Le présent document définit les conditions générales d'utilisation des certificats GO Workforce eIDAS proposés par IN Groupe. Cette version intègre les nouveaux profils de certificats (OIDs) applicables à compter du 1er janvier 2026 et la cessation d'émission des anciens profils au 31 décembre 2025.

**Définitions :**

Client : désigne l'entité personne morale qui acquiert un service de certification auprès des AC GO Workforce eIDAS.

Informations : désigne les informations devant être publiées par le Prestataire, 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 IN Groupe en sa qualité de Prestataire de Service de Confiance

## 1 Contact

Demande d'information :

IN Groupe - Responsable de l'AC
38 avenue de New York
75016 Paris
contact.passin@ingroupe.com

Demande de révocation:

Par **courrier/courriel** en envoyant le formulaire de demande de révocation disponible sur le portail https://crl.pass-in.fr/ à l'adresse suivante : IN Groupe - Service Autorité d'Enregistrement - TSA 21006 - 59359 Douai cedex - France; ou à l'adresse suivante : passin.revocation@ingroupe.com

Par un **appel téléphonique** au centre d'appel (au 0820 670 314) puis en fournissant un formulaire de demande de révocation pour confirmer la demande

## 2 Types de certificat et usages

Les certificats émis par les AC GO Workforce eIDAS ne sont utilisables qu'à des fins d'authentification et/ou 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
À compter du 01/01/2026, seuls les certificats correspondant aux nouveaux OID seront émis.
Les certificats existants émis avant cette date restent valides jusqu'à leur expiration.
La délivrance de certificats correspondant aux anciens OID cessera le 31/12/2025.
Les usages restent conformes aux types de certificat définis dans la présente section.

## 3 Limite d'usage

L'utilisation de ces certificats est interdite :

- ➲ au-delà de leur période de validité ;
- ➲ s'ils ont été préalablement révoqués ;
- ➲ si les AC GO Workforce eIDAS 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.
- ➲ Les limites d'usage s'appliquent aux certificats selon leur date de délivrance et leur OID.
- ➲ Aucun nouveau certificat correspondant aux anciens OID ne sera émis après le 31/12/2025.

## 4 Obligations des porteurs

Le Porteur a le devoir de : (1) communiquer des informations exactes et à jour lors de son inscription et lors des demandes de renouvellement ; (2) signer et se conformer aux CGU qui lui sont remises lors de son inscription; (3) n'utiliser les certificats délivrés par IN Groupe qu'à des fins de d'authentification et de signature conformément aux Politiques de Certification des AC GO Workforce eIDAS ; (4) appliquer la politique de protection de son certificat définie dans le guide d'utilisation des certificats remis à chaque Porteur avec son certificat initial ; (5) protéger sa clé privée par des moyens appropriés à son environnement ; (6) protéger les données d'activation nécessaires (code OTP) à la personnalisation de sa carte ; (7) protéger les données d'activation de la bi-clé correspondante par un code PIN; (8) protéger l'accès au poste sur lequel est installé son

certificat ; (9) informer l'AC de toute modification concernant les informations contenues dans son certificat ; (10) faire, sans délai, une demande de révocation de son certificat directement auprès de l'AE ou de l'AC dans les cas de compromission, suspicion de compromission, vol, perte de la clé privée, non-respect des présentes CGU ; (11) 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'IN Groupe, quelle que soit la cause de révocation ; (12) L'acceptation du certificat par le Porteur est collectée via une case à cocher à l'issue de la phase d'activation de sa carte. Il est de la responsabilité du Porteur de vérifier la cohérence des informations portées dans le certificat. Il est également à noter que tout certificat, qui ne fait pas l'objet d'une acceptation par le Porteur à l'issue de la phase d'activation, est systématiquement révoqué par l'AC. Les droits et obligations des porteurs s'appliquent uniquement aux certificats émis sous des OID valides au moment de la délivrance.

**5 Obligations des tiers utilisateurs**

Les Utilisateurs des certificats doivent : (1) Vérifier l'usage pour lequel le certificat a été émis ; (2) Vérifier que le certificat utilisé a bien été émis par une AC GO Workforce eIDAS ; (3) Vérifier que le certificat n'est pas présent dans les listes de révocation de l'AC correspondante; (4) Vérifier la signature du certificat, et de la chaîne de certification, jusqu'à l'AC « RACINE » ayant délivrée les certificats des AC GO Workforce eIDAS et contrôler la validité des certificats

**6 Limites de garanties et de responsabilités**

Les AC GO Workforce eIDAS garantissent :

- 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 applicables.

Ces garanties sont exclusives de toute autre garantie de l'AC.

