Conditions Générales d'Utilisation

PASS'IN

AC IMPRIMERIE NATIONALE SUBSTANTIEL PERSONNEL

AC IMPRIMERIE NATIONALE ÉLEVÉ PERSONNEL

Etat du document – Classification	Référence
Valide - Publique	Réf. OID PC : 1.2.250.1.295.1.1.8.6.1.101.1 1.2.250.1.295.1.1.8.6.1.102.1 1.2.250.1.295.1.1.20.7.1.102.1

Préambule

Le Groupe Imprimerie Nationale, à travers sa société IN Continu et Services (INCS), offre des services de fourniture de certificats ayant pour objectif la mise en œuvre de fonctions d'authentification et de signature, dans le cadre de la plateforme de gestion des identités numériques.
A ce titre, INCS a mis en place une Infrastructure de Gestion de Clés, baptisée « IGC Elevée », afin de délivrer des certificats répondant aux exigences suivantes :

- Des certificats d'authentification délivrés par l'AC Imprimerie Nationale Substantiel Personnel, conformes aux exigences du Référentiel Général de Sécurité niveau RGS** et aux exigences de la norme ETSI EN 319 411-1 niveau NCP+ ;
- Des certificats de signature délivrés par l'AC Imprimerie Nationale Substantiel Personnel, conformes aux exigences du Référentiel Général de Sécurité niveau RGS** et qualifiés QCP-n-QSCD au regard des exigences du Règlement européen eIDAS ;
- Des certificats de signature délivrés par l'AC Imprimerie Nationale Elevé Personnel, conformes aux exigences du Référentiel Général de Sécurité niveau RGS*** et qualifiés QCP-n-QSCD au regard des exigences du Règlement européen eIDAS.

INCS a été qualifiée, en sa qualité d'Autorité de Certification (et ci-après désignée "**AC**"), selon le schéma français, du Référentiel Général de Sécurité (ci-après désigné "**RGS**") jusqu'au niveau *** par un cabinet d'audit habilité, et est ainsi habilitée à délivrer, à renouveler et à révoquer des certificats électroniques conformes RGS ** et ***. Un audit de contrôle et de surveillance est mené chaque année par ce cabinet pour renouveler cette certification.

La qualification RGS est l'acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de service d'un prestataire de service de certification électronique aux exigences du RGS, pour un niveau de sécurité donné et correspondant au service visé par ce prestataire.
INCS est Prestataire de Service de Certification Électronique (PSCE).

INCS est également qualifiée Prestataire de Services de Confiance (PSCo) par l'Agence Nationale de la Sécurité des Systèmes d'Information (ci-après désignée l'« **ANSSI** »).

La qualification de conformité par rapport au Règlement eIDAS est l'acte par lequel l'ANSSI atteste de la conformité de tout ou partie de l'offre de service d'un prestataire de service de certification électronique aux exigences du Règlement eIDAS, pour un niveau de sécurité donné et correspondant au service visé par ce prestataire.

Les prestations et ces qualifications s'inscrivent dans le cadre des textes suivants, ainsi que des futurs textes participant de la réglementation future :

- La loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
- Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;
- Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;
- la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) ;
- l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation ;
- Règlement 2014/910 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;
- Le Règlement Général européen 2016/679 du 27 avril 2016 relatif à la Protection des Données.

Ce cadre vise à donner un niveau de reconnaissance juridique des signatures électroniques basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature, pouvant :

- répondre aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier
- être recevable comme preuves en justice;

Dès lors, le référentiel documentaire contractuel RGS du Groupe Imprimerie Nationale lié à sa certification RGS (et notamment, les Politiques de certification) et le référentiel documentaire contractuel eIDAS du Groupe Imprimerie Nationale lié à sa certification eIDAS (et notamment, les Politiques de certification) ainsi que les présentes Conditions Générales d'Utilisation constituent un ensemble contractuel qui s'impose au Client.

Le présent document définit les conditions générales d'utilisation de l'Autorité de Certification IGC Elevé d'INCS.

