregistrement de l'IGC/A.

Mandataire de l'autorité de certification racine lors de la cérémonie de signature :

Si l'autorité effectuant la demande ne peut pas représenter l'autorité de certification racine lors de la cérémonie de signature, préciser ici l'identité du mandataire chargé de la représenter :

Nom		**Prénom**	
Fonction			
Adresse de messagerie électronique			
Téléphone / Fax			

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

☐ Le mandataire doit se munir d'une pièce d'identité et de sa carte professionnelle.

N.B. : Le mandataire peut être accompagné d'une personne qui aura un rôle d'observateur pendant la cérémonie ; il émargera la liste des participants et devra se munir d'une pièce d'identité.

Indiquer dans ce cas le nom et le prénom de l'observateur ci-après :
……
……

Visa de l'autorité effectuant la demande :
L'autorité s'engage par cette demande à respecter la PC de l'IGC/A et notamment à prévenir l'ANSSI de tout changement tel que défini dans cette PC, affectant l'IGC de l'autorité.
Fait à : le : Signature :

Accord du HFD, HFDS ou du FSSI de l'organisme[1] :

Je soussigné ……..,

en qualité de …… ……..

appuie la présente demande de certification par l'IGC/A de l'autorité de certification racine dénommée

……

Fait à : le : Signature :

[1] L'accord peut également être présenté sous forme d'une note officielle jointe au présent document.

Contacts techniques :

- Personne à contacter par l'autorité d'enregistrement de l'IGC/A pour l'envoi des certificats de tests :

Nom		**Prénom**	
Fonction			
Téléphone(s)			
Adresse de messagerie électronique			

- Personne à contacter par l'autorité d'enregistrement de l'IGC/A pour la préparation de l'audit :

Nom		**Prénom**	
Fonction			
Téléphone(s)			
Adresse de messagerie électronique			

- Personne à contacter en cas de mise à disposition d'urgence d'une nouvelle liste de certificats d'autorités révoqués (LAR) :

Nom		**Prénom**	
Fonction			
Téléphone(s)			
Adresse de messagerie électronique			

Deuxième personne à contacter en cas d'indisponibilité de la première :

Nom		**Prénom**	
Fonction			
Téléphone(s)			
Adresse de messagerie électronique			

Volet de renseignements techniques utilisés et vérifiés lors de la cérémonie

Nom commun de l'autorité de certification concernée : ……

Précisions sur le contenu du certificat demandé :

Champs de base :

Champ	Valeur	Indications pour renseigner ce champ
Version		Si la valeur de ce champ est différente de 2, ce qui correspond à la version 3 de la norme X509, contacter l'opérateur d'enregistrement.
Algorithme de signature utilisé par l'AC avec sa bi-clé		RSA 4096 avec SHA-256
Date de fin de validité souhaitée		
Sujet / Objet		Indiquer le Nom Distinctif (DN) complet

Extensions obligatoires *(nom du champ précisé en anglais)* :

Champ	Valeur	Criticité	Indications
Utilisations de la clé *(Key usage)*		Critique	Préciser la valeur présente dans le certificat ou la requête de certification de l'AC. Au minimum l'usage « Signature du certificat » doit être mentionné.
Identifiant de clé d'autorité *(Authority Key Identifier)*	valeur du champ « SubjectKeyIdentifier » du certificat de l'ACR de l'IGC/A.	Non critique	Renseigné par l'ANSSI.
Identifiant de la clé du sujet *(Subject Key Identifier)*		Non critique	Indiquer ici la valeur du champ « identifiant de la clé du sujet » du certificat auto-signé ou de la requête de certification de l'AC objet du certificat.
Politiques de certification / stratégies de certificat *(Certificate policies)*	Identificateur de politique = OID de la PC de l'IGC/A régissant l'émission du certificat.	Non critique	Renseigné par l'ANSSI.
Contraintes de base *(Basic Constraints)*		Critique	CA = 1 (type d'objet = Autorité de certification) Valeur en règle générale : pathLenConstraint = Contrainte de longueur de chemin d'accès = aucune
Point de distribution des listes de certificats révoqués *(CRL Distribution Point)*		Non critique	Indiquer le chemin de téléchargement des listes de certificats révoqués communiqué par l'ACR étatique dans sa demande. Le nom de fichier de la liste des certificats d'autorités révoqués publiée par l'IGC/A est « igca4096_2018.crl».

Autres extensions (non obligatoires) :

Champ	Valeur	Criticité	Indications
			A préciser ; l'AE de l'IGC/A se réserve le droit de ne pas intégrer ces informations.

Type de bi-clé à certifier :

RSA 4096	☐	**ECDSA**	☐

Valeur de la Clé publique (optionnel, au format hexadécimal) :

Empreinte numérique du certificat auto-signé (ou de la requête de certification) transmis :

N.B. : Il s'agit d'indiquer ici l'empreinte du fichier entier, c'est-à-dire le condensat SHA-256 du fichier, et non pas l'empreinte calculée pour la signature électronique. Cette empreinte permet la vérification rapide du certificat électronique utilisé, par un simple affichage.

Renseignements complémentaires :

- Nombre d'autorités de certification de la chaîne de certification la plus longue de l'IGC : **…**
- Durée de vie initiale de la clé privée associée à la clé publique à certifier : **…**
- Date prévisionnelle de génération de la prochaine bi-clé : **.. / .. / ..**
- Algorithme de signature devant être utilisé par l'IGC/A pour signer le certificat à délivrer :

RSA avec SHA-256	☐	**ECDSA avec SHA-256**	☐

Publication des listes de certificats d'autorités révoqués (LAR) :

ATTENTION ! Ce champ est particulièrement important, toute erreur de saisie entrainera un dysfonctionnement des applications utilisatrices. C'est pourquoi une confirmation de la valeur portée dans le tableau des champs du certificat est demandée ci-dessous. Il appartiendra à l'organisme de vérifier la validité du point de distribution indiqué dans le certificat de tests qui lui sera envoyé par l'ANSSI avant la certification.

- Point de distribution des LAR à indiquer dans le certificat à délivrer :

……

N.B. : le nom de fichier de la liste des certificats d'autorités révoqués publiée par l'IGC/A pour la bi-clé RSA4096 est « igca4096_2018.crl».