Conditions Générales d'Utilisation de l'AC YOUSIGN SAS - QUALIFIED SIGNATURE CA

v1.2.5 | Diffusion : C1 - Public

HISTORIQUE DES VERSIONS			
Version	**Objet de la modification**	**Date**	**Auteur**
1.2.5	Modification de la raison sociale de Yousin par Youtrust (section Présentation générale et ensemble du document) ; Refonte du parcours d'enregistrement du porteur (section Types de certificats, procédures de validation et restrictions d'usage) ; Suppression des services **[Face à face physique]** : OID 1.2.250.1.302.1.11.1.0 et **[Face à face à distance]** : OID : 1.2.250.1.302.1.15.1.0 ; Généralisation de la terminologie "PVID" vers un vocabulaire multi-fournisseur ; Changement d'adresse du siège social (section Point de contact).	2 juil. 2026	Tony DUFOUR
1.2.4	Changement de la durée de vie des certificats des porteurs à 60 minutes (15 minutes auparavant).	Jan 23, 2024	Tony DUFOUR
1.2.3	Modification mise en page	3 oct. 2023	Sid Ahmed Re...
1.2.2	Complétion des acronymes et ajout des traductions le cas échéant (section acronymes) Mise à jour de l'adresse postale (section conditions générales d'utilisation, rubrique point de contact) Remplacement du terme "client" par "porteur" (section conditions générales d'utilisation, rubrique types de certificats, procédures de validation et restrictions d'usage) Ajout d'une référence vers la Politique de Certification décrivant le processus de révocation et suppression des informations redondantes avec celle-ci (section conditions générales d'utilisation, rubrique types de certificats, procédures de validation et restrictions d'usage)	9 mai 2023	Adrien Van De... Tony Belot

	Ajout d'obligations pour le porteur relatives à la conservation et au partage de la clé privée d'authentification (section conditions générales d'utilisation, rubrique obligations des porteurs) Ajout des liens vers les LCR de `YOUSIGN SAS - QUALIFIED SIGNATURE CA` (section conditions générales d'utilisation, rubrique vérification du statut des certificats) Précision quant à la limite de l'exonération de dommages et intérêts (section conditions générales d'utilisation, rubrique limite de responsabilité) Renommage de la rubrique (section conditions générales d'utilisation, rubrique confidentialité) Suppression de la référence locale pour la législation et la réglementation en vigueur (section conditions générales d'utilisation, rubrique confidentialité) Remplacement des tribunaux compétents de Caen par Paris (section conditions générales d'utilisation, rubrique loi applicable et résolution des conflits) Revue du contenu de la rubrique et ajout d'un pointeur vers la Politique de Confidentialité en ligne (section conditions générales d'utilisation, rubrique gestion des données à caractère personnel) Corrections mineures de fautes d'orthographe et de formulations		
1.2.1	Suppression du champ qualifié `esi4-qcStatement-5` de la section conditions générales d'utilisation, rubrique audit et certification	27 janv. 2023	Sid Ahmed Re...
1.2.0	Ajout d'une notion quant à l'acceptation des présentes CGU par les signataires, conditionnant l'obtention d'un certificat (section présentation générale) Référencement des différentes politiques de certification selon l'OID (section identification du document)	4 janv. 2023	Tony Belot

	Ajout du terme QSCD (section acronymes) Mise à jour de l'adresse postale de la société Yousign (section conditions générales d'utilisation, rubrique point de contact) Ajout des certificats qualifiés de signature électronique qualifiée, de type QCP-n-qscd, avec l'OID 1.2.250.1.302.1.16.1.0 (section conditions générales d'utilisation, rubriques types de certificats, procédures de validation et restrictions d'usage et accords applicables et pratiques de certification) Ajout de l'obligation pour le porteur d'enregistrer un moyen d'authentification dans le cas de l'OID 1.2.250.1.302.1.11.1.0 (section conditions générales d'utilisation, rubrique types de certificats, procédures de validation et restrictions d'usage) Ajout de l'attribut UID dans les DN dans le cas de l'OID 1.2.250.1.302.1.16.1.0 (section conditions générales d'utilisation, rubrique types de certificats, procédures de validation et restrictions d'usage) Modification du composant responsable de la comparaison des nom et prénom fournis par l'AE (section conditions générales d'utilisation, rubrique types de certificats, procédures de validation et restrictions d'usage) Précision de la durée de conservation des dossiers d'enregistrements des porteurs (section conditions générales d'utilisation, rubrique limites d'utilisation) Ajout des obligations des porteurs pour les OID 1.2.250.1.302.1.15.1.0 et 1.2.250.1.302.1.16.1.0 (section conditions générales d'utilisation, rubrique obligations des porteurs) Ajout des documents applicables en lien avec le PVID (section conditions générales d'utilisation, rubrique accords applicables et pratiques de certification)		