Il présente, en synthèse, les politiques de certification (ci-après les « **Politiques de Certification** » ou « **PC** ») pour les AC Fille Substantiel Personnel et Elevé Personnel référencée sous les OID suivants :

- AC Substantiel Personnel :
  - 1.2.250.1.295.1.1.8.6.1.101.1
  - 1.2.250.1.295.1.1.8.6.1.102.1
- AC Elevé Personnel :
  - 1.2.250.1.295.1.1.20.7.1.102.1

Glossaire

Client :	désigne l'entité personne morale qui acquiert un service de certification auprès de l'AC INCS Substantiel Personnel ou Elevé Personnel
Informations :	désigne les informations devant être publiées par l'IGC Elevé, à savoir la liste des certificats révoqués, la politique de certification, les conditions générales d'utilisation et les certificats des Autorités de Certification
Partie(s) :	désigne alternativement ou collectivement le Client et le Prestataire
Porteur :	désigne une personne physique, salarié, employé ou collaborateur du Client
Prestataire :	désigne INCS, entité du Groupe Imprimerie Nationale, en sa qualité d'AC

Conditions Générales d'Utilisation (CGU)

Contact de l'Autorité de Certification	Service SSI Rue des Frères Beaumont 59128 – Flers-en-Escrebieux SSI@imprimerienationale.fr
Type de certificats émis et politiques	Les certificats émis par l'AC IGC INCS sont des certificats de signature ou d'authentification pour les collaborateurs du Client et pour un usage sur les applications du Client ou nécessaires à la réalisation de ses missions. Le certificat de signature qualifié est référencé sous l'OID 1.2.250.1.295.1.1.20.7.1.102.1 Le certificat d'authentification est référencé sous l'OID 1.2.250.1.295.1.1.8.6.1.101.1 Le certificat de signature est référencé sous l'OID 1.2.250.1.295.1.1.8.6.1.102.1 Les certificats sont émis conformément aux politiques de certification de l'AC Renforcée Personnel et l'AC Standard Personnel disponibles à l'adresse suivante : http://www.imprimerienationale.fr/GIN/PC Les certificats des chaînes de certification sont disponibles aux adresses suivantes : AC Substantiel Personnel : http://www.imprimerienationale.fr/GIN/ACR.cer http://www.imprimerienationale.fr/GIN/ACF-SB-P.cer AC Elevé Personnel : http://www.imprimerienationale.fr/GIN/ACR.cer http://www.imprimerienationale.fr/GIN/ACF-EV-P.cer Toute application tierce souhaitant utiliser les certificats de la chaîne de certification doit en faire la demande préalable en écrivant au point de contact défini ci-dessus.
Objet des certificats	Les certificats émis par les AC Substantiel Personnel et Elevé Personnel sont des certificats à destination de Porteurs (personnes physiques) collaborateurs, salariés du Client (personne morale). Ces certificats sont stockés dans un dispositif de création de signature qualifiée (QSCD) remis à chaque Porteur individuellement.
Durée / Entrée en vigueur	Les présentes CGU sont opposables au représentant légal du Client, au Porteur et au mandataire de certification, dès leur acceptation par ces derniers. Ils se portent fort du respect de ces CGU par le Porteur du certificat. Les présentes CGU sont opposables pendant toute la durée du contrat de service de certification (ci-après désigné le « **Service** ») de mise en ligne des services, sans préjudice de leurs éventuelles mises à jour. L'AC s'engage à communiquer au représentant légal du Client, au Porteur et au mandataire de certification (ci-après désigné le « **Mandataire de Certification** » ou le « **MC** »), toutes nouvelles CGU, mises à jour. Toute utilisation des services par le représentant légal du Client, le Porteur et le mandataire de certification après modification des CGU vaut acceptation par ces derniers des nouvelles CGU. La fourniture des services de certification est subordonnée au paiement du prix

