Conditions Générales d'Utilisation de l'AC Technique

CIRCUIT DE VALIDATION

Date application	Version	Objet	Rédaction	Vérification	Approbation
23/11/2018	1.1	Correction chemin documents et point de contact	Le 12/11/2018 L.Flament	Le 13/11/2018 F. Loffredo	Le 23/11/2018 AA-PEKIN

SIGNATURE D'APPROBATION DE l'AA-PEKIN

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA JUSTICE

Signature numérique de Autorité Administrative PEKIN
DN : cn=Autorité Administrative PEKIN, ou=0002 110010014, o=Ministere de la Justice, c=FR
Date : 2018.11.23 14:42:13 +01'00'

DIFFUSION Elargie ☒ Restreinte ☐ Contrôlée ☐ exemplaire n°

Pour action	
Pour information	

HISTORIQUE DES MODIFICATIONS

Date application	Version	Objet	Rédaction	Vérification	Approbation
	0.1	document initial	Le 20/07/2018 L.Flament		
	0.2	séparation PC/DPC, mise à jour OID	Le 10/10/2018 L.Flament		
	1.0	Version approuvée et applicable	Le 12/10/2018 L.Flament	Le 11/10/2018 F. Loffredo	

SOMMAIRE

1. OBJET DES CGU

Les présentes Conditions Générales d'Utilisation, ci-après dénommées CGU ont pour object de préciser le contenu et les modalités d'utilisation des certificats délivrés par l'« AC Technique » du Ministère de la Justice. les CGU précisent également les engagements et obligations respectifs des différents acteurs concernés.

Pour ce faire, les CGU porte à la connaissance des porteurs, des responsables de certificat et des utilisateurs de certificats les informations pertinentes de la politique de certification et de la déclaration des pratiques de certification de l'« AC Technique ». les CGU ne se substituent pas à ces dernières, mais donne une vue synthétique des informations à destination des utilisateurs non initiés à ce type de document.

Le Ministère de la Justice possède une Infrastructure de Gestion de Clés (IGC) afin de gérer les certificats d'AC utilisés dans le cadre de ses projets internes. Cette IGC, appelée PEKIN, possède notamment une autorité dénommée « AC Technique », objet des présentes CGU, dont le rôle est de signer des certificats pour des entités finales (machines et humaines) pour les besoins du MJ.

2. DÉFINITIONS ET ACRONYMES

2.1. ACRONYMES

Les acronymes utilisés dans les présentes CGU sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
ACR	Autorité de Certification Racine
ACS	Autorité de Certification Subordonnée
AE	Autorité d'Enregistrement
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CEN	Comité Européen de Normalisation
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
IGC	Infrastructure de Gestion de Clés
IJ	Infrastructure Justice
KC	Cérémonie des clés (Key Ceremony)
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification

MJ	Ministère de la Justice
OC	Opérateur de Certification
OID	Object Identifier
PC	Politique de Certification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure – X 509
PP	Profil de Protection
PSCE	Prestataire de Services de Certification électronique
RC	Responsable de Certificat
RSA	Rivest Shamir Adelman
SSI	Sécurité des Systèmes d'Information
UC	Utilisateur de Certificat
URL	Uniform Resource Locator
VC	Validateur de Certificat

2.2. DÉFINITIONS

Les termes utilisés dans les présences CGU sont les suivants :

Applications utilisatrices : Services applicatifs exploitant les certificats émis par l'AC, afin de délivrer des certificats aux utilisateurs de certificats pour des besoins d'authentification, de chiffrement ou de signature ou des besoins d'authentification ou de cachet pour des serveurs dont elle a la gestion.

Authentification : L'authentification vise à renforcer selon le besoin, le niveau de confiance entre l'identifiant et la personne associée. On distingue l'authentification dite « faible » (ex : mot de passe) et l'authentification dite « forte » (ex :carte à puce associée à un code PIN).

Autorité Administrative (AA) : entité responsable de l'ensemble des fonctions de l'IGC PEKIN avec pouvoir décisionnaire, L'AA-PEKIN est responsable de toutes les ACs du Ministère de la Justice qu'elle délivre.

