Autorité de certification et d'horodatage

Conditions générales d'utilisation de l'AC YOUSIGN SAS - QUALIFIED SIGNATURE CA

Exporté le 05/01/2021

Créateur : Florent Eudeline - 11/05/2020

Dernier changement : Kevin Dubourg - 22/09/2020

Diffusion : C1 - Public

Sommaire:

1 - Historique

Version	Objet de la révision	Date	Auteur
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
1.0.3	Mise à jour de Vérification du statut des certificats. Précision sur la réponse OCSP.	22 sept. 2020	Kevin Dubourg
1.0.2	Modification mise en page	18 août 2020	Florent Eudeline
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

2 - Introduction

2.1 - Présentation générale

La société Yousign est un Prestataire de Service de Certification Electronique (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 certifiats délivrés par l'Autorité de Certification « YOUSIGN SAS - QUALIFIED SIGNATURE CA ». Ce document synthétise l'ensemble des engagements et des pratiques de Yousign dans le cadre du déploiement et de l'exploitation de l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA », tant sur les plans techniques qu'organisationnels.

2.2 - Identification du document

Les présentes « Conditions Générales d'Utilisation » se rapportent à l'AC « YOUSIGN SAS - QUALIFIED SIGNATURE CA » dont la Politique de Certification applicable est identifiée par l'OID : 1.2.250.1.302.1.11.1.0
D'autres éléments, plus explicites, (nom, numéro de version, date de mise à jour) permettent également de l'identifier.

2.3 - Acronymes

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
DPC	Déclaration des Pratiques de Certification
DPO	Data Protection Officer (Délégué à la Protection des Données)
eIDAS	electronic IDentification, Authentication and trust Services
IGC	Infrastructure à Gestion de Clés
LCR	Liste des Certificats Révoqués
OCSP	Online Certificate Status Protocol
OID	Object Identifier

PC	Politique de Certification
QCP-n	Policy for EU qualified certificate issued to a legal person (politique pour les certificats qualifiés délivrés à une personne physique)

3 - Conditions générales d'utilisation

Les présentes CGU sont basées sur le modèle prévu par l'annexe A de la norme EN 319411-1 (version 1.1.1).

Point de contact	Gestion de l'AC Yousign Yousign SAS 8 allée Henri Pigis 14000 CAEN 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 »

Les certificats émis sont des certificats éphémères qualifiés de signature qui peuvent être utilisés 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. Le porteur peut être une personne ou une personne agissant pour le compte d'une personne morale.

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	organization : Nom de l'entité avec laquelle le porteur est en lien	
C	countryName : Pays de l'autorité d'enregistrement de Yousign, toujours égal à FR (France)	Oui
SerialNumber	serialNumber : Date et heure de la génération du certificat.	Oui

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.

Le certificat généré est utilisable exclusivement dans le cadre du service de signature proposé par Yousign.

La mise en œuvre d'un certificat qualifié nécessite un processus de vérification de l'identité du porteur. Ce processus se réalise lors d'un face à face avec un opérateur d'AE Yousign.

Le porteur doit formuler une demande qui contient les éléments suivants :

- Le formulaire de demande de certificat, signé par le porteur et daté de moins de 3 mois ;
- Les conditions générales d'utilisation en vigueur signées par le porteur ;
- Un justificatif d'identité du porteur en cours de validité parmi les justificatifs suivants :
    - la carte d'identité,
    - le passeport,
    - la carte de séjour ;
- Uniquement pour une demande en lien avec une personne morale :
    - pour une entreprise, toute pièce, valide lors de la demande de certificat, attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;
    - pour une entreprise, tout document signé par le responsable légal et attestant de la qualité du signataire à faire une demande de certificat pour le compte de son entreprise ;
    - pour une administration, une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative ;
    - pour une entreprise ou une administration, le formulaire de demande de certificat doit être signé par un représentant légal de la personne morale en plus de la signature du porteur.

Le formulaire de demande comporte :

- Le type de certificat demandé ;
- Les nom et prénom du porteur, tels qu'ils apparaissent sur la pièce d'identité présentée avec le dossier ;
- Des informations issues de la pièce d'identité présentée : type, numéro, date de validité, autorité émettrice ;
- L'adresse de messagerie électronique du porteur ;
- Un numéro de téléphone pour joindre le porteur ;
- L'acceptation explicite par le porteur de ses obligations ;
- L'engagement d'exactitude des informations du formulaire, et en particulier celles qui seront reprises dans le certificat ;
- Le consentement du porteur à la conservation par l'AC des informations du dossier d'enregistrement et de gestion de ses clés de signature ;

L'AE effectue les opérations suivantes lors du face à face :