	convenu. Le contrat de service auquel s'appliquent les présentes CGU est reconductible automatiquement une fois, pour une durée de trois ans. En cas de non reconduction du contrat de service ou lorsque le Client ne s'est pas acquitté du prix du contrat de service, le contrat de service est résilié de plein droit. Les certificats ne sont alors plus utilisables et font l'objet d'une révocation par l'AC Fille après information du Client.
Collaboration	La nature des Services nécessite une étroite collaboration entre les Parties. Chacune des Parties s'engage à collaborer de bonne foi et en particulier à fournir à l'autre Partie l'ensemble des informations nécessaires et utiles pour l'exécution des Services.
Mise en garde	Le Prestataire met à la disposition du Client son savoir-faire et le conseille au vu des données fournies par celui-ci. Pour permettre au Prestataire de mener à bien ses prestations, le Client s'engage à mettre à la disposition du Prestataire tous les éléments nécessaires à la bonne connaissance de l'objet des prestations et de son environnement, à mettre le Prestataire en relation avec tous les membres de son personnel ou ses partenaires susceptibles de fournir au Prestataire ces éléments, et à mettre en place tous les moyens nécessaires (matériels et humains) pour que le Prestataire puisse accomplir les prestations. Ainsi, il appartient au Client de : • vérifier l'adéquation de son besoin au Service proposé par le Prestataire ; • s'assurer que les prérequis matériels, techniques et/ou logiciels requis par l'AC sont remplis avant d'utiliser le Service ; • disposer de toutes les compétences et moyens nécessaires pour utiliser les prestations, objets du Service ; • de s'assurer de l'exactitude des informations transmises. Sauf stipulation contraire, il incombe au Client de prendre en charge tous les moyens nécessaires pour assurer les liaisons de télécommunication entre ses propres équipements de traitement de données et ceux du Prestataire. Le Prestataire ne pourra être tenu pour responsable de la qualité de la liaison telecom et Internet du Client, mais s'engage à mettre en œuvre, en coopération avec le Client, tous les moyens utiles pour trouver une solution d'amélioration si une défaillance de liaison venait à intervenir. Le Client reconnaît, par ailleurs, avoir été informé des risques inhérents à l'utilisation du réseau Internet ainsi qu'à celle du Service tout particulièrement, en termes de : • non accessibilité aux Informations ; • suspension et/ou non accessibilité du Service ; • défauts de sécurité dans l'envoi ou la réception de messages tels que, notamment, non réception du message par son destinataire, contrôles de la validité du certificat de l'émetteur ou du récepteur ; • rapidité non garantie, dans l'exécution des transactions et dans la transmission des données, des mises à jour, des messages via le Service. Il est convenu que le Prestataire ne peut être tenu responsable d'éventuels dysfonctionnements des équipements appartenant au Client. Il n'est pas responsable des dysfonctionnements faisant suite à une utilisation du Service ou à une manipulation du Client qui ne serait pas conforme à la documentation du Service, ou

	aux instructions du Prestataire. De même, la responsabilité du Prestataire ne s'étend pas au bon fonctionnement (panne, erreur, incompatibilité, etc.) des matériels et logiciels du Client et de son environnement. Le Prestataire ne saurait être tenu responsable des conséquences dues à l'implantation, par le Client, de tous progiciels, logiciels ou système d'exploitation non compatibles avec les Services. Le Prestataire s'efforcera d'offrir au Client la meilleure disponibilité aux applications. Cette garantie ne saurait s'entendre d'une garantie absolue, en termes de disponibilité, de performance, d'accessibilité, compte tenu de la structure du réseau Internet. Le Prestataire pourra interrompre le Service pour des raisons de maintenance des applications.
Modalités d'obtention	Un Porteur peut obtenir un certificat de signature ou d'authentification suivant les scenarii d'enrôlements suivants : • **Présentation de la demande de certificat :** la présentation d'une demande de certificat doit émaner d'un MC mandaté par le représentant légal du Client. Une demande de certificat ne peut être présentée qu'avec le consentement préalable du futur Porteur et un dossier complet. • **Contrôle de la validité du dossier de demande de certificat par l'autorité d'enregistrement (AE)** : vérification de l'identité du Porteur, du Client, de la cohérence des justificatifs fournis, de la signature des CGU par le Porteur. • **Validation du dossier puis décision de rejet ou d'acceptation de la demande** - Rejet : l'AE informe le Porteur ou le MC. Cette notification est réalisée via le suivi de l'application en ligne - Acceptation : l'AC déclenche la génération et la préparation des éléments destinées au Porteur (création du support, génération de la bi-clé, du certificat de clé publique, et du code d'activation) Les demandes de certificats (cas de l'enregistrement d'un Porteur via un MC) nécessitent de fournir *a minima* les informations suivantes : • Identité du Porteur : - Prénom ; - Nom ; - Date de naissance ; - Photocopie d'une pièce d'identité officielle du futur Porteur en cours de validité (CNI, passeport, carte de séjour) ; • Adresse email du Porteur ; • Adresse postale et numéro de téléphone du Porteur (facultatif) ; • Identifiant unique de connexion du Porteur lui permettant l'accès au système d'information du Client (facultatif) • Un numéro unique est attribué par l'AC à chaque Porteur • Les CGU signées et paraphées par le futur Porteur ; • La demande de certificat mentionnant l'identité du futur Porteur, datée de moins de 3 mois et co-signée par le MC et le futur Porteur ; • Organisation du Porteur - Un Kbis ou certificat d'identification au répertoire national des entreprises et de leurs établissements ou inscription au répertoire des

