Conditions Générales d'Utilisation des certificats de cachet serveur émis par l'AC YOUSIGN SAS – SIGN3 CA

v1.0.2 | Diffusion : C1 - Public

HISTORIQUE DES VERSIONS			
Version	**Objet de la modification**	**Date**	**Auteur**
1.0.2	Ajout des PKI Disclosure Statements (section présentation générale) Ajout de l'OID de cachet qualifié (section identification du document) Mise à jour de la définition de l'abonné (section définitions) Ajout d'un paragraphe sur les obligations de l'AC (section obligations de l'AC) Ajout des critères de sélection des modules cryptographiques pour l'OID de cachet qualifié (section audits et références applicables)	14 mai 2025	Tony BELOT Tony DUFOUR
1.0.1	Modifications des obligations de vérification des certificats par les utilisateurs (sections obligations de l'entité sujette et du représentant légal et obligations de l'abonné et du RCC)	28 juin 2024	Jean VERRONS
1.0.0	Ajout de la définition du terme « abonné » (section définitions) Introduction du terme « entité sujette » et de la possible différence entre cette entité et l'abonné (sections définitions, type de certificats émis, modalités d'obtention, limites d'utilisation, obligations de l'entité sujette et du représentant légal, obligations de l'abonné et du RCC et obligations de vérification des certificats par les utilisateurs) Remplacement de la notion de « porteur » par des termes plus précis désignant soit l'abonné ou son représentant légal, soit l'entité sujette ou le RCC (sections modalités d'obtention, obligations de l'entité sujette et du représentant légal et obligations de l'abonné et du RCC)	13 juil. 2023	Tony Belot

HISTORIQUE DES VERSIONS			
Version	**Objet de la modification**	**Date**	**Auteur**
	Clarification des responsabilités de l'abonné (et de son RCC) et de l'entité sujette (et de son représentant légal), ainsi que de leurs relations (sections présentation générale, obligations de l'entité sujette et du représentant légal, obligations de l'abonné et du RCC, limite de responsabilité, gestion des données à caractère personnel et convention sur la preuve) Mise à jour des liens vers la documentation publique (sections type de certificats émis et références documentaires) Alignement de l'objet des certificats entre les CGU et la PC (section objet des certificats) Déplacement des modalités de gestion, stockage, protection et preuve de possession de la clé privée dans la PC (section modalités d'obtention) Modification du terme « serveur » par « service applicatif » (section obligations de l'abonné et du RCC) Déplacement des URL vers les CRL et LAR dans la PC (sections obligations de vérification des certificats par les utilisateurs et vérification du statut des certificats) Corrections mineures syntaxiques et de mise en forme		
0.0.1	Création du document, généré à partir des Conditions Générales d'Utilisation de l'AC - YOUSIGN SAS - SIGN2 CA pour les certificats de cachet, version 1.0.1, avec les modifications suivantes : • Modification des références à l'AC Sign2 pour Sign3, mise à jour de l'OID et des adresses des CRL	23 juin 2023	Tony Belot

HISTORIQUE DES VERSIONS			
Version	**Objet de la modification**	**Date**	**Auteur**
	• Complétion des acronymes et ajout des traductions le cas échéant (section acronymes) • Ajout d'une section pour les définitions (section définitions) • Précision quant à l'identification du document (section identification du document) • Ajout de la norme ETSI et du niveau de certificat applicables (section identification du document) • Mise à jour de l'adresse de contact de l'AC (section conditions générales d'utilisation, rubrique contact de l'Autorité de Certification) • Suppression de l'exemple d'utilisation des certificats pour une signature électronique simple d'une personne physique (section conditions générales d'utilisation, rubrique objet des certificats) • Clarification et simplification des rôles de RCC et de responsable légal, déplacement du contenu du dossier d'enregistrement et des pièces justificatives acceptées dans la PC (section conditions générales d'utilisation, rubrique modalités d'obtention) • Ajout de la communication systématique du certificat au porteur suite à sa génération et suppression de la possibilité de demandes ultérieures (section conditions générales d'utilisation, rubrique modalités d'obtention) • Clarification des modalités de stockage, d'utilisation et de protection des clés privées (section conditions générales d'utilisation, rubrique modalités d'obtention) • Suppression des canaux de révocation par courrier et téléphone, déplacement du détail		