Autorité d'Enregistrement (AE) : entité en charge de la vérification des informations d'identification du Responsable du Certificat, du bénéficiaire dans le cas d'un certificat destiné à une personne physique, de la validité du formulaire de demande de certificat conformément aux notices décrivant le contenu attendu pour ce dernier. Si la demande est valide, elle est transmisse au service de génération des certificats.

Autorité de Certification (AC) : entité qui délivre et est responsable des certificats électroniques signés en son nom. L'AA-PEKIN assure elle-même l'exploitation de l'IGC PEKIN, elle dispose de locaux sécurisés, du personnel et de l'infrastructure technique qui lui permettent de réaliser l'ensemble des tâches de gestion des certificats.

Bi-clé : Couple clé privée/publique utilisé dans des algorithmes de cryptographie asymétrique.

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, le terme "certificat électronique" désigne uniquement un certificat délivré à une AC subordonnée et portant sur une bi-clé de signature, sauf mention explicite contraire.

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

Dispositif de protection des éléments secrets : Dispositif de stockage des éléments secrets remis au porteur ou au RC (exemples : clé privée, code PIN, etc). Il peut prendre la forme d'une carte à puce, d'une clé USB à capacités cryptographique ou se présenter au format logiciel (exemple : fichier PKCS#12).

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

Module matériel de sécurité : matériel dédié à la génération, au stockage et à la destruction d'éléments cryptographiques sensibles (clés privées, secrets). L'usage d'un Module matériel de sécurité rend très difficile la compromission des éléments qu'il contient (divulgation, altération) grâce à des protections physiques et cryptographiques.

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 : La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat

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 (AC Racines / 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.

Public Key Infrastructure (PKI) : cf. IGC

Qualification d'un produit de sécurité : - Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le Référentiel Général de Sécurité. La procédure de qualification des produits de sécurité est décrite dans le Décret du RGS. Le RGS précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

Responsable de certificat (RC) : Le responsable de certificat est désigné par et placé sous la responsabilité de l'entité cliente qui dans les présentes CGU ne peut-être qu'un service du Ministère de la Justice. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et les attributs des services applicatifs ou des porteurs de cette entité

Usager : Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques au sein du Ministère de la Justice. Selon le contexte, un usager peut être un porteur, un RC, un VC ou un utilisateur de certificats.

Utilisateur de certificat : Entité ou personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur de cachet ou d'authentification serveur provenant du service applicatif auquel le certificat est rattaché, ou pour établir une clé de session, ou pour vérifier une signature électronique ou une valeur d'authentification provenant du porteur du certificat ou chiffrer des données à destination du porteur du certificat

Validateur de certificat (VC) : Le validateur de certificat est désigné et placé sous la responsabilité de l'AE. Il s'agit d'une personne physique en charge de la validation des demandes émanant des RC.

3. CONTACT DE L'AC TECHNIQUE

Autorité Administrative de l'IGC PEKIN :

Ministère de la Justice / Secrétariat Général / Services des Systèmes d'Information et de Communication

13 Place Vendôme

75042 Paris Cedex 01

4. TYPE DE CERTIFICATS ÉMIS

La politique de certification de l'« AC Technique » couvre huit politiques de certification pour les différents usages de certificats :

- Personne physique :
  - PC pour les certificats d'authentification, identifiée par l'OID 1.2.250.1.120.3.3.201.1 ;
  - PC pour les certificats de signature, identifiée par l'OID 1.2.250.1.120.3.3.207.1 ;
  - PC pour les certificats d'authentification IPSec, identifiée par l'OID 1.2.250.1.120.3.3.208.1 ;
- Service applicatif :
  - PC pour les certificats d'authentification, identifiée par l'OID 1.2.250.1.120.3.3.202.1 ;

- PC pour les certificats d'horodatage, identifiée par l'OID 1.2.250.1.120.3.3.203.1 ;
- PC pour les certificats cachet serveur, identifiée par l'OID 1.2.250.1.120.3.3.205.1 ;
- PC pour les certificats d'authentification IPSec, identifiée par l'OID 1.2.250.1.120.3.3.209.1 ;
- PC pour les certificats de signature de code, identifiée par l'OID 1.2.250.1.120.3.3.210.1.