	métiers ou avis de situation juridique de l'INSEE, attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat. Ces documents devront être conformes à la situation légale du Porteur (dernière état du Kbis, etc.…). - Pour une administration, une pièce valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative (les éventuelles délibérations, décrets et/ou arrêtés de nomination, désignation concernant l'autorité administrative)
Modalités de renouvellement	Le Porteur est averti de l'arrivée à expiration de son certificat par courriel 90, 60 et 30 jours avant l'expiration. Deux cas de renouvellement sont à distinguer : • le premier renouvellement du certificat qui ne nécessite pas de réémission de support (à condition que le certificat ne soit pas arrivé à échéance ou qu'il n'ait pas fait l'objet d'une révocation). Seul ce premier renouvellement peut faire l'objet d'une procédure simplifiée en ligne avec signature électronique de la demande de renouvellement et des CGU en cours de validité au moment de la demande. • Tout renouvellement s'effectue selon les mêmes conditions et selon les mêmes modalités que la demande initiale (fourniture d'un dossier de demande complet). Il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante qui sera générée par l'AC.
Modalités de révocation	Une demande de révocation de certificat peut émaner du Porteur du certificat, de n'importe quel MC du Client, du représentant légal du Client ou de l'AC émettrice du certificat ou d'une de ses composantes (AE). Le Porteur doit être informé par le MC du nom des personnes/entités susceptibles d'effectuer une demande de révocation de son certificat. **Révocation par le Porteur** La demande de révocation d'un certificat Porteur peut être faite, dans les meilleurs délais, selon les modalités suivantes : • **En ligne**, par le Porteur lui-même à l'adresse https://cms.pass-in.fr/cms-fo/page/operation/request/entry/revocation/revocation-support.xhtml après identification avec sa carte ; • Par un **appel téléphonique** au centre d'appel (au 0820 670 315) en fournissant son jeu de question réponse ; • Par **courrier** en envoyant le formulaire de demande de révocation à l'adresse suivante : Imprimerie Nationale - Service Autorité d'Enregistrement - TSA 21006 - 59359 Douai cedex - France; • Par **email** en envoyant le formulaire de demande de révocation à l'adresse suivante : passin.revocation@ingroupe.com Dans tous les cas, la révocation est effectuée par l'AE qui valide ainsi la demande. Si la demande est validée, le certificat est alors révoqué par l'AE dans un délai maximum de 24h. Le demandeur de la révocation est tenu informé, par l'envoi d'un courrier électronique, du bon déroulement de l'opération et de la révocation effective du certificat.

