Conditions Générales d'Utilisation de Certigna SSL PRIS v3.4

Objet

Les présentes conditions ont pour objet de préciser les modalités de demande et d'utilisation d'un certificat Certigna SSL PRIS, proposé à un FUTUR RCAS et/ou à un RCAS, ainsi que les engagements et obligations respectifs des parties liées aux présentes. Les conditions générales d'utilisation découlent de la Politique de Certification de Certigna SSL PRIS, disponible à l'adresse :
http://politique.certigna.fr/PCcertignasslpris.pdf.

Définitions

- CERTIFICAT : certificat Certigna SSL PRIS constitué d'un fichier de données électroniques signé numériquement, conforme à la norme X.509 v3, contenant des informations sur le site ou le SERVEUR, permettant à un UTILISATEUR tiers d'identifier ce site ou ce serveur et permettant que les échanges entre l'UTILISATEUR tiers et ce site ou ce serveur soient sécurisés ;
- AC : Autorité de Certification Certigna SSL PRIS de la société DHIMYOTIS, délivrant les CERTIFICATS ;
- AC RACINE : Autorité de plus haut niveau de l'IGC Certigna qui certifie les AUTORITES EMETTRICES ;
- AC EMETTRICE : Autorité dont le certificat a été signé par l'AUTORITE RACINE. L'AC est une autorité émettrice dans l'IGC Certigna ;
- AE : Autorité d'Enregistrement Certigna SSL PRIS de la société DHIMYOTIS, contrôlant les demandes de CERTIFICAT et les éventuelles demandes de REVOCATION de ces derniers ;
- AUTORITE D'ENREGISTREMENT DELEGUEE (AED) : entité tierce externe à l'IGC avec laquelle DHIMYOTIS a conclu un contrat de délégation par lequel il sous-traite une partie de l'activité de l'AE, à savoir, la collecte et le contrôle des dossiers d'enregistrement, l'identification des demandeurs de CERTIFICAT et la soumission des demandes de REVOCATION ;
- FUTUR RCAS : personne physique qui effectue la demande de CERTIFICAT.
- DEMANDE DE CERTIFICAT : ensemble constitué du formulaire de demande signé (acceptant les présentes conditions générales) accompagné des pièces justificatives et de la requête générée informatiquement ;
- RCAS : personne physique pour laquelle la demande de CERTIFICAT a été acceptée et traitée par l'AC, qui est responsable de ce CERTIFICAT et de la clé privée correspondante ;
- CONTRAT : relations entre l'AC et le RCAS;
- LCR : Liste des Certificats Révoqués ;
- OID : identifiant d'objet (Object IDentifier) ;
- REVOCATION : opération consistant à anticiper la fin de validité d'un CERTIFICAT initialement prévue et dont la date est inscrite dans le CERTIFICAT ;
- SERVEUR : serveur informatique hébergeant un service sécurisé par un CERTIFICAT, permettant l'authentification de ce service par des UTILISATEURS et la sécurisation des échanges avec ces derniers ;
- MANDATAIRE DE CERTIFICATION (MC) : personne désignée et placée sous la responsabilité de l'entité cliente. Elle est en relation directe avec l'AE et assure pour elle un certain nombre de vérifications concernant l'identité, éventuellement les attributs des porteurs de cette entité ;
- UTILISATEUR : utilisateur d'un CERTIFICAT. Il peut s'agir de :
    - Une personne physique (particulier, agent d'une administration ou employé d'une entreprise) accédant à un serveur informatique, qui utilise un certificat et un dispositif d'établissement de session afin d'*authentifier le serveur* auquel il accède, qui est identifié dans le certificat, et afin d'*établir une clé de session* partagée entre son poste et le serveur.

Qualification

L'AC Certigna SSL PRIS a été qualifiée, selon le schéma français, RGS (Référentiel Genéral de Sécurité) au niveau * par un cabinet d'audit accrédité par le COFRAC (Comité Français d'Accréditation).
Chaque année un audit de contrôle et de surveillance est mené par ce cabinet pour renouveler cette certification.
La qualification RGS est l'acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de service d'un prestataire de service de certification électronique aux exigences du RGS, pour un niveau de sécurité donné et correspondant au service visé par ce prestataire.

Durée

Le CONTRAT est conclu pour une durée choisie par le FUTUR RCAS (3 ans maximum) et démarre le jour de la délivrance du CERTIFICAT par l'AE.