	Ajout des qualifications et certifications applicables au Remote QSCD et au PVID (section conditions générales d'utilisation, rubrique audit et certification) Ajout des niveaux de certificat et des champs qualifiés supplémentaires (section conditions générales d'utilisation, rubrique audit et certification) Correction d'erreurs typographiques dans les champs qualifiés supplémentaires (section Conditions Générales d'Utilisation, rubrique Audit et certification)		
1.1.1	Ajout des adresses de diffusion des informations de révocation de l'AC, par exemple en cas de compromission de celle-ci (section vérification du statut des certificats)	28 juil. 2022	Tony Belot
1.1.0	Modification de la mise en page Ajout du face à face à distance Mise à jour de la clause "Gestion des données à caractère personnel" en ce qui concerne les droits du porteur Vérification du certificat complétée en lien avec la Trusted List eIDAS Mise à jour et complétion des obligations du porteur Correction des URL de publication des CRL Précision des coordonnées d'envoi des demandes de révocation	27 mai 2022	Tony Belot
1.0.4	Mise à jour des acronymes Modification de l'adresse email de contact de l'autorité de certification Mise à jour de la clause "Limite de responsabilité" Ajout des clauses "Gestion des données à caractère personnel" et "Langue"	21 déc. 2020	yves.rocha@y...
1.0.3	Mise à jour de Vérification du statut des certificats. Précision sur la réponse OCSP.	22 sept. 2020	Kévin Dubourg

1.0.2	Modification mise en page	18 août 2020	Florent Eudeli...
1.0.1	Mise à jour des responsabilités du porteur et ajout d'un test de signature lors de l'enregistrement du porteur	2 nov. 2018	Antoine Louiset
1.0.0	Création du document	25 sept. 2018	Antoine Louiset

Table des matières

1. Introduction **6**
1.1. Présentation générale 6
1.2. Identification du document 7
1.3. Acronymes 7
2. Conditions Générales d'Utilisation **8**

1. Introduction

1.1. Présentation générale

La société Youtrust est un Prestataire de Service de Certification Électronique (PSCE) qui fournit auprès de ses clients et pour son usage propre des services impliquant des certificats électroniques et en particulier une signature électronique.

Dans ce cadre, ce document constitue les Conditions Générales d'Utilisation des certificats délivrés par l'Autorité de Certification « YOUSIGN SAS - QUALIFIED SIGNATURE CA ». Ce document présente les modalités de gestion des certificats ainsi que les engagements et les obligations des différentes parties.

Le porteur de certificat accepte explicitement ces Conditions Générales d'Utilisation dans la phase de demande du certificat. Dans le cas contraire, aucun certificat ne peut lui être délivré par l'Autorité de Certification « YOUSIGN SAS - QUALIFIED SIGNATURE CA ».

La société Youtrust a été dénommée Yousign jusqu'au 01/07/2026, date à laquelle sa dénomination sociale a été modifiée au RCS sans changement de SIREN. De ce fait, les Autorités de Certification portent le nom de Yousign et conservent un identifiant correct de la personne morale Youtrust.

1.2. Identification du document

Les présentes « Conditions Générales d'Utilisation » se rapportent à l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA » qui délivre des certificats selon sa Politique de Certification.
Les profils de certificats sont identifiés par leurs OID respectifs :

- **[Signature qualifiée]** : OID 1.2.250.1.302.1.16.1.0

D'autres éléments, plus explicites, (nom, numéro de version, date de mise à jour) permettent également de l'identifier.

