Conditions Générales d'Utilisation - YOUSIGN SAS - SIGN2 CA

1-Introduction

1.1 Présentation générale

Ce document définit les Conditions Générales d'Utilisation (CGU) des certificats délivrés dans le cadre du processus de signature électronique par l'Autorité de Certification « YOUSIGN SAS - SIGN2 CA ».

Ces CGU sont acceptées par le Porteur de certificat durant le processus de signature. Ce document a pour objectif de présenter de manière synthétique les exigences respectées par l'Autorité de Certification et qui sont définies plus explicitement dans la Politique de Certification de l'AC « YOUSIGN SAS – SIGN2 CA ».

Le Porteur de certificat est une personne physique.

Si le Porteur de certificat signe au nom et pour le compte d'une personne morale, il déclare avoir le pouvoir d'engager juridiquement cette personne morale dans le cadre de l'opération pour laquelle le processus de signature électronique est mis en œuvre.

1.2 Identification du document

Ce document est référencé par son numéro de version : 1.1.0.

Ce numéro est amené à évoluer de manière indépendante à l'OID de la Politique de Certification.

Cette version des CGU s'applique donc aux OID suivants :

- OID : 1.2.250.1.302.1.5.1.0 pour les certificats générés au niveau LCP de la norme EN 319 411-1,
- OID : 1.2.250.1.302.1.6.1.0 pour les certificats générés avec au moins un facteur d'identification du Porteur par une AE interne à Yousign,
- OID : 1.2.250.1.302.1.8.1.0 pour les certificats générés avec au moins un facteur d'identification du Porteur par une AE externe à Yousign.

Les éléments spécifiques à un OID seront précédés de l'OID entre crochets : [OID]. Plusieurs OID peuvent être spécifiés, ils sont séparés par des points-virgules.

1.3 Acronymes & définitions

AC	Autorité de Certification	En cryptographie, une Autorité de Certification (AC ou CA pour Certificate Authority en anglais) est un tiers de confiance permettant d'authentifier l'identité des Porteurs. Une autorité de certification délivre des certificats décrivant des identités numériques et met à disposition les moyens de vérifier la validité des certificats qu'elle a fourni.
AE	Autorité d'Enregistrement	Dans le cadre de la délivrance de certificats électroniques en vue notamment de mettre en œuvre la signature électronique, l'Autorité d'Enregistrement (généralement abrégée AE) est l'entité qui vérifie que les demandeurs ou les Porteurs de certificat sont identifiés, que leur identité est authentique et que les contraintes liées à l'usage d'un certificat sont remplies, tout cela conformément à la Politique de Certification.
CGU	Conditions Générales d'Utilisation	
CIL	Correspondant Informatique et Libertés	Vous pouvez exercer vos droits et obtenir communication des informations vous concernant, en adressant un e-mail à cil@yousign.fr
DPC	Déclaration des Pratiques de Certification	
IGC	Infrastructure à Gestion de Clés	Une infrastructure à clés publiques est un ensemble de composants physiques (ordinateurs, équipements cryptographiques logiciels ou matériel type HSM ou encore des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques.
LCP	Lightweight Certificate Policy	En français appelé "Politique de Certification Légère". Il s'agit du

		niveau de certification défini dans le contexte des normes européennes (EN 319 411-1).
OID	Object Identifier	L'OID ou Identificateur d'objet, est un identificateur alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques. L'objectif des OID est d'assurer l'interopérabilité entre différents logiciels.
PC	Politique de Certification	La Politique de Certification est un document important dans le cadre de la mise en œuvre des applications mettant en jeu une signature électronique. Couramment abrégée par le sigle PC la Politique de Certification est l'ensemble de règles, définissant les exigences auxquelles l'Autorité d'Enregistrement se conforme dans la mise en place de prestations adaptées à certains types d'applications. La Politique de Certification doit être identifiée par un OID défini par l'Autorité de Certification.
LRC	Liste de Révocation de Certificats	La Liste de Révocation de Certificats (CRL, Certificate Revocation List) est la liste des identifiants des certificats qui ont été révoqués ou invalidés et qui ne sont donc plus dignes de confiance.
HSM	Hardware Security Module	Le Module Matériel de Sécurité est un appareil considéré comme inviolable offrant des fonctions cryptographiques.
ISO	Nom court pour désigner un organisme de normalisation international.	Organisation internationale de normalisation.
URL	Uniform Resource Locator	Le sigle URL (de l'anglais Uniform Resource Locator, littéralement « localisateur uniforme de ressource »), auquel se substitue informellement l'expression adresse web, désigne une