Le présent document peut être identifié par le numéro d'IDentifiant d'Objet (OID) du profil concerné. D'autres éléments, plus explicites, comme le nom, le numéro de version et la date d'application permettent également de l'identifier sans ambiguïté.

Les certificats sont émis au travers de la chaîne de certification :

- ACR Infrastructure Justice
- AC Technique

Les certificats de ces ACs, la PC correspondante et les présentes CGU sont disponibles sur le site internet public du Ministère de la Justice :

- la politique de certification dans sa version en cours de validité :
  - http://www.justice.gouv.fr/igc/sdit/mj_pc_ac-technique.pdf
- le certificat de l'« AC Technique » ;
  - http://www.justice.gouv.fr/igc/sdit/mj_ac-technique.cer
- la LCR de l'« AC Technique » ;
  - http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl
- le certificat de l'« ACR Infrastructure Justice » signataire de l'« AC Technique » :
  - http://www.justice.gouv.fr/igc/sdit/mj_acr-infra_justice.cer
- la LAR de l'« ACR Infrastructure Justice » signataire de l'« AC Technique » :
  - http://www.justice.gouv.fr/igc/sdit/mj_arl-infrastructure.crl
- les Conditions Générales d'Utilisation liées au service de certification :
  - http://www.justice.gouv.fr/igc/sdit/mj_cgu_ac-technique.pdf

5. TARIFS

Les certificats sont uniquement délivrés par le Ministère de la Justice pour ces besoins internes. La tarification est par conséquent sans objet.

6. VALIDITÉ DES CGU

Les CGU sont valables à compter du premier jour de leur mise en ligne jusqu'au premier jour de la mise en ligne

d'une nouvelle version. Les CGU qui s'appliquent sont celles dont la date d'application figure sur les présentes CGU.

Les présentes CGU entrent automatiquement en vigueur au moment de l'utilisation des certificats. Elles sont disponibles sur le site http://www.justice.gouv.fr/igc/sdit.

7. MODALITÉS D'OBTENTION DU CERTIFICAT

La gestion de la demande d'un certificat pour un service applicatif ou un porteur est faite par l'Autorité d'Enregistrement de l'« AC Technique ». L'AE se charge de prendre en compte la demande de certificat et de vérifier sa conformité avec les processus en place avant de soumettre la délivrance du certificat à l'AC. Seul l'AC est en capacité d'émettre le certificat après validation que la procédure et les éléments fournis sont corrects.

Les demandes que ce soient pour un service applicatif ou un porteur doivent être effectuées par le RC qui est en charge du service applicatif ou, dans le cas d'un porteur, est en charge de l'entité à laquelle le porteur est rattaché. Les vérifications sont effectuées sur la base d'informations internes au Ministère de la Justice est de la connaissance des personnels. Le processus est par ailleurs simplifié dans la mesure où les RC sont connus de l'AE et qu'ils possèdent un certificat numérique leur permettant de signer numériquement les demandes de certificat pour les services applicatifs et les porteurs. Ils ont en charge la validation, pour le compte de l'AE, des demandes effectuées par les porteurs et les responsables des services applicatifs. Dans les deux cas, la validation est également simplifiée par la connaissance des personnels dont ils sont généralement responsable hiérarchiquement.

Afin de procéder à une demande de certificat les RC doivent remplir toutes les informations requises dans la dernière version du formulaire de demande de certificat en se basant sur la notice de ce dernier. Ils doivent ensuite signer numériquement la demande avec le certificat qu'ils ont reçus de l'IGC PEKIN pour cet usage, puis transmettre le formulaire à l'AE pour traitement.