1.3. Acronymes

Acronyme	Signification	Traduction
AC	Autorité de Certification	-
AE	Autorité d'Enregistrement	-
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	-
CGU	Conditions Générales d'Utilisation	-
DN	Distinguished Name	Nom distinctif
DPC	Déclaration des Pratiques de Certification	-
DPO	Data Protection Officer (Délégué à la Protection des Données)	-
eIDAS	electronic IDentification, Authentication and trust Services	Identification électronique et services de confiance
IGC	Infrastructure à Gestion de Clés	-
LAR	Liste des certificats d'AC Révoqués	-
LCR	Liste des Certificats Révoqués	-
OCSP	Online Certificate Status Protocol	Protocole de vérification de certificat en ligne
OID	Object Identifier	Identifiant d'objet
PC	Politique de Certification	-
PVID	Prestataire de Vérification d'Identité à Distance	-
QCP-n	Policy for EU qualified certificate issued to a natural person (politique pour les certificats qualifiés délivrés à une personne physique)	-
QSCD	Qualified Signature Creation Device	Dispositif de création de signature électronique qualifié

2. Conditions Générales d'Utilisation

Les présentes CGU sont basées sur le modèle prévu par l'annexe A de la norme EN 319 411-1 (version 1.3.1).

Point de contact	Youtrust Gestion de l'AC Yousign 36 rue de Saint Petersbourg 75008 Paris authority@yousign.com
Types de certificats, procédures de validation et restrictions d'usage	Les certificats couverts par les présentes CGU sont émis par la chaîne d'Autorité de Certification suivante : ● AC Racine : « YOUSIGN SAS - ROOT2 CA » ○ AC Émettrice : « YOUSIGN SAS - QUALIFIED SIGNATURE CA » L'AC délivre des certificats qualifiés éphémères, utilisés selon le processus, pour la signature électronique qualifiée à distance ou la signature électronique avancée au sens du règlement eIDAS. Les certificats qualifiés pour la signature électronique qualifiée à distance sont remis après une vérification initiale d'identité à distance. La clé privée du porteur est générée et utilisée dans un dispositif qualifié de création de signature à distance (Remote QSCD). Le porteur peut enregistrer un moyen d'authentification forte, conforme aux exigences des moyens d'identification électronique du niveau substantiel, permettant d'obtenir de nouveaux certificats de signature électronique qualifiée à distance. Ces certificats portent l'OID 1.2.250.1.302.1.16.1.0, et lorsque des règles s'appliquent spécifiquement à ce type de certificat, elles sont identifiées dans ce document par la mention **[Signature qualifiée]**. Les certificats ne peuvent être utilisés que dans le cadre du service de signature proposé par Youtrust, pour signer un document ou un message dans tous les domaines pour lesquels une signature est requise à titre de validité ou de preuve et en particulier : ● signature électronique par un porteur, puis vérification de cette signature par une administration ou une entreprise par voie électronique ; ● signature électronique par un porteur, puis vérification de cette signature par une personne physique. Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du

consentement du signataire quant au contenu de ces données. La signature électronique qualifiée est de plus présumée fiable et est équivalente, au titre du règlement eIDAS, à une signature manuscrite.

Le porteur est une personne physique.

Les DN sont construits de la façon suivante :

Attribut	Description	Présence
CN	commonName : Nom et prénom du porteur	Oui
SN	surname : Nom du porteur	Oui
GN	givenName : Prénom du porteur	Oui
OI	organizationIdentifier : Identifiant de l'entité avec laquelle le porteur est en lien, selon la syntaxe eIDAS : NTRFR-<numéro de SIREN>	Uniquement en cas de lien avec une personne morale
OU	organizationUnit : Identifiant de l'entité avec laquelle le porteur est en lien, selon la syntaxe RGS : 0002 <numéro de SIREN>	
O	organizationName : Nom de l'entité avec laquelle le porteur est en lien	
C	countryName : Pays de l'autorité d'enregistrement de Youtrust, toujours égal à FR (France)	Oui
SerialNumber	serialNumber : Date et heure de lancement de la génération du certificat.	Oui
UID	userIdentifier : Identifiant de transaction du signataire dans l'infrastructure Youtrust.	[Signature qualifiée] uniquement