	chaîne de caractères utilisée pour adresser les ressources d'internet.
YOUSIGN SAS - SIGN2 CA	"YOUSIGN SAS - SIGN2 CA" est le nom complet de l'Autorité de Certification (AC) de Yousign.
Certificat Électronique de Signature	Un certificat de signature électronique est un document sous forme électronique qui a pour but d'authentifier l'identité du Porteur, l'intégrité des documents échangés et l'assurance de non-répudiation. Le certificat va permettre de signer les documents qui seront présentés pour signature électronique.
Chaîne de Certification	Liste des Certificats Racines qui émettent les certificats associés aux Porteurs.
Clef Privée	La cryptographie asymétrique peut être illustrée avec l'exemple du chiffrement à clef publique et privée, qui est une technique de chiffrement, c'est-à-dire que le but est de garantir la confidentialité d'une donnée. Par convention, on appelle la clef de déchiffrement la Clef Privée et la clef de chiffrement la clef publique. La clef qui est choisie privée n'est jamais transmise à personne alors que la clef qui est choisie publique est transmissible sans restrictions.
Bi-clé	Il s'agit du couple de clefs dites "privée" et "publique". Ces éléments de cryptographique sont définis pour la notion de "Clef Privée".
Certificats Racines	En cryptographie et en sécurité informatique, un Certificat Racine est un certificat électronique qui identifie une Autorité de Certification.
Porteur	Il s'agit de la personne réalisant l'opération de signature électronique en tant que signataire.
Utilisateur	Il s'agit de la personne ouvrant le document PDF signé électroniquement. Il peut donc s'agir

	du Porteur mais aussi de toute autre personne ayant le document PDF signé électroniquement en sa possession.
Client de Yousign	Il s'agit de la personne ou la société ayant contractualisé aux services de signature électronique auprès de la société Yousign.

2-Conditions Générales d'Utilisation

Contact de l'Autorité de Certification	Gestion de l'AC Yousign Yousign SAS 8 allée Henri Pigis 14000 CAEN contact@yousign.fr
Type de certificats émis	Les CGU s'appliquent aux certificats spécifiés au paragraphe 1.2. Les certificats émis par l'AC sont des certificats de signature pour les Clients de Yousign dans le cadre du processus de signature électronique proposé par Yousign. Il s'agit de certificats éphémères générés par l'AC au nom du Porteur durant le processus de signature. Ces certificats ne peuvent être utilisés dans d'autres contextes. Les certificats sont émis à travers la Chaîne de Certification suivante : YOUSIGN SAS – ROOT2 CA | YOUSIGN SAS – SIGN2 CA Les certificats de la Chaîne de Certification sont disponibles à l'adresse suivante https://yousign.fr/fr/public/document.
Objet des certificats	Les certificats émis par l'AC sont des certificats à destination de personnes physiques. Ces certificats sont stockés dans un module de sécurité sous contrôle de l'AC et ne sont utilisables que durant la transaction de signature.
Modalités d'obtention	Le Porteur de certificat est une personne physique. [OID : 1.2.250.1.302.1.5.1.0] L'enregistrement d'un Porteur se fait directement auprès de YOUSIGN qui valide l'identité du Porteur grâce, au moins à sa pièce d'identité, son adresse e-mail et/ou son numéro de téléphone. [OID : 1.2.250.1.302.1.6.1.0 ; 1.2.250.1.302.1.8.1.0]

	La validation initiale de l'identité du Porteur est ainsi réalisée : l'AE valide au moins un critère d'identification du Porteur. Voici une liste non exhaustive des critères pouvant être vérifiés : code unique envoyé par email, code unique envoyé par SMS, validation d'une pièce d'identité, prise de photo du Porteur. ***Validation de l'identité d'un individu (Porteur) pour l'obtention d'un certificat*** [OID : 1.2.250.1.302.1.5.1.0] L'enregistrement du futur Porteur nécessite au moins la validation de sa pièce d'identité, de l'existence d'une adresse e-mail et/ou d'un numéro de téléphone personnels. Les pièces d'identité acceptées peuvent être les suivantes : - la carte d'identité, - le passeport, - la carte de séjour. Pour ce faire, nous réaliserons le processus suivant : ● utilisation d'une URL unique ; ● vérification de la pièce d'identité téléchargée par le Porteur ; ● envoi d'un Code d'authentification[1] ; Lorsque le futur Porteur s'est rendu sur l'URL unique, puis à, au moins, téléchargé sa pièce d'identité qui a été instantanément vérifiée et nous a fourni le Code d'authentification, son identité est validée. [OID : 1.2.250.1.302.1.6.1.0 ; 1.2.250.1.302.1.8.1.0] L'enregistrement du futur Porteur nécessite la vérification d'un paramètre d'identification. L'identification peut se faire de plusieurs manières. Voici une liste non exhaustive des critères pouvant être vérifiés : code unique envoyé par email, code unique envoyé par SMS, validation d'une pièce d'identité, prise de photo du Porteur. Pour ce faire, nous réaliserons le processus suivant : ● utilisation d'une URL unique ; ● identification du Porteur via le système choisi ; Lorsque le futur Porteur s'est rendu sur l'URL unique, a réalisé l'identification souhaitée, son identité est validée.

