Autorité de certification et d'horodatage

Conditions Générales d'Utilisation de l'AC _ YOUSIGN SAS - QUALIFIED SEAL2 CA

Exporté le 11/05/2020

Créateur : Florent Eudeline - 11/05/2020

Dernier changement : Florent Eudeline - 11/05/2020

Diffusion : C1 - Public

Sommaire:

1 - Historique 3
2 - Introduction 3
2.1 - Présentation générale 3
2.2 - Identification du document 3
2.3 - Acronymes 3
3 - Conditions Générales d'Utilisation 4

1 - Historique

Version	Date	Rédigé par	Mise à jour
1.0.0	17/10/2018	Antoine Louiset	Création du document
1.0.1	03/01/2019	Antoine Louiset	Prise en compte des remarques de l'auditeur

Etat du document – Classification	Référence
Validé – C1 (document public)	OID de la PC : 1.2.250.1.302.1.13.1.0

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 certificats délivrés par l'Autorité de Certification « YOUSIGN SAS - QUALIFIED SEAL2 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 SEAL2 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 SEAL2 CA » dont la Politique de Certification applicable est identifiée par l'OID : 1.2.250.1.302.1.13.1.0
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
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
LCR	Liste des Certificats Révoqués
OID	Object Identifier
PC	Politique de Certification
RCC	Responsable de Certificats Cachets

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 Adresse de messagerie : contact@yousign.fr	
Types de certificats, procédures de validation et restrictions d'usage	Les certificats couverts par es présentes CGU sont émis par la chaîne d'Autorité de Certification suivante : • AC Racine : « YOUSIGN SAS - ROOT2 CA » • AC Émettrice : « YOUSIGN SAS - QUALIFIED SEAL2 CA » Il s'agit de certificats cachets qualifiés permettant de réaliser des opérations de scellement en utilisant des sceaux électroniques. Ces certificats sont délivrés à un Responsable de Certificats Cachets qui est un représentant formel de l'Abonné au service Yousign et qui en charge la gestion et la mise en œuvre de ces certificats. Les DN sont construits de la façon suivante :	
Attribut	**Description**	**Présence**

CN	*commonName* : Nom libre désignant le service applicatif porteur du certificat. Le nom doit contenir le nom officiel de l'entité	Oui
OI	*organizationIdentifier* : Identifiant de l'entité du RCC structurée sous la forme : NTRFR-*<numéro de SIREN>*	Oui
OU	*organizationUnit : Identifiant de l'entité avec laquelle le porteur est en lien, selon la syntaxe RGS :* *0002 <numéro de SIREN>*	Oui
O	*organization :* Nom de l'entité.	Oui
C	*countryName* : Pays de l'autorité d'enregistrement de Yousign., toujours égal à FR (France)	Oui

Les certificats de test émis par l'AC «YOUSIGN SAS - QUALIFIED SEAL2 CA » sont identifiables immédiatement par l'ajout du préfixe « TEST – » dans la valeur de l'attribut CN, par exemple :
CN = TEST – Service de cachet ENTITE,…
En dehors de cette spécificité, les certificats de tests émis par l'AC «YOUSIGN SAS - QUALIFIED SEAL2 CA » suivent les mêmes processus que les certificats de production nominale.
Le RCC est en charge de paramétrer ou de faire faire le paramétrage permettant d'accéder à l'infrastructure mise à disposition par Yousign. Chaque accès au certificat cachet est authentifié.
Le RCC doit faire une demande formelle auprès de l'AE Yousign pour obtenir son certificat. Cela se fait lors d'un face à face et la demande de certificat contient :

- Le formulaire de demande de certificat, daté de moins de 3 mois, signé par un représentant autorisé de l'entité ;
- un mandat, daté de moins de 3 mois, désignant le futur RCC comme étant habilité à être RCC pour le service de création de cachet pour lequel le certificat de cachet doit être délivré. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCC ;
- pour une entreprise, toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers, ...), 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 attestant de la qualité du signataire de la demande de certificat,
- pour une administration, une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,
- un justificatif d'identité du futur RCC en cours de validité parmi les justificatifs suivants :
    - la carte d'identité,
    - le passeport,
    - la carte de séjour ;
- les conditions générales d'utilisation en vigueur signées par le futur RCC.

Le formulaire de demande comporte :

- Le nom du service de création de cachet concerné par cette demande ;
- Le nom, le numéro SIREN et l'adresse postale de l'entité du futur RCC ;
- Les nom et prénom du futur RCC, 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 futur RCC ;
- Un numéro de téléphone pour joindre le RCC ;
- L'acceptation explicite par le futur RCC de ses obligations ;
- L'engagement d'exactitude des informations du formulaire, et en particulier celles qui seront reprises dans le certificat ;
- Le consentement du futur RCC à la conservation par l'AC des informations du dossier d'enregistrement et de gestion des clés de cachet ;

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

- Vérification de la complétude et de la signature du formulaire de demande par un représentant autorisé de l'entité ;
- Vérification de la validité du mandat et de sa signature par un représentant autorisé de l'entité et par le futur RCC ;
- Vérification des pièces justificatives produites par l'entreprise ou l'administration à laquelle est rattachée le futur RCC ;
- Vérification de la signature par le futur RCC des conditions générales d'utilisation du service de signature ;
- Validation de l'identité du futur RCC par contrôle de l'original de la pièce d'identité ;
- Vérification de la cohérence des informations portées dans le formulaire de demande avec les pièces justificatives.