HISTORIQUE DES VERSIONS			
Version	**Objet de la modification**	**Date**	**Auteur**
	du processus de révocation dans la PC (section conditions générales d'utilisation, rubrique modalités de révocation) • Clarification du service autorisé à utiliser le certificat (section conditions générales d'utilisation, rubrique limites d'utilisation) • Renforcement des obligations du porteur et clarification du délai nécessaire aux opérations de renouvellement des certificats (section conditions générales d'utilisation, rubrique obligations des porteurs) • Précision quant à la limite de l'exonération de dommages et intérêts (section conditions générales d'utilisation, rubrique limite de responsabilité) • Suppression de la rubrique relative aux conditions d'indemnisation (section conditions générales d'utilisation) • Suppression de la mention à la DPC (section conditions générales d'utilisation, rubriques références documentaires et audits et références applicables) • Mise à jour du Tribunal compétent de Caen vers 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) • Suppression du contrôle de conformité et précision quant à l'audit réalisé régulièrement (section conditions générales d'utilisation,		

HISTORIQUE DES VERSIONS			
Version	**Objet de la modification**	**Date**	**Auteur**
	rubrique audits et références applicables) • Modifications diverses facilitant la lecture du document		

Table des matières

1. Introduction

1.1. Présentation générale

Ce document définit les CGU des certificats de cachet serveur délivrés par l'Autorité de Certification `YOUSIGN SAS - SIGN3 CA`.

Ces CGU sont acceptées par l'abonné et l'entité sujette durant le processus de demande. Ce document présente les modalités de gestion des certificats ainsi que les engagements et les obligations des différentes parties.

Ce document est conforme au modèle des PKI Disclosure Statements au sens de la norme EN 319 411-1.

1.2. Identification du document

Ce document est référencé par son titre et son numéro de version. Ce numéro est amené à évoluer de manière indépendante des évolutions de l'OID de la Politique de Certification.

Cette version des CGU s'applique aux OID suivants :

- `1.2.250.1.302.1.18.1.0` pour les certificats de niveau LCP de la norme ETSI 319 411-1, utilisés dans le cadre des certificats de cachet serveur émis pour une personne morale;
- `1.2.250.1.302.1.24.1.0` pour les certificats qualifiés de niveau QCP-l de la norme ETSI 319 411-2 utilisés dans le cadre des certificats de cachet serveur émis pour la personne morale Yousign SAS.

Les éléments spécifiques à une politique sont précédés de l'OID de cette politique entre crochets. Plusieurs OID peuvent être spécifiés, dans ce cas ils sont ajoutés les uns à la suite des autres. Dans le cas où un élément s'applique à tous les OID décrits dans ce document, soit le tag `[tous les OID]` est utilisé, soit aucun tag n'est précisé.

1.3. Acronymes

Acronyme	Signification	Traduction
AC	Autorité de Certification	-
AE	Autorité d'Enregistrement	-
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
IGC	Infrastructure à Gestion de Clés	-
LAR	Liste des certificats d'Autorités de Certification Révoqués	-
LCP	Lightweight Certificate Policy	Politique de certificat légère
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	-
RCC	Responsable du Certificat de Cachet	-
URL	Uniform Resource Locator	Localisateur uniforme de ressource

1.4. Définitions

Terme	Signification
Abonné	[1.2.250.1.302.1.18.1.0] L'abonné est une personne morale cliente de la société Yousign. Un lien contractuel existe entre l'abonné et la société Yousign.

Terme	Signification
	[1.2.250.1.302.1.24.1.0] L'abonné est la personne morale Yousign SAS.
Entité sujette	L'entité sujette est la personne morale pour laquelle le certificat a été émis. Cette personne morale est représentée par un représentant légal, enregistré par l'AE. Le DN du certificat permet d'identifier cette entité.
Responsable du Certificat de Cachet	Le RCC est la personne physique qui est responsable de la protection des données d'activation de la clé privée correspondant au certificat de l'entité sujette. Le RCC est par défaut un responsable légal de l'entité sujette. Il peut alternativement être une personne nommée par un représentant légal de l'entité sujette. Dans ce dernier cas, le RCC peut être hiérarchiquement rattaché à l'entité sujette, ou rattaché à une autre entité avec laquelle un lien contractuel ou réglementaire existe. Le RCC peut être amené à changer en cours de validité du certificat (départ du RCC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.) sans remettre en cause la validité du certificat.
Utilisateur	Un utilisateur est une personne physique ou morale ayant accès à un fichier signé, dont la signature a été générée par la clé privée d'un certificat émis par l'AC couverte par ces CGU. Il est à noter qu'aucun lien direct n'existe entre la société Yousign et un utilisateur.