Le formulaire et la notice de demande de certificat sont disponibles sur le site de la GED du Ministère de la Justice et accessibles pour toute les personnes ayant un besoin d'usage.

8. MODALITÉS D'ACCEPTATION DU CERTIFICAT

Le téléchargement par le RC ou le porteur du certificat mis à disposition par l'AC vaut acceptation de ce dernier dans le cas de l'envoi par email du lien, de l'identifiant et du code d'activation du certificat. l'AC est informé du téléchargement du certificat par le RC ou le porteur.

Dans le cas de la fourniture par l'AC d'un PKCS#12, l'acceptation est tacite à compter de la transmission du PKCS#12 et du mot de passe par email au RC dans le cas d'un service applicatif, et à compter de la transmission du mot de passe par téléphone pour un porteur.

9. MODALITÉS DE RENOUVELLEMENT DU CERTIFICAT

L'AC n'émet pas de nouveau certificat pour la bi-clé d'un service applicatif ou d'un porteur déjà détenteur d'un certificat. Le renouvellement passe par la génération d'une nouvelle bi-clé et d'une nouvelle demande de certificat. La procédure est donc identique à celle décrite dans Modalités d'obtention du certificat.

10. MODALITÉS DE RÉVOCATION DU CERTIFICAT

Le porteur ne peut pas accéder aux services de révocation directement. Lorsqu'il souhaite procéder à la révocation de son certificat, il doit s'adresser à son RC.

Afin de procéder à une révocation de certificat les RC doivent remplir toutes les informations requises dans la dernière version du formulaire de révocation de certificat en se basant sur la notice de ce dernier. Ils doivent ensuite signer numériquement la demande avec le certificat qu'ils ont reçus de l'IGC PEKIN pour cet usage, puis transmettre le formulaire à l'AE (qui gère également les demandes de révocation pour le compte de l'AC) pour traitement.

Le formulaire et la notice de révocation de certificat sont disponibles sur le site de la GED du Ministère de la Justice et accessibles pour toute les personnes ayant un besoin d'usage.

11. LIMITES D'USAGES DU CERTIFICAT

Les RC (pour le compte des services applicatifs) et les porteurs doivent respecter strictement les usages autorisés des certificats, à savoir :

- **Cachet serveur :**

  Signature électronique de données et la vérification de signature électronique. Ces données peuvent être, par exemple, un accusé de réception suite à la transmission d'informations par un usager à un service applicatif, une réponse automatique à une demande formulée par un usager, un jeton d'horodatage, un code applicatif, un certificat de répondeur OCSP, ou encore une archive.

- **Authentification serveur :**

  Authentification du serveur auprès d'autres serveurs ou auprès de personnes, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient protégés (intégrité, confidentialité).
  L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique par le client et chiffrement de cette clé symétrique avec la clé publique du serveur) ou de type Diffie-Hellman (obtention de la clé symétrique via un algorithme combinant la clé privée du client et la clé publique du serveur, et inversement).

- **Authentification :**

  Authentification du porteur auprès de serveurs ou auprès d'autres porteurs, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient protégés (intégrité, confidentialité).

  L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique et chiffrement de cette clé symétrique avec la clé publique du serveur) ou de type Diffie-Hellman (obtention de la clé symétrique via un algorithme combinant la clé privée du client et la clé publique du serveur, et inversement).

- **Signature :**

  Signature électronique de données. Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

- **Authentification et signature :**

  L'ensemble de ceux identifiés ci-dessus pour les usages séparés d'authentification et de signature.

En cas d'usage autres que ceux décrits, la responsabilité du RC ou du porteur pourrait être engagée.

L'usage autorisé du certificat est également indiqué dans le certificat lui-même, via les extensions X.509 « Key Usage » et « Extended Key Usage ».

Par ailleurs les certificats sont délivrés pour une durée maximale de 3 ans et une date de fin de validité est inscrite dans le certificat. Tout usage du certificat après sa date d'expiration engagerai la responsabilité du RC ou du porteur.