Il est expressément entendu que IN Groupe 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 IN Groupe 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.
Les garanties et responsabilités s'appliquent uniquement aux certificats valides à la date de leur délivrance.
Les certificats émis sous d'anciens OIDs, pour lesquels la délivrance est cessée au 31/12/2025, conservent leur garantie jusqu'à expiration.

## 7 Politiques de certifications

À compter du 01/01/2026, l'AC **Imprimerie Nationale Substantiel Personnel** émet uniquement des certificats correspondant aux nouveaux profils de certificats qualifiés utilisant des clés RSA 3072 bits ou équivalentes.

**OID et statuts des certificats :**

- **1.2.250.1.295.1.1.8.6.1.101.1 (authentification)** – Retiré, plus d'émission possible
- **1.2.250.1.295.1.1.8.6.1.102.1 (signature)** – Retiré, tous les certificats révoqués suite à la perte de qualification du QSCD
- **1.2.250.1.295.1.1.8.0.1.101.0 (authentification)** – Valide, émission jusqu'au 31/12/2025
- **1.2.250.1.295.1.1.8.0.1.102.0 (signature)** – Valide, émission jusqu'au 31/12/2025
- **1.2.250.1.295.1.1.8.0.1.101.1 (authentification)** – Nouveau profil, effectif à partir du 01/01/2026
- **1.2.250.1.295.1.1.8.0.1.102.1 (signature)** – Nouveau profil, effectif à partir du 01/01/2026

Les certificats émis sous les anciens OID (1.2.250.1.295.1.1.8.6.1.101.1 et 1.2.250.1.295.1.1.8.6.1.102.1) ont été révoqués. Les certificats associés délivrés par paire (authentification et signature) ont également été révoqués.

Les certificats correspondant aux OID 1.2.250.1.295.1.1.8.0.1.101.0 (authentification) et 1.2.250.1.295.1.1.8.0.1.102.0 (signature) resteront émis jusqu'au 31 décembre 2025 inclus.

À partir du 01/01/2026, tous les certificats qualifiés nouvellement émis devront utiliser des clés RSA 3072 bits ou un algorithme équivalent offrant un niveau de sécurité comparable, tel que ECDSA P-256 ou supérieur. Les nouveaux profils de certificats sont identifiés par les OID 1.2.250.1.295.1.1.8.0.1.101.1 (authentification) et 1.2.250.1.295.1.1.8.0.1.102.1 (signature).

## 8 Politique de confidentialité

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 :

➲ Le responsable de traitement est IN Groupe dans le cadre de l'émission des cartes GO Workforce eIDAS

➲ Le traitement de données est mis en œuvre par IN Groupe, qui assure la fabrication, la personnalisation de la carte GO Workforce eIDAS et la gestion de son cycle de vie (renouvellement, révocation ...)

➲ L'AC collecte et traite des informations relatives aux personnes physiques identifiées dans les demandes de carte GO Workforce eIDAS afin d'emmètre des certificats. Il s'agit du Porteur, du mandataire de certification, du représentant légal du Client ainsi que les contacts pour la facturation du Client.

➲ Le traitement est mis en œuvre sur la base du contrat signé entre les Parties 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.

➲ 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 GO Workforce eIDAS. Les dossiers de demande d'émission de carte GO Workforce eIDAS sont archivés hors du traitement de données pendant 10 ans, selon les exigences du règlement (UE) 910/2014.

➲ La personne concernée a également le droit d'introduire une réclamation auprès du responsable de l'AC (voir contact) si elle considère que le traitement la concernant constitue une violation à la règlementation applicable relative à la protection des données personnelles.

➲ Toutes les données collectées sont nécessaires à la réalisation de la carte GO Workforce eIDAS, 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 GO Workforce eIDAS 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.

## 9 Politique de remboursement

Les politiques de remboursement sont définies par les conditions générales de ventes annexées à la commande ou par contrat spécifique entre le prestataire et le client.

## 10 Loi applicable, 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.

## 11 Référencements et audits

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 infrastructure ou suite à toute modification significative au sein d'une composante, l'AC fera également procéder à un contrôle de conformité de cette composante.
L'AC Substantiel Personnel a obtenu la qualification de son 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 et NCP+.
Les informations d'audit et de qualification s'appliquent aux certificats selon les OID valides au moment de leur émission.
Les audits complémentaires pour les nouveaux OID sont planifiés conformément aux procédures en vigueur.

| | |
|---|---|
| Nom : | Prénom : |
| Date : | |
| ATTESTE AVOIR PRIS CONNAISSANCE ET ACCEPTE LES PRESENTES CGU DES CERTIFICATS | |
| Signature du Porteur : | |