2. Conditions Générales d'Utilisation

Contact de l'Autorité de Certification	Yousign SAS Gestion de l'AC Yousign 507, rue de Suède et de Norvège 14000 Caen authority@yousign.com
Type de certificats émis	Les CGU s'appliquent aux certificats spécifiés au paragraphe identification du document. Les certificats sont délivrés à un RCC qui est un représentant formel de l'Abonné au service Yousign et qui est chargé de la gestion et de la mise en œuvre de ces certificats.

	Les certificats émis par l'AC sont des certificats de cachet serveur, émis pour le compte d'une entité sujette identifiée dans le certificat. Les certificats sont émis à travers la chaîne de certification suivante : • AC Racine : `YOUSIGN SAS - ROOT2 CA` • AC Émettrice : `YOUSIGN SAS - SIGN3 CA` Les certificats de la chaîne de certification sont disponibles à l'adresse suivante https://yousign.com/fr-fr/documentation-technique-des-certifications.
Objet des certificats	Les certificats émis par l'AC sont des certificats de cachet serveur permettant de garantir l'authenticité et l'intégrité des données.
Modalités d'obtention	Le RCC doit faire une demande formelle envoyée auprès de l'AE. Le dossier d'enregistrement est décrit dans la PC. Le certificat produit est communiqué au RCC suite à sa génération et demeure ultérieurement accessible dans chaque document signé. La possession de la clé privée doit être prouvée conformément à la méthode décrite dans la PC.
Modalités de renouvellement	Le processus de renouvellement correspond à une nouvelle demande de certificat.
Modalités de révocation	La demande de révocation d'un certificat doit se faire par courriel, à l'adresse renseignée à la section « Contact de l'Autorité de Certification ». Un formulaire de demande de révocation doit être complété et signé par le demandeur. Le processus de traitement de la demande de révocation est documenté dans la PC.
Limites d'utilisation	L'utilisation d'une clé privée de serveur et du certificat associé est strictement réservée au service de création de cachet stipulé dans le dossier d'enregistrement. Les certificats ont une durée de validité de trois (3) ans. Les clés privées correspondantes sont détruites à l'issue de cette période sans possibilité de recouvrement. Yousign conserve pendant dix-sept (17) ans les journaux et les traces concernant la délivrance et l'utilisation des clés privées associées aux certificats.

Obligations de l'AC	`[tous les OID]`
	L'AC est responsable :
	● de la validation et de la publication de la PC, et des présentes CGU de l'AC ;
	● de la conformité vis-à-vis de la PC et des présentes CGU.
	
	`[1.2.250.1.302.1.24.1.0]`
	L'AC est responsable :
	● en cas d'incident majeur (perte, compromission ou vol de la clé privée des certificats par exemple) de signaler l'incident à l'ANSSI dans les 24 heures.

Obligations de l'entité sujette et du représentant légal	L'entité sujette, représentée par son représentant légal, prend en compte les exigences suivantes : ● disposer d'un lien contractuel, hiérarchique ou réglementaire avec l'abonné ; ● s'obliger à fournir les informations et justificatifs requis dans le dossier d'enregistrement, à jour et valides ; ● vérifier que le contenu du certificat remis est correct ; ● mettre uniquement en œuvre le certificat dans les conditions d'usage prévues par la PC et reprises dans les présentes CGU, en respectant les limites d'utilisation ; ● consentir à ce que toute authentification réussie auprès du service de cachet électronique soit présumée réalisée avec l'accord du RCC et de l'entité sujette ; ● s'obliger à notifier l'AC sans délai indu lorsqu'une des causes de révocation suivante est établie : ○ une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ou dans le certificat ; o 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 ; ○ la données d'activation sont suspectées de compromission, compromises, perdues, volées ou révoquées. ● s'interdire d'utiliser le certificat dès lors que les données d'activation, la clé privée ou l'AC sont suspectées de compromission, compromises, perdues, volées ou révoquées ; ● s'obliger à vérifier le statut du certificat délivré à travers les LCR publiées par l'AC ; ● consentir à la conservation par l'AE et l'AC des informations du dossier d'enregistrement et de gestion des clés et du certificat.