	Les certificats de test émis par l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA » sont identifiables immédiatement par l'ajout du préfixe « TEST – » dans la valeur de l'attribut CN, par exemple : CN = TEST – Jean DUPONT,... En dehors de cette spécificité, les certificats de tests émis par l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA » suivent les mêmes processus que les certificats de production nominale. La mise en œuvre d'un certificat qualifié nécessite un processus de vérification de l'identité du porteur. **1. Cas de la validation avec un document d'identité physique** La validation initiale de l'identité du porteur est réalisée sur le site Web de l'AE lors d'un face à face à distance. Le processus de vérification à distance comprend les étapes suivantes : ● le porteur se connecte sur le site de l'AE via un lien unique qu'il a reçu sur son adresse email, et doit s'assurer de disposer d'un smartphone équipé d'une caméra ; ● l'AE affiche au porteur les informations d'identité utilisées pour sa demande de certificat : ○ nom et prénom ; ○ adresse de messagerie électronique ; ● le porteur confirme avoir pris connaissance des conditions générales d'utilisation en vigueur et accepte de les signer sans réserve ; ● le porteur confirme l'exactitude des informations présentées et consent à signer le formulaire de demande de certificat établi sur cette base ; ● si le porteur n'est pas sur un appareil mobile, il lui est demandé de poursuivre son identification sur un appareil mobile (équipé d'une caméra), via un QR code à scanner ou via la réception d'un SMS ;

	• la vérification d'identité à distance est réalisée par un prestataire PVID certifié (impliquant une validation par un opérateur humain), et intègre les étapes suivantes : ○ le porteur accepte les CGU et la politique de confidentialité du service PVID et consent au traitement de ses données biométriques afin que le PVID puisse s'assurer de son identité ; ○ le porteur s'assure de disposer d'un ordiphone respectant les exigences exposées par le PVID ; ○ le porteur présente à la caméra un document officiel d'identité en cours de validité parmi les justificatifs suivants : ○ la carte d'identité ; ○ le passeport ; ○ la carte de séjour ; et suit les consignes successives données par le PVID ; ○ le PVID vérifie la validité et l'authenticité du document présenté, et en extrait les informations d'identité du porteur ; ○ le PVID demande au porteur de présenter son visage à la caméra et de respecter les instructions qui lui sont données dynamiquement ; ○ le porteur suit les consignes successives données par le PVID ; ○ le PVID s'assure que le visage du porteur correspond à la photographie présente sur le document d'identité ; ○ le PVID renvoie le résultat de la vérification d'identité à l'AE. Le verdict final du PVID est envoyé de manière asynchrone, après la vérification des éléments par un opérateur humain.

	2. Cas de la validation d'une identité à l'aide d'un moyen d'identification électronique La validation initiale de l'identité du porteur est réalisée sur le site ou l'application mobile du fournisseur de moyen d'identification électronique.. Le processus de vérification à distance comprend les étapes suivantes : ● le porteur doit disposer au préalable d'un moyen d'identification électronique supporté par l'AE et actif ; ● le porteur se connecte sur le site de l'AE via un lien unique qu'il a reçu sur son adresse email ; ● l'AE affiche au porteur les informations d'identité utilisées pour sa demande de certificat : ○ nom et prénom ; ○ adresse de messagerie électronique ; ● le porteur confirme avoir pris connaissance des conditions générales d'utilisation en vigueur et accepte de les signer sans réserve ; ● le porteur confirme l'exactitude des informations présentées et consent à signer le formulaire de demande de certificat établi sur cette base ; ● le porteur est redirigé vers une page web ou une application appartenant au fournisseur du moyen d'identification électronique ; ● le porteur doit s'authentifier auprès du fournisseur du moyen d'identification électronique ; ● le fournisseur du moyen d'identification électronique renvoie le résultat de la vérification d'identité à l'AE. L'AE archive alors le formulaire de demande de certificat signé, les CGU signées ainsi que les preuves de vérification d'identité du porteur. Suite à cette vérification initiale d'identité, le porteur peut enregistrer un moyen d'authentification qui lui permettra d'obtenir de nouveaux certificats qualifiés de signature qualifiée par la suite sans refaire la vérification initiale d'identité. En son absence, le signataire devra réaliser une