- Vérification de la complétude et de la signature par le futur porteur du formulaire de demande ;
- Vérification de la signature par le futur porteur des conditions générales d'utilisation du service de signature ;
- Validation de l'identité du futur porteur par contrôle de l'original de la pièce d'identité ;
- Vérification de la cohérence des informations portées dans le formulaire de demande avec la pièce d'identité ;

	• Pour le cas demande en lien avec une personne morale :
	  • Vérification de la validité des pièces justificatives supplémentaires ;
	  • Vérification de la signature par la personne morale de la demande.
	La vérification de l'adresse de messagerie du porteur est effectuée durant le processus de création de compte du porteur sur le service Yousign.
	Lors de ce processus initial, l'opérateur soumet un document à faire signer électroniquement par le porteur. Cela lui permet de s'assurer directement que les informations d'identité qui sont portées dans son certificat sont bien à jour.
	
	Une fois la validation d'identité obtenue, le porteur met en œuvre un moyen d'authentification forte. Ce moyen est enrôlé par Yousign pour permettre au porteur de s'authentifier fortement pour exprimer son consentement lors du processus de signature.
	Les informations d'identité portées dans le certificat éphémère sont celles qui ont été validées initialement par l'opérateur d'AE. Ces informations restent valables pour une durée de 3 ans avant que le client ou le porteur ne soit obligé de refaire valider les informations d'identité.
	Il est de la responsabilité du client ou 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 ne peut pas renouveler son certificat, chaque transaction de signature génère un nouveau certificat qualifié éphémère. Le porteur peut révoquer par téléphone ou courriel son certificat durant sa période de validité en utilisant un des moyens suivants :
	
	• Révocation via téléphone : le demandeur contacte Yousign par téléphone et demande la révocation d'un certificat. Afin de s'assurer de l'identité du demandeur, une série de deux questions lui est posée. Ces questions sont fondées sur les informations en possession de Yousign. La validation de la demande est effective après la réception d'une confirmation obtenue via un courrier électronique.
	• Révocation par courriel : le demandeur contacte Yousign par message électronique et demande la révocation d'un certificat. Afin de s'assurer de l'identité du demandeur, Yousign prend contact avec le demandeur par téléphone et pose une série de 2 questions aléatoires concernant son identité. Ces questions sont fondées sur les informations en possession de Yousign. La validation de la demande est effective après cette confirmation par téléphone.

Limites d'utilisation	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 17 ans les journaux et les traces concernant la délivrance et l'utilisation des clés privées des porteurs.

Obligations de l'abonné	L'abonné prend en compte les exigences suivantes :
	• S'obliger à fournir des éléments d'identité à jour et valides lors du processus d'enregistrement ;
	• 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 ;
	• 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	Yousign 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). Yousign fait son affaire de toute conséquence dommageable résultant du non-respect du présent document par elle-même. Sauf à démontrer que Yousign n'a commis aucune faute intentionnelle ou de négligence, Yousign 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. Yousign 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, Yousign 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/yousignsasqualifsign2ca.crl • http://crl2.yousign.fr/crl/yousignsasqualifsign2ca.crl • http://crl3.yousign.fr/crl/yousignsasqualifsign2ca.crl Yousign 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 expirés. 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. Dans le cas d'une fin de vie de l'AC, Yousign 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 Yousign arrête l'activité de l'AC, il s'engage à maintenir disponible les LCR et les réponses OCSP pré-générées.
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. En tout état de cause, Yousign 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	La politique de certification décrivant les exigences qu'entend respecter l'AC est publiée à l'adresse suivante : https://yousign.fr/fr/public/document sous l'OID 1.2.250.1.302.1.11.1.0

Politique de 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. Yousign applique des procédures de sécurité pour garantir la confidentialité de ces informations. Yousign s'engage à respecter la législation et la réglementation en vigueur sur le territoire français.
Politique d'assurance	Yousign 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 Caen.
Gestion des données à caractère personnel	Yousign 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 suppose la mise en œuvre par Yousign de traitements de données à caractère personnel auquel le porteur consent, conformément à la politique de confidentialité de Yousign disponible à l'adresse https://yousign.com/fr-fr/confidentialite. 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 DPO de Yousign, à l'adresse dpo@yousign.com.
Audit et certification	Le module cryptographique utilisé par Yousign est qualifié par l'ANSSI. Les certificats sont conformes à la norme ETSI 319 411-2 au niveau QCP-n et sont qualifiés, au sens du règlement eIDAS, par l'ANSSI. Les certificats émis contiennent les champs qualifiés suivants : • esi4- qcStatement-1 = id-etsi-qcsQcCompliance • esi4- qcStatement-6 = id-etsi-qct-esign