[1] Code d'authentification - code permettant d'authentifier un Porteur pour valider une signature, envoyé sur son numéro de téléphone ou sur son adresse e-mail personnels.

	Méthode pour accéder à la Clef Privée et utiliser le Certificat Électronique de Signature La Clef Privée est entièrement gérée, stockée et protégée par l'infrastructure Yousign. Néanmoins, nous mettons en œuvre des moyens techniques et organisationnels afin d'assurer que la Clef Privée ne sera utilisée que par le Porteur. En aucun cas Yousign pourra utiliser cette clef pour son propre usage ou pour le compte d'une autre personne que le Porteur. La Clef Privée est associée de manière logique au Porteur et ce dernier est le seul à posséder les données d'activation. En effet, pour pouvoir utiliser sa Clef Privée, le Porteur devra s'authentifier successivement via deux canaux : ● via l'obtention d'une URL unique ; ● via un Code d'authentification. Il convient de noter que l'obtention de l'URL unique est transparent pour le Porteur car celle-ci est soit transmise par e-mail lorsque le Porteur clique sur le bouton permettant d'accéder aux documents à signer ou bien de façon transparente si le processus de signature est imbriqué dans une application tiers gérée par le Client de Yousign. Notre architecture technique ne permet l'utilisation d'une Clef Privée qu'à condition que le Code d'authentification soit saisi par le Porteur. De plus, une signature réalisée via l'AC « YOUSIGN SAS - SIGN2 CA » n'est valable que si l'IGC Yousign peut attester le cycle complet d'une demande de signature via un ensemble de journaux, et de traces qui sont documentés. Ces journaux et traces sont archivés pendant 10 ans.
Modalités de renouvellement	Il n'y a pas de processus de renouvellement.
Modalités de révocation	La demande de révocation d'un certificat pourra se faire par téléphone ou par mail. Voici la procédure à suivre : ● Révocation via téléphone : le Porteur pourra contacter Yousign par téléphone afin de demander la révocation de son certificat. Pour ce faire, Yousign s'assure de son identité. Une série de 2 questions aléatoires concernant son identité sera posée au Porteur. Ces questions seront fondées sur les informations en possession de Yousign. La validation sera effective, suite à une confirmation obtenue via un autre canal que l'appel téléphonique. Par exemple, nous pouvons lui envoyer un lien de confirmation sur son adresse courrier électronique.

	● Révocation par courriel : le Porteur pourra contacter Yousign par mail afin de demander la révocation de son certificat. Pour ce faire, Yousign s'assure de son identité. Une série de 2 questions aléatoires concernant son identité sera posée au Porteur. Ces questions seront fondées sur les informations en possession de Yousign. La validation sera effective, suite à une confirmation obtenue via un autre canal que le mail. Par exemple, nous pouvons : o lui envoyer un code sur son numéro de téléphone o effectuer un appel téléphonique pour avoir une confirmation La révocation d'un certificat ne peut intervenir que durant la période de validité du certificat, soit pendant les 15 minutes après la génération du certificat. Cette période extrêmement courte entraîne le fait que le processus de révocation sera difficilement utilisable dans le cadre de la présente Politique de Certification.
Limites d'usages	Les certificats délivrés ne sont utilisables que pour les transactions de signature assurées par l'infrastructure Yousign. Les certificats des Porteurs ont une durée de validité de 15 minutes. Les clés privées correspondantes ont une durée de vie équivalente à la durée du processus de signature. Yousign conserve pendant 10 ans les journaux et les traces concernant la délivrance et l'utilisation des Clés Privées des Porteurs.
Obligations des Porteurs	Le Porteur a le devoir de : ● communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ; ● protéger ses données d'authentification ; ● accepter les présentes Conditions Générales d'Utilisation du service de signature Yousign ; ● vérifier que les données présentes dans le certificat du document signé qui lui est remis sont correctes ; ● demander le renouvellement de son certificat avec un délai raisonnable avant son expiration ; ● faire, sans délai, une demande de révocation de son certificat auprès de Yousign en cas de compromission ou de suspicion de compromission de ses données d'authentification. L'acceptation d'un certificat émis par l'AC est tacite dès la signature effectuée via le système de signature Yousign. Avant cette utilisation, le Porteur peut refuser la génération du certificat en interrompant le processus de signature. Si la Bi-clé avait déjà été