Tarif

Sauf accord de l'AC, le prix de vente du CERTIFICAT est celui fixé dans la grille tarifaire disponible sur demande auprès du service commercial de DHIMYOTIS. Le prix du certificat est payable à la commande (envoi règlement avec le dossier de demande), sauf accord explicite.

Engagements du FUTUR RCAS

Lors de sa DEMANDE DE CERTIFICAT, le FUTUR RCAS doit être vigilant dans la fourniture des informations d'enregistrement, un CERTIFICAT n'étant pas modifiable. Il transmet à l'AE, le cas échéant à l'AED, ou à un MC de son entité, en main propre ou par voie postale, le formulaire d'inscription généré lors de la demande en ligne sur le site https://www.certigna.fr, le paiement, ainsi que les pièces justificatives. Pour la requête en ligne, le FUTUR RCAS suit toutes les étapes de la procédure figurant sur le site https://www.certigna.fr.
L'AE accuse par mail de la réception de la demande électronique. Il appartient au FUTUR RCAS de se rapprocher de l'AE en cas de non transmission par cette dernière de cet accusé de réception.

Engagements propres à l'AE et à l'AC

A réception complète de la DEMANDE DE CERTIFICAT (réception des documents papier et de la requête en ligne), l'AE vérifie la conformité de la demande : vérification des documents papier et de la requête en ligne. En cas de conformité de la demande, l'AE informe par mail le FUTUR RCAS que sa DEMANDE DE CERTIFICAT est validée. Puis, l'AC crée le CERTIFICAT dans un délai de cinq jours ouvrés, et le transmet par mail au FUTUR RCAS, qui prend le statut de RCAS. En cas de non conformité de la demande ou en cas de dossier incomplet, l'AE demandera par mail au FUTUR RCAS d'effectuer les modifications sous 7 jours calendaires, le cas échéant elle pourra rejeter la demande. Toute collecte et tout usage de données à caractère personnel par l'AC sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, notamment par rapport à la CNIL et à l'article 226-13 (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002) du Code Pénal. L'AC est tenue à une obligation de moyens pour toutes les obligations relatives à la gestion du cycle de vie du CERTIFICAT qu'elle émet. Elle fournit un service de maintenance technique par téléphone aux heures de bureau ; elle fournit également un service de consultation en ligne sur le site https://www.certigna.fr permettant à tout moment aux tiers de vérifier la validité des CERTIFICATS émis par elle (cf. chapitre *Moyens offerts pour la vérification des certificats*). L'adresse postale, l'adresse électronique de l'AC, ainsi que le numéro de téléphone sont précisés dans le chapitre *Coordonnées de la société Dhimyotis* et sont également disponibles sur le site https://www.certigna.fr.

Engagements du RCAS

Le RCAS accepte explicitement le CERTIFICAT lors de son installation. En cliquant sur le bouton d'acceptation à la fin de la phase d'installation effectuée en ligne, un accusé de réception (AR) et une acceptation sont générés, puis transmis à l'AE. En cas de réception d'une non-acceptation par le RCAS, le CERTIFICAT est automatiquement révoqué par l'AE. A défaut de réception de l'AR et de l'acceptation, le CERTIFICAT est réputé être accepté par le RCAS dans les 7 jours calendaires suivant son envoi par l'AE ou au moment de sa première utilisation, selon celle de ces deux dates qui sera la plus proche dans le temps. Le RCAS dispose de 30 jours pour récupérer son certificat après validation du dossier par l'AE. Le RCAS est responsable de la conservation du code de révocation qui lui a été remis avec son CERTIFICAT, et qui permettra de l'identifier lors d'une éventuelle demande de révocation en ligne. Il s'engage à ne pas le communiquer à un tiers et à le conserver de façon confidentielle. Le RCAS est le seul responsable de l'installation du CERTIFICAT. Il a l'obligation de prendre toutes les mesures propres à s'assurer la sécurité de ou des ordinateurs sur lesquels est installé le CERTIFICAT. Il s'engage à sauvegarder sa clé privée associée. Si elle est stockée sur disque dur, il doit créer, pour sa protection, un mot de passe complexe (c'est-à-dire constitué d'une combinaison de 8 caractères parmi chiffres, lettres minuscules et majuscules, et caractères spéciaux). En cas de changement de RCAS pendant la validité du CERTIFICAT, le nouveau RCAS doit être obligatoirement enregistré auprès de l'AE. Le CERTIFICAT doit être utilisé uniquement pour les usages décrits dans la Politique de Certification correspondante et repris également dans le chapitre *Conditions d'usage des certificats et des clés privées associées*.