12. OBLIGATION DES PORTEURS ET DES RC

Les porteurs de certificats ou les RC (service applicatif) sont responsables des informations qu'ils fournissent auprès de l'AE/l'AC. Ils doivent notamment :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- gérer de manière sécurisée les secrets et éléments sensibles qui leur sont remis à l'issue de la procédure de génération du certificat En particulier, ils sont garant de la sécurité et du contrôle exclusif de la clé privée associée au certificat délivré ;
- accepter les conditions d'utilisation de la clé privée et du certificat correspondant ;
- informer l'AE de toute modification concernant les informations contenues dans le certificat ;
- faire, sans délai, une demande de révocation du certificat auprès de l'AE en cas de perte, ou de découverte d'une non-conformité, ou d'une suspicion de compromission de la clé privée ou des données d'activation, ou de cessation d'activité du service applicatif.

13. OBLIGATION DE VÉRIFICATION DES CERTIFICATS PAR LES APPLICATIONS UTILISATRICES

Les utilisateurs (personnes ou applications) utilisant les certificats doivent :

- Vérifier que le certificat a bien été émis par l'AC
- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Contrôler que le certificat signé par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- Pour chaque certificat de la chaine de certification, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (date de validité, statut de révocation) ;

Les certificats de la chaîne de confiance de l'AC et les LAR/LCR correspondantes sont disponibles 24h/24 7j/7 sur le site internet du Ministère de la Justice :

- le certificat de l'« AC Technique » ;
  - http://www.justice.gouv.fr/igc/sdit/mj_ac-technique.cer

- la LCR de l'« AC Technique » ;
  - http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl
- le certificat de l'« ACR Infrastructure Justice » signataire de l'« AC Technique » :
  - http://www.justice.gouv.fr/igc/sdit/mj_acr-infra_justice.cer
- la LAR de l'« ACR Infrastructure Justice » signataire de l'« AC Technique » :
  - http://www.justice.gouv.fr/igc/sdit/mj_arl-infrastructure.crl

14. LIMITE DE RESPONSABILITÉ DE L'AC

L'AC ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation, des LAR/CRL ainsi que de tout autre équipement ou logiciel mis à disposition.

L'AC décline en particulier sa responsabilité pour tout dommage résultant :

- d'un emploi des bi-clés pour un usage autre que ceux prévus ;
- de l'usage de certificats révoqués ou expirés ;
- d'un cas de force majeur tel que défini par les tribunaux français.

L'AC décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le RC.

L'AC ne pourra pas être tenu pour responsable pour les dommages résultant de réclamation de tiers, de perte de clientèle, d'arrêt de travail ou de tout autre dommage, notamment indirects ou engendrant une perte commerciale.

15. DONNÉES À CARACTÈRE PERSONNEL ET CONSERVATION DES DONNÉES

Toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi CNIL. Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les RC et les porteurs à l'AC ne doivent ni être divulguées ni transférées à un tiers sauf en cas de consentement préalable du porteur ou sur décision judiciaire ou autre autorisation légale.

De par sa nature, le Ministère de la Justice applique les lois en vigueur sur le territoire français, dans le cadre de la divulgation d'informations personnelles.

16. INTÉGRALITÉ DES CGU

Les parties reconnaissent que les présentes CGU constituent l'intégralité des accords entre elles en ce qui concerne la réalisation de l'objet des présentes, et annulent et remplacent tous accords et propositions antérieurs ayant le même objet quelle qu'en soit la forme.

17. RÈGLEMENTS DES LITIGES ET LOI APPLICABLE

Les présentes CGU sont soumises au droit français. Tout litige relatif à la validité, l'interprétation, l'exécution des présentes CGU sera soumis à la législation et de la réglementation en vigueur sur le territoire français.

18. AUDITS ET RÉFÉRENCES APPLICABLES

Un contrôle de conformité de l'« AC technique » à la PC et à la DPC qui lui sont applicables pourra être effectué, sur demande de l'Autorité Administrative de l'IGC PEKIN.

l'« AC technique » s'engage à effectuer ce contrôle tous les 3 ans à minima.