Obligations de l'abonné et du RCC	L'abonné, représenté par le RCC, prend en compte les exigences suivantes : ● disposer d'un lien contractuel, hiérarchique ou réglementaire avec l'entité sujette ; ● s'obliger à obtenir l'accord formel d'un représentant légal de l'entité sujette préalablement à toute demande de certificat ; ● s'obliger à fournir les informations et justificatifs requis dans le dossier d'enregistrement, à jour et valides ; ● vérifier que le contenu du certificat remis est correct ; ● accepter tacitement le certificat émis par l'AC dès sa remise par l'AE ; ● assurer la confidentialité des éléments d'activation permettant au service applicatif d'accéder au service de cachet électronique ; ● consentir à ce que toute authentification réussie auprès du service de cachet électronique soit présumée réalisée avec l'accord du RCC et de l'entité sujette ; ● n'utiliser le certificat qu'avec l'accord de l'entité sujette, dans le cadre convenu avec l'entité sujette et dans les limites d'utilisation prévues par les CGU ; ● s'obliger à notifier l'AC sans délai indu lorsqu'une des causes de révocation suivante est établie : ○ une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ou dans le certificat ; o 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 ; ○ la données d'activation sont suspectées de compromission, compromises, perdues, volées ou révoquées. ● s'interdire d'utiliser le certificat dès lors que les données d'activation, la clé privée ou l'AC sont suspectées de compromission, compromises, perdues, volées ou révoquées ; ● s'obliger à notifier l'AE préalablement à toute invalidation du rôle du RCC connu ; ● s'obliger à vérifier le statut du certificat délivré à travers les LCR publiées par l'AC ; ● demander le renouvellement du certificat au moins trois (3) mois avant son expiration ; ● consentir à la conservation par l'AE et l'AC des informations du dossier d'enregistrement et de gestion des clés et du certificat.

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 de l'entité sujette 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) ; • vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la PC. Les CRL sont publiées aux URL renseignées dans les certificats et rappelées dans la PC.
Vérification du statut des certificats	En cas de révocation de l'AC, par exemple suite à une compromission de sa clé privée, l'information de révocation est mise à disposition dans une LAR publiée aux URL renseignées dans les certificats et rappelées 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 l'abonné ou l'entité sujette. En tout état de cause, et dans la stricte mesure permise par la loi applicable, 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.
Références documentaires	La Politique de Certification de l'AC YOUSIGN SAS - SIGN3 CA pour les cachet serveur est accessible à l'adresse suivante : https://yousign.com/fr-fr/documentation-technique-des-certifications.
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	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). L'abonné et l'entité sujette sont informés que la délivrance de certificats électroniques implique la mise en œuvre par Yousign de traitements de données à caractère personnel. Ils sont invités 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.

Audits et références applicables	`[tous les OID]`
	Yousign met en œuvre un Comité de Direction Technique Yousign.
	
	Un audit de sécurité technique est 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 sécurité des systèmes d'information.
	
	`[1.2.250.1.302.1.24.1.0]`
	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.

Convention sur la preuve	Pour chaque cachet électronique réalisé, Yousign, l'abonné et l'entité sujette acceptent que les éléments contenus dans : ● le dossier d'enregistrement, tels que : ○ les éléments d'identification de l'abonné et de son RCC ; ○ les éléments d'identification de l'entité sujette et de son représentant légal ; ○ les pièces justificatives fournies ; ● le dossier de preuve, tels que :

	○ les procédés utilisés pour apposer le cachet électronique sur les documents (processus d'authentification par exemple) ; ○ le certificat électronique de cachet ; ○ les éléments d'horodatage ; ○ 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. Le dossier d'enregistrement et le dossier de preuve seront archivés et horodatés par Yousign.