	générée, cette dernière est détruite de manière automatique par un processus technique.
Obligations de vérification des certificats par les Utilisateurs	Les Utilisateurs des certificats doivent : ● vérifier et respecter l'usage pour lequel un certificat a été émis ; ● pour chaque certificat de la Chaîne de Certification, du certificat du Porteur jusqu'à l'AC « YOUSIGN SAS – ROOT2 CA », vérifier la signature électronique (à l'aide d'un logiciel supportant les standards de la signature électronique) de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ; les Utilisateurs peuvent utiliser un fichier signé électroniquement par Yousign pour faire ces vérifications. Le contenu du certificat peut être vérifié et contrôlé. ● vérifier et respecter les obligations des Utilisateurs de certificats exprimées dans la PC.
Limite de responsabilité	Yousign ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme des données d'authentification, des certificats, des LCR, ainsi que de tout autre équipement ou logiciel mis à disposition. Yousign décline 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 Porteur. De plus, dans la mesure des limitations de la loi française, Yousign ne saurait être tenu responsable : ● d'aucune perte financière ; ● d'aucune perte de données ; ● d'aucun dommage indirect lié à l'utilisation d'un certificat ; ● d'aucun autre dommage. En toute hypothèse, la responsabilité de Yousign sera limitée, tous faits générateurs confondus et pour tous préjudices confondus, au montant payé à Yousign pour l'accès au service de signature et ce, dans le respect et les limites de la loi applicable.
Références documentaires	La Politique de Certification de l'AC « YOUSIGN SAS – SIGN2 CA » est accessible à l'adresse suivante : https://yousign.fr/fr/public/document La DPC est accessible sur demande à l'AC en utilisant les coordonnées fournies ci-dessus.
Conditions d'indemnisation	Sans objet
Loi applicable	Les présentes Conditions Générales d'Utilisation sont soumises au droit français.

Gestion des données à caractère personnel	Le Porteur est informé que la délivrance de certificats électroniques et l'exécution du processus de signature électronique suppose la mise en œuvre par Yousign de traitements de données à caractère personnel auquel le Porteur consent. Yousign est le Responsable des traitements. Le Porteur est informé que la communication de ses données est obligatoire et nécessaire pour prendre en compte sa demande et l'exécution du processus de signature électronique. Le Porteur dispose d'un droit d'accès, de modification, de rectification et de suppression aux données le concernant ainsi qu'un droit d'opposition auprès du CIL de Yousign. Les données à caractère personnel qui seront collectées ne seront pas transférées à des tiers, sauf aux entreprises chargées de la mise en œuvre des solutions Yousign aux côtés de Yousign. Yousign s'engage à garantir la confidentialité et la sécurité des données qui seraient concernées.
Audits et références applicables	L'Autorité de Certification " YOUSIGN SAS - SIGN2 CA " est certifiée conforme, pour les certificats issus selon la politique 1.2.250.1.302.1.5.1.0, à la norme EN 319 411-1 pour le niveau LCP. Yousign met en œuvre un Comité de Direction Technique Yousign. Celui-ci procède à la validation de la conformité de la DPC par rapport à la PC. Un contrôle de conformité est réalisé lors de la mise en service du système et suite à toute modification significative. De plus, un audit sera réalisé au moins tous les ans. Les audits sont réalisés en interne par du personnel de Yousign ou bien sous la forme d'une prestation auprès d'acteurs spécialistes de la sécurité des systèmes d'information et ayant des compétences reconnues dans le domaine de la signature électronique. Dans le cadre d'obtention de certifications des services de l'IGC, l'audit de certification est réalisé par une société externe dûment accréditée.
Convention sur la preuve	Pour chaque signature électronique réalisée, Yousign et le Porteur acceptent que : - les éléments d'identification utilisés afin de procéder à la signature électronique des documents, à savoir le nom et prénom du Porteur, le numéro de téléphone personnel utilisé, son adresse e-mail, le Certificat Électronique de Signature, les pièces justificatives, - les éléments d'horodatage , - les procédés utilisés pour signer électroniquement les documents (saisie du code de sécurité envoyé par sms par exemple), - le dossier de preuves contenant un ensemble de traces informatiques, soient admissibles devant les tribunaux et fassent preuve des données et des éléments qu'ils contiennent ainsi que des procédés d'authentification qu'ils expriment. Ce dossier sera ensuite archivé et horodaté par le tiers archiveur.
Archivage auprès d'un tiers archiveur	L'ensemble des documents signés électroniquement seront archivés, auprès d'un tiers archiveur (CDC ARKHINEO), dans des conditions de nature à garantir la sécurité et l'intégrité dans le temps, conformément aux exigences de l'article 1367 du Code civil.

	Le Porteur peut, à tout moment, demander à Yousign une copie des documents signés électroniquement .