Révocation

Les principales causes de révocation possibles sont les suivantes :
- Compromission ou suspicion de compromission de la clé privée associée au CERTIFICAT ;
- Non conformité avec l'identité du serveur des informations contenues dans le CERTIFICAT ;
- Non respect des engagements du RCAS (notamment sur les conditions d'usage du CERTIFICAT), ou le cas échéant du MC, engagements découlant de la PC de l'AC ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- Pour des raisons techniques (échec de l'envoi du certificat,...) ;
- Destruction ou altération du support (disque dur) ;
- L'arrêt définitif du serveur ou la cessation d'activité de l'entité du RCAS de rattachement du serveur ;

En cas de connaissance d'une des précédentes conditions, le RCAS s'engage à demander immédiatement la révocation du CERTIFICAT auprès de l'AE. En conséquence, l'AE révoquera de fait le CERTIFICAT.
La demande de révocation peut être effectuée par :
- Le RCAS ;
- Un représentant légal de l'entité cliente, ou le cas échéant un MC de cette entité ;
- L'AC ou l'AE.

La demande de révocation peut être effectuée :
- Par courrier signé ;
- En ligne, sur https://www.certigna.fr (uniquement pour le RCAS ou le cas échéant le MC).

Afin que la demande de révocation soit traitée, son demandeur doit être authentifié et son habilitation vérifiée. Ce dernier doit fournir des données personnelles renseignées dans la demande initiale de certificat. Pour les demandes par courrier, la signature est vérifiée par rapport au dossier d'enregistrement (dossier d'enregistrement du RCAS, le cas échéant dossier d'enregistrement du MC). Pour les demandes en ligne, le demandeur doit être authentifié sur son espace client.
L'AC révoque le CERTIFICAT dans le délai d'un jour ouvré à compter de la réception de toute demande dont le demandeur peut être authentifié et son habilitation vérifiée. En cas de REVOCATION, le prix versé par l'entité reste acquis à l'AC. Le RCAS s'engage à ne plus utiliser un CERTIFICAT suite à l'expiration ou à la révocation de ce dernier.

Conditions d'usage des certificats et des clés privées associées

La clé privée associée au CERTIFICAT est utilisée pour que le SERVEUR puisse s'authentifier dans le cadre d'établissement de sessions sécurisées, de type SSL/TLS. Le CERTIFICAT est utilisé pour vérifier l'authentification du SERVEUR. L'utilisation de la clé privée du SERVEUR est strictement limitée à cet usage. En cas de non respect de l'usage de la clé privée, la responsabilité du propriétaire du SERVEUR pourrait être engagée.

Engagement des utilisateurs

Les UTILISATEURS doivent respecter les usages autorisés de ces CERTIFICATS.
Dans le cas contraire, leur responsabilité pourrait être engagée.
L'UTILISATEUR d'un CERTIFICAT est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (cf. chapitre *Moyens offerts pour la vérification des certificats*) est à l'appréciation de l'UTILISATEUR selon leur disponibilité et les contraintes liées à l'application qu'il utilise.
Si le certificat de l'AC racine Certigna n'est pas installé sur le poste de l'UTILISATEUR, ce dernier doit le télécharger à partir du site https://www.certigna.fr, précisément aux adresses suivantes :
http://autorite.certigna.fr/ACcertigna.crt; http://autorite.dhimyotis.com/ACcertigna.crt
De même, le certificat de l'AC peut être téléchargé depuis les adresses suivantes :
http://autorite.certigna.fr/ACcertignasslpris.crt
http://autorite.dhimyotis.com/ACcertignasslpris.crt

Moyens offerts pour la vérification des certificats

Afin de vérifier la chaîne de certification, l'UTILISATEUR d'un CERTIFICAT peut télécharger les certificats d'autorité (AC RACINE et AC EMETTRICES) depuis le site : https://www.certigna.fr.
Le certificat d'AUTORITE RACINE peut être déjà installé sur le poste de travail de l'UTILISATEUR suivant la configuration logicielle de ce dernier.
Les éditeurs, Microsoft, Apple, et Mozilla, reconnaissent l'AC racine Certigna comme une autorité de confiance et intègrent son certificat dans les versions récentes de leurs logiciels. La liste de ces éditeurs pouvant évoluer, l'UTILISATEUR peut se connecter au site https://www.certigna.fr pour obtenir la dernière mise à jour.
Afin de vérifier le statut de REVOCATION d'un CERTIFICAT, l'AC publie de façon périodique la LCR et offre un service d'information sur le statut de révocation des CERTIFICATS (serveur OCSP, pour On-line Certificate Status Protocol).
Cette liste des certificats révoqués et ces services sont accessibles pour les applications utilisant les certificats aux adresses contenues dans les CERTIFICATS :
- PDL, Point de Distribution des LCR : adresses http et ldap pour télécharger les LCR
- Adresses http des serveurs OCSP pour interrogation sur le statut du CERTIFICAT