	Révocation suite au départ du Porteur du Client Le Porteur, le MC et/ou le représentant légal du Client doit faire la demande de révocation sans délai. Le Porteur, le MC et/ou le représentant légal du Client réalise cette demande de révocation : • **En ligne**, à l'adresse https://cms.pass-in.fr/cms-fo/page/operation/request/entry/revocation/revocation-support.xhtml après identification avec sa carte ; • Par un **appel téléphonique** au centre d'appel (au 0820 670 315) en fournissant son jeu de question réponse ; • Par **courrier** en envoyant le formulaire de demande de révocation à l'adresse suivante : Imprimerie Nationale - Service Autorité d'Enregistrement - TSA 21006 - 59359 Douai cedex - France; • Par **email** en envoyant le formulaire de demande de révocation à l'adresse suivante : passin.revocation@ingroupe.com L'AE procède, sans délai, à une validation de la demande de révocation. Une fois la demande authentifiée et contrôlée, le certificat est révoqué. Une notification de la révocation par courrier électronique est envoyée instantanément au Porteur, aux MC et/ou représentant légal du Client. L'AE complète, signe et archive le dossier de révocation. **Révocation d'urgence** Dans le cas d'une révocation d'urgence, le Porteur, le MC et/ou le représentant légal du Client doivent agir dans les plus prompts et brefs délais en utilisant les modalités suivantes : • **En ligne**, à l'adresse https://cms.pass-in.fr/cms-fo/page/operation/request/entry/revocation/revocation-support.xhtml après identification avec sa carte ; • Par un **appel téléphonique** au centre d'appel (au 0820 670 315) en fournissant son jeu de question réponse ; • Par **email** en envoyant le formulaire de demande de révocation à l'adresse suivante : passin.revocation@ingroupe.com Si la demande est validée, le certificat est alors révoqué par l'AE dans un délai maximum de 24h. Le demandeur de la révocation est tenu informé, par l'envoi d'un courrier électronique, du bon déroulement de l'opération et de la révocation effective du certificat.
Domaines d'utilisation du certificat	Les certificats émis par l'AC Substantiel Personnel, conformément à la PC de l'AC Substantiel Personnel, ne sont utilisables qu'à des fins d'authentification et de signature dans le cadre d'échanges dématérialisés. Les certificats émis par l'AC Elevé Personnel, conformément à la PC de l'AC Elevé Personnel, ne sont utilisables qu'à des fins de signature dans le cadre d'échanges dématérialisés. La signature d'un document avec un certificat de signature, outre (i) l'authentification du signataire (ii) l'intégrité des données ainsi signées et (iii) l'origine du document, permet également de garantir de manière probante sa date et la manifestation du consentement du signataire quant au contenu de ces données. Les certificats sont émis pour une durée de 3 ans, sauf révocation.

	Le Client se porte fort du respect de ces stipulations par les Porteurs.
Limites d'utilisation	L'utilisation de ces certificats est interdite : • au-delà de leur période de validité ; • s'ils ont été préalablement révoqués ; • si les AC Substantiel Personnel et Elevé Personnel qui les a émis ont cessé leur activité ; • Pour un quelconque usage, autre que ceux autorisés par la PC, tel que listés au point « Domaine d'utilisation des certificats ». Le Client se porte fort du respect de ces stipulations par les Porteurs.
Obligations des Porteurs	Les Porteurs de certificats sont responsables de la protection de leurs clés privées. Ils doivent pour cela les protéger par un code PIN. Le Porteur a le devoir de : • communiquer des informations exactes et à jour lors de son enrôlement et lors des demandes de renouvellement ; • signer et se conformer aux CGU qui lui sont remises lors de son enrôlement ; • n'utiliser les certificats délivrés par les AC Substantiel Personnel et Elevé Personnel qu'à des fins de d'authentification et de signature conformément aux Politiques de Certification des AC Substantiel Personnel et Elevé Personnel ; • appliquer la politique de protection de son certificat définie dans le guide d'utilisation des certificats remis à chaque Porteur avec son certificat initial ; • protéger sa clé privée par des moyens appropriés à son environnement ; • protéger les données d'activation de la bi-clé correspondante par un code PIN; • protéger l'accès au poste sur lequel est installé son certificat ; • informer l'AC de toute modification concernant les informations contenues dans son certificat ; • faire, sans délai, une demande de révocation de son certificat directement auprès de l'AE ou de l'AC dans les cas suivants : - compromission, suspicion de compromission, vol, perte de la clé privée, dysfonctionnement irréversible du support ; - les informations du Porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant la fin de validité du certificat ; - non-respect par le MC de ses obligations découlant de la PC, connu par le Porteur. • Arrêter toute utilisation du certificat et de la clé privée associée, en cas d'arrêt d'activité de l'AC, ou de révocation du certificat de l'AC par l'INCS, quelle que soit la cause de révocation. Il est à noter que le MC ou le représentant légal du Client pourront également demander la révocation des certificats dans les cas suivants : - erreur détectée dans le dossier d'enregistrement ; - non-respect par le Porteur de ses obligations découlant de la PC ; - non acceptation du certificat par le Porteur après sa délivrance ; - décès du Porteur, départ du Porteur (démission, licenciement, retraite …), cessation d'activité du Client ;

