

# CONDITIONS GÉNÉRALES POUR LES ABONNÉS

## 1. Objet

Les présentes Conditions Générales ont pour objet de préciser le contenu et les conditions d'utilisation des Certificats Qualifiés et des Signatures Électroniques Avancées fournies lors de l'utilisation des Applications de Confiance. Les présentes conditions générales constituent donc un accord entre vous et le SPF Justice, dont le siège social est situé 115 Boulevard de Waterloo, 1000 Bruxelles, sous le numéro d'entreprise 0308.357.753. L'acceptation des présentes conditions générales est requise pour pouvoir utiliser les Applications de confiance.

## 2. Définitions

**Abonné** : l'utilisateur d'une Application de Confiance qui peut être porteur d'un certificat.

**Conditions générales** : les présentes conditions générales, y compris leurs annexes.

**Règlement eIDAS** : Règlement 910/2014 du 23 juillet 2014 relatif à l'identité électronique et aux services de confiance pour les transactions électroniques dans le marché intérieur.

**AC** : l'entité qui délivre et est responsable des certificats électroniques qualifiés (Autorité de Certification).

**Certificat** : un fichier électronique attestant l'identité de l'Abonné et qui est conforme aux exigences relatives aux Certificats Qualifiés pour Signatures Électroniques Avancées ou Signatures Électroniques Qualifiées visées à l'article 3.14 du Règlement eIDAS.

**Certificat qualifié** : un certificat qualifié tel que défini à l'article 3.15 du règlement eIDAS.

**Signature électronique avancée** : une signature électronique qui remplit les conditions d'une signature électronique avancée telles que prévues à l'article 3.11 du règlement eIDAS.

**AE** : l'entité chargée de vérifier l'identité et de recevoir et valider les demandes des Abonnés, à savoir appartenant au SPF Justice, ainsi que le personnel désigné par celui-ci (autorité d'enregistrement).

**Partie utilisatrice** : toute partie s'appuyant sur l'authenticité d'un Certificat qualifié, d'une Signature électronique avancée ou d'une Signature électronique qualifiée.

**Applications de confiance** : l'application JustSendSign, offerte par le SPF Justice, et qui utilise notamment les Certificats.

**Journaux d'événements** : toutes les données relatives aux événements (tels que les requêtes entrantes et sortantes) liés aux applications de confiance.

### **3. Utilisation des applications de confiance**

Avant que les Applications de confiance puissent être utilisées, l'Abonné doit être identifié. Ce processus est le suivant :

- L'identité de l'Abonné est authentifiée sur base de ses nom, prénom, adresse e-mail, et éventuellement de son Lieu de Travail et de sa Fonction et sur base de ses moyens d'identification électroniques.
- En cas d'authentification réussie, une paire de clés privée/publique est créée. Une clé privée et un identifiant d'utilisateur unique sont attribués à l'abonné, qui est ensuite confirmé par le certificat attribué.
- Cette identité est périodiquement revalidée.

Le Certificat attribué permet à l'Abonné de signer les documents nécessaires par le biais des Applications de Confiance au moyen d'une Signature Électronique Avancée.

### **4. Obligations de l'Abonné**

L'Abonné déclare et garantit qu'il est le propriétaire légitime des ressources d'identité qu'il utilise lors de l'utilisation des Applications de confiance.

L'Abonné s'engage à :

- fournir des informations exactes et à jour dans le processus d'identification, d'authentification ou de signature ;
- de communiquer au SPF Justice toute modification pertinente concernant les informations relatives à l'identité
- à garder secrètes les données confidentielles et sensibles qui lui sont fournies lors de la génération d'un Certificat et à ne pas les partager avec des tiers ;
- d'utiliser le Certificat et la clé privée exclusivement pour le placement de Signatures Électroniques Avancées dans l'environnement des Applications de Confiance ;
- adresser immédiatement une demande de révocation du Certificat délivré au SPF Justice si l'Abonné a connaissance en cas de perte ou de suspicion de compromission de sa clé privée ou de ses données d'activation, ou de son eID.

En outre, l'Abonné s'engage à ne prendre aucune des mesures suivantes à l'égard des Certificats émis et des Applications de confiance :

- Se livrer à des activités illégales (telles que des cyberattaques).
- La délivrance de nouveaux certificats ou la diffusion d'informations sur la validité des certificats.
- L'utilisation des Certificats délivrés à d'autres fins que la signature de documents dans le cadre de ses activités professionnelles au sein du Ministère de la Justice.
- Signature de documents via le Certificat qui peuvent avoir des conséquences indésirables (tels que des documents de test).

### **5. Révocation**

Pour révoquer un Certificat, l'Abonné doit :

- Soit contacter l'AE (SPF Justice) ou ses services physiques, soit via [JustSign\\_Registration\\_Authority@just.fgov.be](mailto:JustSign_Registration_Authority@just.fgov.be). Dans ce cas, l'AE identifiera le titulaire du Certificat si elle en a les moyens, ou elle révoquera elle-même le Certificat concerné ;
- Ou contactez le service d'assistance désigné par le SPF Justice. Dans ce cas, le service d'assistance identifiera le titulaire du certificat, révoquera le certificat s'il en a les moyens, ou transmettra la demande à l'AE correspondant.
- Ou contactez le service téléphonique 24h/24 et 7j/7 pour toute demande de révocation, numéro de téléphone disponible sur <https://pki.almerys.com/revoquer.html>.