Une fois ces contrôles effectués avec succès, l'AE date et signe le formulaire puis enregistre la demande dans l'IGC.
L'AE archive le formulaire de demande, les CGU ainsi que les pièces justificatives. Le RCC obtient une copie du formulaire et des conditions générales d'utilisation.
Le RCC délègue à l'AC la gestion de la clé privée du certificat qu'il demande. L'AC génère la clé privée après validation de la demande du RCC et la protège afin de garantir sa confidentialité et sa disponibilité. Le clé privée n'est activée que sur réception d'une requête authentifiée du RCC. L'AC détruit la clé privée en fin de vie du certificat ou en cas de révocation du certificat.
L'AC ne propose pas de services de renouvellement autre que la fourniture par le RCC d'une nouvelle demande. Le processus est identique à celui de la délivrance initiale.
La demande de révocation d'un certificat doit être réalisée par le RCC ou à défaut par un représentant légal de l'entité de rattachement du certificat de cachet.
L'identité du demandeur est vérifiée par l'AE:

- Lorsque la demande est faite par le RCC, Yousign soumet une série de deux questions aléatoires concernant son identité ;
- Lorsque la demande est faite par le représentant légal, celui-ci doit soumettre un dossier papier contenant la demande de révocation signée, le KBis de la société, une copie de la pièce d'identité du demandeur et un pouvoir s'il ne s'agit pas d'un responsable légal de l'entité.

Dans les deux cas, un opérateur de révocation Yousign prend contact directement avec le demandeur pour s'assurer de sa volonté de révoquer.
Le RCC est informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat dans les CGU de celui-ci.
L'initiation de la demande de révocation d'un certificat pourra se faire par téléphone ou par courriel au service de support. L'opérateur de révocation Yousign ouvre un ticket de support et fournit au demandeur le formulaire de demande de révocation de certificat de cachet. Le demandeur doit remplir ce formulaire, le signer puis en renvoyer une copie numérisée au support, l'original devant être envoyé par courrier postal à Yousign.
Lorsque la demande est réalisée par le RCC et que l'opérateur de révocation Yousign est en possession de cette demande signée, il rappelle le RCC en utilisant les coordonnées communiquées à la demande du certificat (ou au changement de RCC). L'opérateur Yousign vérifie l'identité du demandeur en lui posant

deux questions aléatoires basées sur les informations confidentielles en possession de Yousign. La demande de révocation est validée une fois ces vérifications réalisées avec succès.
Lorsque la demande est réalisée par un représentant légal, celui-ci doit envoyer par courrier postal un dossier comprenant la demande de certificat signée, un KBis de la société, la copie de la carte d'identité du demandeur et un pouvoir s'il n'est pas lui-même le responsable légal. L'opérateur Yousign vérifie les pièces de ce dossier et valide la demande une fois les contrôles réalisés.
Les informations suivantes doivent figurer dans la demande de révocation de certificat :

- le nom du demandeur de la révocation ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série, identifiant de l'entité, identité du RCC, dates de validité) ;
- la cause de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation sera diffusée au minimum via une LCR signée par une entité désignée par l'AC.
Le demandeur de la révocation sera informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le RCC du certificat n'est pas le demandeur, il sera également informé de la révocation effective de son certificat.
L'entité est informée de la révocation de tout certificat des RCC qui lui sont rattachés. L'opération est enregistrée dans les journaux d'évènements.

Limites d'utilisation	Les certificats délivrés ne peuvent être mis en œuvre que par un RCC formellement identifié. Les certificats cachets ont une durée de validité de 3 ans. Les clés privées correspondantes ont une durée de vie équivalente. Yousign conserve pendant 17 ans les journaux et les traces concernant la délivrance et l'utilisation des clés privées.
Obligations de l'abonné	L'abonné prend en compte les exigences suivantes :

- S'obliger à fournir des éléments d'identité à jour et valide lors du processus d'enregistrement
- Mettre en œuvre le certificat de signature en respectant les limites d'utilisation prévues et notamment à assurer la confidentialité des éléments d'authentification et d'activation permettant au serveur sous responsabilité du RCC d'accéder au service de cachet électronique
- S'obliger à prévenir l'AC lorsqu'une des causes de révocation suivante est établie :
    - les informations figurant dans le 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 le dossier d'enregistrement
    - la clé privée est suspectée de compromission, est compromise ou, est perdue (éventuellement les données d'activation associées)
    - Les éléments d'authentification et d'activation pour autoriser l'accès au certificat cachet ont été compromis ou suspectés de compromission
- S'obliger à vérifier le statut du certificat délivré à travers les LCR publiées par l'AC et le service OCSP mis en œuvre
- Utiliser le certificat 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

- De la protection des clés privées de cachet, depuis leur génération jusqu'à leur destruction, et de leur activation par le seul RCC autorisé
- 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 ;
- 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 seront alors 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/yousignsasqualifseal2ca.crl
- http://crl2.yousign.fr/crl/yousignsasqualifseal2ca.crl
- http://crl3.yousign.fr/crl/yousignsasqualifseal2ca.crl

Yousign met également en œuvre un service OCSP accessible à l'adresse suivante : http://ocsp.yousign.fr

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 l'AC est toujours valide, « good » si cette dernière est expirée.

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 garantie et 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.|

Accords applicables et pratiques de certification	La politique de certification décrivant les exigences qu'entend respecter l'AC est publiée sur le site suivant : http://yousign.fr/fr/public/document sous l'OID 1.2.250.1.302.1.13.1.0
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 RCC,
- les causes de révocations, sauf accord explicite du RCC.
  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	L'AC applique des niveaux de couverture d'assurance raisonnables et a souscrit à cet effet une assurance responsabilité civile au titre de la réalisation de son activité professionnelle.
Loi applicable et résolution des conflits	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.

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-l 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-eseal