	- révocation du certificat de l'AC ; Il est également à noter que, conformément au paragraphe IV.4.1 « Démarche d'acceptation du certificat » de la PC, tout certificat pour lequel l'AE n'aura pas reçu la preuve d'acceptation par le Porteur dans un délai de 40 jours après réception de la carte, sera révoqué par l'AC.
Obligations de vérification des certificats par les Utilisateurs	Les Utilisateurs des certificats doivent : • Vérifier l'usage pour lequel le certificat a été émis ; • Vérifier que le certificat utilisé a bien été émis par l'AC Substantiel Personnel ou l'AC Elevé Personnel ; • Vérifier que le certificat n'est pas présent dans les listes de révocation des AC Substantiel Personnel et Elevé Personnel ; • Vérifier la signature du certificat, et de la chaîne de certification, jusqu'à l'AC « RACINE » ayant délivrée les certificats de l'AC Substantiel Personnel et de l'AC Elevé Personnel et contrôler la validité des certificats. La liste de révocation des certificats émis par les AC Substantiel Personnel et Elevé Personnel sont disponibles aux adresses suivantes : AC Substantiel Personnel : http://crl.imprimerienationale.fr/GIN/cert/ACF-SB-P.crl http://www.imprimerienationale.fr/GIN/CRL/cert/ACF-SB-P.crl AC Elevé Personnel : http://crl.imprimerienationale.fr/GIN/cert/ACF-EV-P.crl http://www.imprimerienationale.fr/GIN/CRL/cert/ACF-EV-P.crl A défaut de pouvoir consulter les listes de révocations aux adresses précédentes, il également possible d'en prendre connaissance aux adresses des répondeurs OSCP suivantes : AC Substantiel Personnel : http://ocsp-acf-sb-p.imprimerienationale.fr AC Elevé Personnel : http://ocsp-acf-ev-p.imprimerienationale.fr
Limite de responsabilité et de garantie	Les AC Substantiel Personnel et Elevé Personnel garantissent au travers de leurs services d'IGC: • Leur identification et authentification grâce à leur certificat signé par l'AC Racine ; • L'identification et l'authentification des Porteurs grâce aux certificats qu'elles leur délivrent ; • La gestion des certificats correspondants et des informations de validité des certificats selon les PC des AC Substantiel Personnel et Elevé Personnel. Ces garanties sont exclusives de toute autre garantie de l'AC. Il est expressément entendu que INCS ne saurait être tenue pour responsable ni d'un dommage résultant d'une faute ou négligence d'un Client et/ou de ses Porteurs ni d'un dommage causé par un fait extérieur ou un cas de force majeur, notamment en cas de : • Utilisation de la clé privée pour un autre usage que celui défini dans le certificat associé, la PC, et les CGU ;

- Utilisation d'un certificat pour une autre application que les Applications autorisées ;
- Utilisation d'un certificat pour garantir un autre objet que l'identité du Porteur ;
- Utilisation d'un certificat révoqué ;
- Mauvais modes de conservation de la clé privée du certificat du Porteur ;
- Utilisation d'un certificat au-delà de sa limite de validité ;
- Faits extérieurs à l'émission du certificat tels qu'une défaillance de l'application pour laquelle il peut être utilisé ;
- Cas de force majeure tels que définis par la législation française.

La responsabilité de l'AC peut seulement être engagée dans les cas limitativement énumérés ci-dessous (et ce sous réserve du respect par le Client des obligations mises à sa charge, et en particulier celles déléguées au Mandataire de certification):

- en cas de dommage direct prouvé causé à un Porteur ou une application / utilisateur de certificat à la suite d'un manquement aux procédures définies dans la PC et à la DPC associée, la faute de l'AC devant être dûment prouvée;
- en cas de compromission prouvée, entièrement et directement imputable à l'AC.