Pour des questions de disponibilité, chaque serveur est doublé.
Les différentes adresses sont les suivantes :
- Pour accéder à la LCR
    http://crl.certigna.fr/certignasslpris.crl
    http://crl.dhimyotis.com/certignasslpris.crl
    ldap://ldap.certigna.fr/cn=Certigna SSL PRIS, OU=IGC, DC=certigna, DC=fr?certificateRevocationList;binary
    ldap://ldap.dhimyotis.com/cn=Certigna SSL PRIS, OU=IGC, DC=certigna, DC=fr?certificateRevocationList;binary

- Pour accéder au serveur OCSP
    http://sslpris.ocsp.certigna.fr ; http://sslpris.ocsp.dhimyotis.com

Etendue de responsabilité

La responsabilité de l'AC ne peut être engagée en cas de compromission de la clé privée du SERVEUR. L'AC ne sera en aucun cas responsable des éventuels dommages ayant leur origine dans l'utilisation d'un CERTIFICAT. L'AC ne saurait être tenue responsable de problèmes relevant de la force majeure, au sens du Code civil. Si un cas de force majeure a une durée supérieure à quinze jours, le RCAS sera autorisé à mettre un terme au CONTRAT et il n'y aura pas de préjudice.

Contrat et modifications

Le CONTRAT annule tout engagement antérieur. Le RCAS convient que, pendant la durée du CONTRAT, l'AC pourra modifier les conditions générales d'utilisation. Toutefois, les conditions acceptées et signées par le RCAS restent valides pendant toute la durée du CONTRAT, sauf si le RCAS accepte explicitement les nouvelles conditions émises et publiées par l'AC sur le site https://www.certigna.fr. Un courrier doit dans ce cas être adressé à l'AC en y joignant les nouvelles conditions générales d'utilisation sur lesquelles sont portées la mention "lu et approuvé", la date et la signature du RCAS. En cas de renouvellement du CONTRAT (renouvellement du CERTIFICAT à la fin de validité de ce dernier ou après sa révocation), le nouveau CERTIFICAT est soumis aux conditions générales d'utilisation en vigueur.

Résiliation

Au cas où l'une des parties n'exécuterait pas l'une des obligations découlant des présentes conditions générales, l'autre partie pourra lui notifier d'exécuter ladite obligation. A défaut pour la partie défaillante de s'être exécutée dans les quinze jours de cette notification, l'autre partie pourra résilier le CONTRAT.

Conditions de remboursement

La commande de CERTIFICAT ne peut être annulée dès lors que le dossier est en cours de traitement. Tout CERTIFICAT émis ne peut faire l'objet d'une demande de remboursement.

Données personnelles

Les données personnelles seront utilisées par l'AC uniquement dans le cadre des services de certification. Ces données sont archivées par l'AC pendant toute la durée du CONTRAT augmentée d'un délai de trois mois.
Le RCAS est informé que ses informations personnelles d'identité peuvent être utilisées comme données d'authentification lors d'une éventuelle demande de REVOCATION. L'AC informe le RCAS que les dossiers de demande de certificat comportant les données personnelles sont archivés aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable. Les informations que tout RCAS remet à l'AE sont intégralement protégées contre la divulgation sans le consentement de celui-ci, une décision judiciaire ou autre autorisation légale.

Cession du contrat

Le RCAS ne peut pas céder ses droits liés au CONTRAT.

Règlement de conflits

Le CONTRAT est soumis au droit français. Les parties s'engagent à tenter de résoudre à l'amiable tout différend susceptible d'intervenir entre elles, soit directement soit via un médiateur, dans les 2 mois de la réception du courrier avec accusé réception informant du différend. Les éventuels frais de médiation seront supportés par moitié par chacune des parties. Le cas échéant, l'affaire sera portée devant le tribunal de commerce de Lille.

Coordonnées de la société Dhimyotis

Dhimyotis S.A., Zone de la plaine 20 allée de la râperie 59650 Villeneuve d'Ascq
Tél: +33 320 792 409 - Fax: +33 956 952 412
Email: contact@dhimyotis.com