

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 le niveau LCP de la norme ETSI 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

AC	Autorité de Certification
AE	Autorité d'Enregistrement
CGU	Conditions Générales d'Utilisation
CIL	Correspondant Informatique et Libertés
DPC	Déclaration des Pratiques de Certification
IGC	Infrastructure à Gestion de Clés
LCP	Lightweight Certificate Policy
OID	Object Identifier
PC	Politique de Certification
LRC	Liste de Révocation de Certificats

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	<p>Les CGU s'appliquent aux certificats spécifiés au paragraphe 1.2.</p> <p>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.</p> <p>Les certificats sont émis à travers la chaîne de certification suivante :</p> <p style="text-align: center;">YOUSIGN SAS – ROOT2 CA YOUSIGN SAS – SIGN2 CA</p> <p>Les certificats de la chaîne de certification sont disponibles à l'adresse suivante https://yousign.fr/fr/public/document.</p>

Objet des certificats	<p>Les certificats émis par l'AC sont des certificats à destination de personnes physiques.</p> <p>Ces certificats sont stockés dans un module de sécurité sous contrôle de l'AC et ne sont utilisables que durant la transaction de signature.</p>
Modalités d'obtention	<p>Le porteur de certificat est une personne physique. [OID : 1.2.250.1.302.1.5.1.0]</p> <p>L'enregistrement d'un porteur se fait directement auprès de YOUSIGN qui valide l'identité du porteur grâce à sa pièce d'identité, son adresse 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]</p> <p>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 signataire.</p> <p><i>Validation de l'identité d'un individu pour l'obtention d'un certificat</i></p> <p>[OID : 1.2.250.1.302.1.5.1.0]</p> <p>L'enregistrement du futur porteur nécessite la validation de sa pièce d'identité, de l'existence d'une adresse mail et/ou d'un numéro de téléphone.</p> <p>Les pièces d'identité acceptées sont :</p> <ul style="list-style-type: none"> - la carte d'identité, - le passeport, - la carte de séjour. <p>Pour ce faire, nous réaliserons le processus suivant :</p> <ul style="list-style-type: none"> • utilisation d'une URL unique ; • vérification de la pièce d'identité envoyée par le porteur ; • envoi d'un Code d'authentification¹ ; <p>Lorsque le futur porteur s'est rendu sur l'URL unique, a téléchargé sa pièce d'identité qui a été instantanément vérifiée et nous a fourni le Code d'authentification, son identité est validée.</p>

¹ Code d'authentification - code permettant d'authentifier un porteur pour valider une signature.

	<p>[OID : 1.2.250.1.302.1.6.1.0 ; 1.2.250.1.302.1.8.1.0]</p> <p>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 signataire.</p> <p>Pour ce faire, nous réaliserons le processus suivant :</p> <ul style="list-style-type: none"> • utilisation d'une URL unique ; • identification du signataire via le système choisi ; <p>Lorsque le futur porteur s'est rendu sur l'URL unique, a réalisé l'identification souhaitée, son identité est validée.</p> <p><i>Méthode pour accéder à la clé privée et utiliser le certificat de signature</i></p> <p>La clé privée est entièrement gérée, stockée et protégée par l'infrastructure Yousign.</p> <p>Néanmoins, nous mettons en œuvre des moyens techniques et organisationnels afin d'assurer que la clé privée ne sera utilisée que par le porteur. En aucun cas Yousign pourra utiliser cette clé pour son propre usage ou pour le compte d'une autre personne que le porteur.</p> <p>La clé privée est associée de manière logique au porteur et ce dernier est le seul à posséder les données d'activation.</p> <p>En effet, pour pouvoir utiliser sa clé privée, le porteur devra s'authentifier successivement via deux canaux :</p> <ul style="list-style-type: none"> • via l'obtention d'une URL unique ; • via un Code d'authentification. <p>Notre architecture technique ne permet l'utilisation d'une clé privée qu'à condition que le Code d'authentification soit saisi par l'utilisateur. 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.</p>
Modalités de renouvellement	Il n'y a pas de processus de renouvellement.
Modalités de	La demande de révocation d'un certificat pourra se faire par téléphone ou par mail. Voici la procédure à suivre :

<p>révocation</p>	<ul style="list-style-type: none"> • Révocation via téléphone : l'utilisateur 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 : l'utilisateur 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 : <ul style="list-style-type: none"> ○ lui envoyer un code sur son numéro de téléphone ○ effectuer un appel téléphonique pour avoir une confirmation <p>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.</p> <p>Cette période extrêmement courte entraîne le fait que le processus de révocation sera difficilement utilisable dans le cadre de la présente Politique de Certification.</p>
<p>Limites d'usages</p>	<p>Les certificats délivrés ne sont utilisables que pour les transactions de signature assurées par l'infrastructure Yousign.</p> <p>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.</p> <p>Yousign conserve pendant 10 ans les journaux et les traces concernant la délivrance et l'utilisation des clés privées des porteurs.</p>
<p>Obligations des porteurs</p>	<p>Le porteur a le devoir de :</p> <ul style="list-style-type: none"> • communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ; • protéger ses données d'authentification ; • accepter les conditions d'utilisation du service de signature Yousign ; • vérifier que les données présentes dans le certificat du document

	<p>signé qui lui est remis sont correctes ;</p> <ul style="list-style-type: none"> • 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. <p>L'acceptation d'un certificat émis par l'AC est tacite dès la signature effectuée via le système de signature Yousign.</p> <p>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.</p>
Obligations de vérification des certificats par les utilisateurs	<p>Les utilisateurs des certificats doivent :</p> <ul style="list-style-type: none"> • 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 numérique 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 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	<p>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.</p> <p>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.</p> <p>De plus, dans la mesure des limitations de la loi française, Yousign ne saurait être tenu responsable :</p> <ul style="list-style-type: none"> • d'aucune perte financière ; • d'aucune perte de données ; • d'aucun dommage indirect lié à l'utilisation d'un certificat ; • d'aucun autre dommage. <p>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.</p>
	<p>La Politique de Certification de l'AC « YOUSIGN SAS – SIGN2 CA » est</p>

Références documentaires	<p>accessible à l'adresse suivante : https://yousign.fr/fr/public/document</p> <p>La DPC est accessible sur demande à l'AC en utilisant les coordonnées fournies ci-dessus.</p>
Conditions d'indemnisation	Sans objet
Loi applicable	<p>La présente Politique de Certification est soumise au droit français.</p> <p>En cas de litige entre les parties découlant de l'interprétation, l'application et/ou l'exécution du contrat et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée au tribunal de commerce de Caen.</p>
Gestion des données à caractère personnel	<p>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.</p> <p>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.</p>
Audits et références applicables	<p>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 ETSI 319 411-1 pour le niveau LCP.</p> <p>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.</p> <p>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.</p> <p>Dans le cadre d'obtention de certifications des services de l'IGC, l'audit de certification est réalisé par une société externe dument accréditée.</p>