	nouvelle vérification initiale d'identité lors de sa prochaine signature électronique qualifiée. Les informations d'identité portées dans le certificat éphémère généré à chaque signature sont celles qui ont été validées par le face à face à distance. Ces informations restent valables pour une durée de 3 ans au maximum avant que le porteur ne soit obligé de refaire valider les informations d'identité, cette durée devant être réduite en concordance avec la date d'expiration du titre d'identité ou du moyen d'identification électronique présenté à la délivrance du moyen d'authentification. Il est de la responsabilité du porteur de demander une mise à jour des informations d'identité si ces dernières n'étaient plus à jour avant la durée des 3 ans. Le porteur doit effectuer une demande de révocation de son moyen d'authentification dans les cas suivants : ● sa clé privée est suspectée de compromission, est compromise ou, est perdue (éventuellement les données d'activation associées) ; ● son moyen d'authentification pour autoriser une transaction de signature a été compromis ou suspecté de compromission. Une demande de révocation garantit au porteur qu'aucune nouvelle signature ne sera permise avec son moyen d'authentification actuel.
Limites d'utilisation	Les certificats délivrés ne sont utilisables que pour les transactions de signature assurées par l'infrastructure Youtrust. Les certificats des porteurs ont une durée de validité de 120 minutes. Les clés privées correspondantes ont une durée de vie équivalente à la durée du processus de signature. Youtrust conserve pendant 10 ans les dossiers d'enregistrement des porteurs (20 ans pour les certificats délivrés dans le cadre d'un processus de signature électronique initié par un client de Youtrust établi en Italie). Youtrust conserve pendant 17 ans les journaux et les traces concernant la délivrance et l'utilisation des clés privées des porteurs.
Obligations des porteurs	Le porteur prend en compte les exigences suivantes : ● s'obliger à fournir des éléments d'identité à jour et valides lors du processus d'enregistrement ; ● respecter les obligations relatives au service de vérification d'identité à distance, imposées par le prestataire de vérification d'identité à distance ; ● accepter tacitement le certificat émis par l'AC en validant la création de la signature, après validation du formulaire de demande et acceptation des CGU ;

	• accepter la conservation par l'AC des informations du dossier d'enregistrement et de gestion de ses clés de signature ;
	• s'obliger à utiliser le moyen d'authentification forte enrôlé initialement par l'AE ;
	• mettre en œuvre le certificat de signature en respectant les limites d'utilisation prévues ;
	• pour garantir le contrôle exclusif de sa clé privée de signature et en cas d'enregistrement d'un moyen d'authentification, le porteur doit :
	  ○ configurer une authentification robuste sur son téléphone (code PIN ou mot de passe, avec limite du nombre de tentatives de déverrouillage) ;
	  ○ ne jamais prêter son téléphone, y compris à une personne de confiance ;
	  ○ en cas de perte ou de vol, appliquer les mesures préconisées par le fournisseur du téléphone (effacement à distance par exemple) et révoquer l'identité en contactant Youtrust ;
	  ○ en cas de transmission définitive du téléphone à un tiers (vente, cession, etc.), appliquer les mesures préconisées par le fournisseur du téléphone pour le réinitialiser et contacter Youtrust pour la révocation de l'identité ;
	  ○ maintenir à jour son téléphone, en installant les évolutions logicielles proposées par son fabricant et par l'éditeur du système d'exploitation ;
	  ○ n'installer sur le téléphone que des applications publiées sur les magasins officiels du système d'exploitation, éviter les applications potentiellement dangereuses (dont les outils de jailbreak), et maintenir à jour les applications installées ;
	  ○ conserver sa clé privée d'authentification et toute autre information relative à son identité sur son téléphone de manière confidentielle ;
	  ○ ne pas partager sa clé privée d'authentification ou toute autre information relative à son identité sur un autre téléphone ou appareil, quand bien même cet autre téléphone ou appareil appartiendrait au porteur ou à une autre personne en ce compris une personne de confiance.
	