L'AC décline toute responsabilité à l'égard de l'usage qui est fait des certificats qu'elle a émis dans des conditions et à des fins autres que celles prévues dans sa PC ainsi que dans tout autre document contractuel applicable associé, en particulier :

- utilisation d'un certificat pour un usage autre que l'authentification et la signature du Porteur ou la protection de la messagerie électronique ;
- utilisation d'un certificat pour garantir un autre objet que l'identité du Porteur pour lequel il a été émis ;
- utilisation d'un certificat révoqué ;
- utilisation d'un certificat au-delà de sa limite de validité.

L'AC décline toute responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, et quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication.

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.

L'AC ne saurait être tenue responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de sa PC lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1218 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des juridictions françaises, les conflits sociaux, la défaillance du réseau ou des installations ou réseaux de télécommunications externes.

L'AC décline toute responsabilité concernant les dommages indirects (notamment tout préjudice financier ou commercial) qui, par conséquent, n'ouvrent pas droit à

	réparation. En tout état de cause, les éventuelles indemnisations que INCS en qualité d'AC pourrait être amenée à versée au titre d'un manquement prouvé à ses obligations ne sauraient dépasser le(s) montant(s) défini dans le contrat de services.
Audits et références applicables	Un contrôle de conformité de la PC pourra être effectué, sur demande du comité de surveillance de l'AC et sous la responsabilité du service de l'audit interne (ou service faisant office de) de l'AC. A ce titre, l'AC pourra auditer la conformité des opérations réalisées par le Mandataire de certification. L'AC s'engage à effectuer ce contrôle au minimum une fois par an. Par ailleurs, avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC fera également procéder à un contrôle de conformité de cette composante. Les AC Substantiel Personnel et Elevé Personnel ont aussi obtenu la qualification de leur offre de certificats électroniques de signature vis-à-vis du Règlement européen eIDAS ; L'AC Substantiel Personnel a également obtenu la conformité de son offre de certificat électroniques d'authentification au regard de la norme ETSI EN 319 411-1 au niveau NCP+.
Données à caractère personnel	Les données à caractère personnel recueillies par l'AC pour la réalisation des Prestations peuvent l'être directement auprès de la personne concernée ou indirectement auprès du représentant légal du Client ou du mandataire de certification. Conformément aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, ainsi qu'aux dispositions du Règlement Général UE 2016/679 du 26 avril 2016 relatif à la Protection des Données, les personnes concernées par la collecte de données à caractère personnel sont informées que : 1. Le responsable de traitement est le Client, c'est à dire l'employeur du Porteur de carte Pass'IN 2. Le traitement de données est mis en œuvre pour le compte du Client par l'Imprimerie Nationale, qui assure la fabrication, la personnalisation de la carte Pass'IN et la gestion de son cycle de vie (renouvellement, révocation, ..) 3. Le traitement a pour finalité le contrôle et/ou l'authentification d'accès physique et/ou logique aux locaux, matériels, outils, logiciels, applications informatiques, systèmes d'information du Client, employeur du Porteur de carte Pass'IN. Le traitement est mis en œuvre sur la base du contrat signé entre les Parties et selon le Référentiel Général de Sécurité 2.0 français, et le règlement (UE) 910/2014 et les normes afférentes EN 319 401, EN 319 411-1 et EN 319 411-2, fixant les exigences pour la qualification de certificats d'authentification et de signature, et la qualification de services de délivrance de certificats qualifiés de signature électronique. 4. Les données collectées sont conservées dans le traitement pendant une durée de 12 mois à l'issue de la durée de validité de la carte Pass'IN. Les dossiers de demande d'émission de carte Pass'IN sont archivés hors du traitement de données pendant 10 ans, selon les exigences du règlement (UE) 910/2014. 5. La personne concernée peut exercer ses droits d'accès, de rectification, de suppression, de limitation auprès de son employeur. La personne concernée a également le droit d'introduire une réclamation auprès de l'autorité de contrôle