## 6. Obligations des parties utilisatrices

Les Parties utilisatrices vérifieront la validité d'un Certificat ou d'une Signature électronique avancée en fonction des méthodes de vérification fournies.

Étapes de vérification qui doivent être effectuées par l'application qui utilise les certificats :

- Vérifier l'usage pour lequel le Certificat a été émis
- Vérifier que le certificat est émis par l'autorité de certification (AC) « BE-YS USER SIGNING CA NA »
- Vérifier l'accessibilité et l'accès à la liste des certificats révoqués (LCR) de l'autorité de certification « BE-YS USER SIGNING CA NA »
- Vérifier la signature du Certificat et la chaîne de certification jusqu'à la racine de l'AC « ALMERYS ROOT CA » et vérifier la validité des Certificats au regard des LCR des différentes AC. La chaîne de certificats de confiance et les LCR sont disponibles à l'adresse suivante : <https://Pki.be-ys.com>. L'information du statut de révocation au-delà de la durée de validité des certificats est publiée dans la LCR, les numéros de série des certificats révoqués ne sont jamais supprimés de la LCR. Ces informations sont disponibles 24h/24.

## 7. Disponibilité

Le SPF Justice s'engage à faire tous les efforts raisonnables pour offrir les services mentionnés dans les présentes Conditions Générales sans fournir aucune garantie. Toutefois, cette disponibilité peut être valablement limitée si cela est nécessaire pour ne pas compromettre la sécurité ou l'intégrité des services, ou si cela est nécessaire pour la maintenance technique ou pour des réparations.

## 8. Restrictions d'utilisation

Les certificats émis ne peuvent être utilisés que dans le cadre de la signature électronique avancée.

La durée de validité d'un certificat expire à la date d'expiration spécifiée ou lorsque le certificat est révoqué.

Les journaux d'événements sont conservés pendant une période de dix ans.

## **9. Durée et résiliation**

Le contrat entrera en vigueur à la date à laquelle l'Abonné accepte les présentes Conditions Générales. Le présent contrat est conclu pour la durée pendant laquelle l'Abonné est employé et reste employé au sein du Ministère de la Justice. À la cessation de cet emploi, le présent contrat prend fin de plein droit.

## **10. Responsabilité**

Le SPF Justice ne peut être tenu responsable de tout dommage ou perte résultant directement ou indirectement d'une utilisation non autorisée, incorrecte ou négligente des Certificats, de la clé privée, d'autres informations secrètes et/ou des Applications de confiance, telles que visées à l'article 4.

En aucun cas, le SPF Justice ne pourra être tenu responsable des dommages indirects, accidentels, particuliers, punitifs ou consécutifs (même s'il a été informé de la possibilité de tels dommages). Cela inclut, mais sans s'y limiter, la perte d'utilisation ou de données, la perte de revenus ou de bénéfices, ou tout dommage dû à une interruption d'activité, découlant de ou lié de quelque manière que ce soit aux Certificats ou aux Applications de confiance.

La responsabilité du SPF Justice n'est pas engagée en cas de force majeure à caractère permanent ou temporaire. Par force majeure, on entend tout événement ou circonstance échappant au contrôle raisonnable et sans faute de la partie concernée, qui empêche temporairement ou définitivement la partie concernée de remplir (davantage) ses obligations contractuelles. Ces événements ou circonstances comprennent, sans s'y limiter : les émeutes, les guerres, les actes de terrorisme ; séismes, incendies et autres catastrophes naturelles ; sabotage; grèves; épidémies ou pandémies ; interruptions et dysfonctionnements des installations informatiques, etc.

## **11. Traitement des données à caractère personnel**

Le SPF Justice traite les données à caractère personnel conformément au Règlement 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) et à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Le traitement des données à caractère personnel a pour seul but de remplir les tâches du SPF Justice en tant qu'AE et en tant que fournisseur des Applications de confiance. Le SPF Justice ne traitera pas les données à caractère personnel à des fins commerciales.

Conformément au RGPD, l'Abonné dispose d'un droit de copie et d'accès, de rectification, d'effacement, de limitation du traitement, d'opposition, de portabilité, ainsi que d'un droit d'opposition à la prise de décision automatisée.

## **12. Règlement des litiges, juridiction compétente et droit applicable**

Le présent contrat est régi par le droit belge.

Les demandes d'informations et les réclamations relatives aux services mentionnés dans les présentes conditions générales peuvent être adressées à [Just-Sign Management Authority@just.fgov.be](mailto:Just-Sign Management Authority@just.fgov.be). Dans la mesure du possible, les litiges seront réglés à l'amiable.

En l'absence d'accord amiable, toutes les réclamations découlant du présent contrat ou en relation avec celui-ci seront réglées exclusivement par les tribunaux belges situés à Bruxelles.

### **13.Documentation applicable**

Les documents et politiques suivants s'appliquent :

- [Site de publication du Certificate Authority](#)
- [site de publication de la Justice belge](#)

### **14.Divers**

Si une disposition ou une partie d'une disposition des présentes Conditions générales devait être nulle ou inapplicable, les autres dispositions des présentes Conditions générales et la partie restante de la disposition en question resteront pleinement en vigueur et de plein effet dans toute la mesure permise par la loi. La disposition nulle ou inapplicable est remplacée de plein droit par une disposition valide et exécutoire qui se rapproche le plus possible de la disposition originale en droit et en économie.