	Toute signature réalisée après authentification sur le téléphone est présumée être faite par le porteur qui a enregistré ce téléphone, le principe de non-répudiation ne permet pas au porteur de nier avoir signé.

	• s'obliger à prévenir l'AC lorsqu'une des causes de révocation suivante est établie :
	  ○ les informations figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
	  ○ une erreur (intentionnelle ou non) a été détectée dans son dossier d'enregistrement ;
	  ○ sa clé privée du porteur est suspectée de compromission, est compromise ou, est perdue (éventuellement les données d'activation associées) ;
	  ○ son moyen d'authentification pour autoriser une transaction de signature a été compromis ou suspecté de compromission ;
	• s'obliger à vérifier le statut du certificat de signature délivré à travers les LCR publiées par l'AC et le service OCSP mis en œuvre ;
	• utiliser le certificat de signature dans les conditions d'usage prévues par la PC et reprises dans les présentes CGU.

Obligations de l'AC	Youtrust est responsable : • de la validation et de la publication de la PC, de la DPC et des CGU de l'AC ; • de la conformité des certificats émis vis-à-vis de la PC ; • du respect de tous les principes de sécurité par les différentes composantes, et des contrôles afférents ; • en cas d'incident majeur (perte, suspicion de compromission, compromission ou vol de clé privée de gestion des certificats par exemple) de signaler l'incident à l'ANSSI (supervision-eIDAS@ssi.gouv.fr). Youtrust est responsable de toute conséquence dommageable résultant du non-respect du présent document par elle-même. Sauf à démontrer que Youtrust n'a commis aucune faute intentionnelle ou de négligence, Youtrust est responsable de tout préjudice causé à toute personne physique ou morale qui se fie raisonnablement aux certificats délivrés dans chacun des cas suivants : • les informations contenues dans le certificat ne correspondent pas aux informations fournies lors de l'enregistrement ; • la délivrance du certificat n'a pas donné lieu à la vérification de la possession de la clé privée correspondante par le porteur ; • l'AC n'a pas fait procéder à l'enregistrement de la révocation d'un certificat, et publié cette information conformément à ses engagements.

	Youtrust n'est pas responsable du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation. En cas d'arrêt d'activité de l'AC, les certificats émis et encore dans leur période de validité seront révoqués. Enfin, Youtrust engage sa responsabilité en cas de faute ou de négligence dans les précautions à prendre en termes de confidentialité des données personnelles qui lui sont confiées par les porteurs.
Vérification du statut des certificats	L'utilisateur d'un certificat est tenu de vérifier l'état des certificats y compris ceux de la chaîne de confiance correspondante. L'AC met à disposition des utilisateurs une LCR à jour, publiée sur Internet sur le site : • http://crl.yousign.fr/crl/yousignsasqualifsignca.crl • http://crl2.yousign.fr/crl/yousignsasqualifsignca.crl • http://crl3.yousign.fr/crl/yousignsasqualifsignca.crl Youtrust met également en œuvre un service OCSP accessible à l'adresse suivante : http://ocsp.yousign.fr. Ces informations sont disponibles sept jours sur sept, vingt-quatre heures sur vingt-quatre, avec une disponibilité de 99.7% sur un mois. La LCR contient l'extension « ExpiredCertsOnCRL » et conserve les numéros de série de tous les certificats révoqués, même ceux qui ont expiré. Le service OCSP met en œuvre l'extension « archive cutoff », comme prévu par la RFC 6960, avec une date identique à la date de début de validité du certificat de l'AC et maintien disponible le statut de révocation du certificat après son expiration. Si la requête OCSP contient une demande pour un numéro de série non émis par l'AC, alors le serveur OCSP mettra dans la réponse correspondante le statut « unknown ». Si la requête OCSP contient une demande pour un numéro de série émis par l'AC, la réponse OCSP sera conforme avec les standards IETF RFC 6960. Les certificats émis par l'AC sont des certificats qualifiés au titre du règlement eIDAS. Il convient de le vérifier sur la base