	si elle considère que le traitement la concernant constitue une violation à la règlementation applicable relative à la protection des données personnelles. 6. Toutes les données collectées sont nécessaires à la réalisation de la carte Pass'IN, à son envoi et à l'envoi de son code d'activation à son porteur en conformité avec les processus décrits dans les Politiques de Certification. Si l'une des données est manquante ou absente, la délivrance de la carte Pass'IN sera impossible. Les données recueillies ne seront traitées que pour les finalités en vue desquelles elles ont été collectées. L'AC déclare et garantit que la collecte des données à caractère personnel dans le cadre des présentes ainsi que leurs traitements dont elle est responsable sont réalisés conformément aux dispositions de la règlementation applicable en matière de protection des données. L'AC assure la confidentialité et la sécurité des données collectées dans le cadre des présentes. L'AC met en œuvre des mesures techniques et organisationnelles de sécurité appropriées pour protéger les données. Les données ne sont divulguées qu'aux seules personnes ayant besoin d'y accéder dans le cadre de l'exécution des prestations. Les données pourront être transmises à l'opérateur technique de l'AC, qui respecte la même politique de confidentialité que l'AC.
Propriété intellectuelle et industrielle	Les Parties déclarent et garantissent avoir la libre disposition des marques, noms, dénominations, et autres signes distinctifs destinés à être utilisés dans le cadre des présentes. L'AC reste propriétaire des éléments tels que marques, noms, dénominations, et autres signes distinctifs destinés à être utilisés dans le cadre des présentes et, de manière générale, les éléments protégés par le droit de la propriété intellectuelle et industrielle.
Assurance	L'AC a souscrit, pour l'ensemble des dommages corporels, matériels et immatériels résultant de son activité, auprès d'une compagnie notoirement solvable une assurance couvrant les conséquences de sa responsabilité civile professionnelle.
Cession	Le Porteur ne peut pas céder ses droits liés à la Politique de Certification et aux présentes Conditions Générales d'Utilisation.
Loi applicable et règlement des litiges	La loi applicable aux CGU est la loi française. En cas de difficulté d'exécution des CGU et préalablement à la saisine de la juridiction compétente, la Partie la plus diligente adressera à l'autre Partie une lettre recommandée avec avis de réception décrivant le différend né entre les Parties (ci-après le « **Différend** ») et demandant la mise en place d'une procédure de résolution amiable du Différend dont le déroulement sera le suivant : • dans les dix jours de la réception de cette lettre, les représentants de chacune des Parties devront se rencontrer afin de trouver une issue amiable à leur Différend, • la procédure de résolution amiable ne pourra excéder soixante jours à compter de la réception de la lettre recommandée avec avis de réception décrivant le Différend, sauf accord exprès des Parties pour proroger ce délai, • toutes les informations échangées au cours de cette procédure de résolution amiable seront considérées comme confidentielles et ce, même si elles ne portent pas de mention de confidentialité ; les Parties pourront se faire assister

	de leur conseil, si elles le souhaitent, au cours des réunions de résolution amiable sous réserve d'en avertir l'autre Partie préalablement, • les décisions prises lors de cette procédure de résolution amiable ont valeur contractuelle, dès lors qu'un avenant ou un protocole transactionnel est signé par les représentants habilités des deux Parties. Toutefois, les Parties sont convenues qu'elles ne sont pas tenues d'appliquer la procédure de résolution amiable avant la mise en œuvre d'une procédure d'urgence ou conservatoire en référé ou par requête. Tout différend relatif à l'existence, la validité, la formation, l'exécution, l'interprétation ou la cessation des Services et des relations commerciales est, à défaut d'accord amiable, de la compétence exclusive du Tribunal de commerce de Paris. Cette clause s'applique également en cas de référé, de recours en garantie, de demande incidente ou de pluralité de défendeurs et quels que soient le mode et les modalités de paiement.

Visa du demandeur* :	Visa du RL ou MC (barrer la mention inutile) :
Nom :	Nom :
Prénom :	Prénom :
Date :	Date :

*Les CGU doivent être paraphées à chaque bas de pages (initiales) par les deux parties (Porteur et RL/MC).
Ces CGU doivent être signées par les deux parties dans les encarts prévus à cet effet (voir ci-dessus)
Cas particulier : si vous êtes le représentant légal et le demandeur en même temps ne signer que la partie Visa du demandeur.