	de la liste de confiance (Trusted List) émise par l'ANSSI sous https://www.ssi.gouv.fr/eidas/TL-FR.xml. Cette liste doit en particulier intégrer le certificat de l'AC et son statut de qualification. En cas de révocation de l'AC, par exemple suite à une compromission de sa clé privée, l'information de révocation est publiée dans une LAR accessible sur : ● http://crl.yousign.fr/crl/yousignsasroot2ca.crl ● http://crl2.yousign.fr/crl/yousignsasroot2ca.crl ● http://crl3.yousign.fr/crl/yousignsasroot2ca.crl Dans le cas d'une fin de vie de l'AC, Youtrust génèrera : ● une dernière LCR dont la date d'expiration sera positionnée à la valeur 99991231235959Z ; ● une dernière réponse OCSP sera pré-générée pour chaque certificat émis et contenant une date de fin de validité positionnée à la valeur 99991231235959Z. Si Youtrust arrête l'activité de l'AC, il s'engage à maintenir disponible les LCR et les réponses OCSP pré-générées.
Limite de responsabilité	Youtrust 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. Youtrust 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. En tout état de cause, et dans la stricte mesure permise par la loi applicable, Youtrust ne saurait être redevable du paiement de dommages et intérêts, de quelque nature qu'ils soient, directs, matériels, commerciaux, financiers ou moraux, en raison de l'exécution des présentes.
Accords applicables et pratiques de certification	Les politiques de certification décrivant les exigences qu'entend respecter l'AC sont publiées à l'adresse https://yousign.fr/fr/public/document, La politique de service et les conditions d'utilisation du service de vérification d'identité à distance du partenaire de Youtrust sont applicables.
Confidentialité	Les informations considérées comme confidentielles sont au moins les suivantes : ● les procédures internes de l'AC ;

	• les clés privées de l'AC, des composantes et des porteurs de certificats ; • les données d'activation associées aux clés privées d'AC et des porteurs ; • tous les secrets de l'IGC ; • les journaux d'évènements des composantes de l'IGC ; • les dossiers d'enregistrement des porteurs ; • les causes de révocations, sauf accord explicite du porteur. Youtrust applique des procédures de sécurité pour garantir la confidentialité de ces informations. Youtrust s'engage à respecter la législation et la réglementation en vigueur.
Politique d'assurance	Youtrust certifie qu'elle est titulaire d'une police d'assurance garantissant sa responsabilité civile professionnelle. Elle s'engage à maintenir en vigueur cette police d'assurance pendant toute la durée de son activité professionnelle.
Langue	Les présentes CGU ont été rédigées en plusieurs langues, dont le français. La langue d'interprétation sera la langue française en cas de contradiction ou de contestation sur la signification d'un terme ou d'une disposition.
Loi applicable et résolution des conflits	Les présentes CGU sont régies et interprétées selon le droit français. 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 aux tribunaux de Paris.
Gestion des données à caractère personnel	Youtrust s'engage à respecter la législation et la réglementation en vigueur concernant la gestion des données à caractère personnel, en particulier le règlement européen n°2016/679 du 27 avril 2016 dit « Règlement Général sur la Protection des Données » (RGPD). Le porteur est informé que la délivrance de certificats électroniques et l'exécution du processus de signature électronique impliquent la mise en œuvre par Youtrust de traitements de données à caractère personnel. Le porteur est invité à consulter la Politique de Confidentialité pour plus d'information sur comment sont traitées ses données à caractère personnel et sur comment exercer ses droits.
Audit et certification	Le module cryptographique utilisé par Youtrust pour l'AC et la signature électronique avancée est qualifié par l'ANSSI.

	Le dispositif de création de signature électronique qualifiée est un dispositif qualifié de création de signature à distance (“Remote QSCD”), qualifié au titre du règlement eIDAS. Le service de vérification d’identité à distance est certifié par l’ANSSI au niveau de garantie substantiel ou élevé.Les certificats sont conformes à la norme ETSI 319 411-2 et sont qualifiés, au sens du règlement eIDAS, par l'ANSSI. Les certificats sont de niveau QCP-n-qscd. Les certificats contiennent les champs qualifié s suivants : ● esi4-qcStatement-4 = id-etsi-qcs-QcSSCD ● esi4-qcStatement-1 = id-etsi-qcs-QcCompliance ● esi4-qcStatement-6 = id-etsi-qct-esign