Conditions Générales d'Utilisation du cachet serveur
AC Adria DigiTrust Corporate
Cachet serveur avancé

Objet	Conditions Générales d'Utilisation du certificat à la volée délivré par Adria DigiTrust
OID	1.2.504.1.2.2.19

Date	Version	Rédacteur	Evolutions
11/12/2023	1.0	Adria Digitrust	Création de document
22/03/2024	1.1	Adria Digitrust	• Mise à jour de la partie eKYC • Mise à jour de la partie traitement des données personnelles
29/03/2024	1.2	Adria DigiTrust	• Mise à jour de l'OID de la PC/DPC de l'AC de signature et l'URL des ressources sur le portail Adria DigiTrust. • Mise à jour des règles de gestion et utilisation des clés privées de cachet serveur et compromission de la clé privée du cachet serveur. • Mise à jour des modalités de traitement d'une demande de cachet serveur et engagement/responsabilités des acteurs • Introduction de l'engagement de l'Autorité d'Enregistrement Déléguée (AED). • Intégration de la section Conformité à la norme ETSI EN 319 411-1 LCP
01/10/2024	1.3	Adria DigiTrust	• Mise à jour de la section Engagements du RCCS • Mise à jour de la section Méthode pour inviter le RCCS à activer sa clé privée pour le cachetage • Mise à jour de la section Engagements et obligations du RCCS

Date	Version	Validation
02/10/2023	1.0	Rachid BEKKAR/DG
22/03/2024	1.1	Rachid BEKKAR/DG
08/04/2024	1.2	Rachid BEKKAR/DG
10/10/2024	1.3	Rachid BEKKAR/DG

Table des matières

1. Objet

Les présentes conditions ont pour objet de préciser les modalités de demande et d'utilisation d'un certificat Cachet Serveur avancé, ainsi que les engagements et obligations respectifs des parties liées aux présentes. Les conditions générales d'utilisation découlent de la Politique de certification et Déclaration des pratiques de certification (PC/DPC) de l'Autorité déléguée des certificats Cachet Serveur avancé Adria DigiTrust disponible à l'adresse : https://pki.adria-digitrust.com/cp.html et enregistrée sous l'OID : 1.2.504.1.2.2.1.2

Le porteur de certificat accepte les présentes CGUs au moment de la réalisation de l'opération de cachetage électronique dans la plateforme Adria DigiTrust.

2. Définitions

- **Certificat** : certificat Adria DigiTrust Cachet Serveur constitué d'un fichier de données électroniques signé numériquement, conforme à la norme X.509 v3, contenant des informations sur l'application Métier d'une personne morale, lui permettant de signer d'importants volumes de documents en simultané pour garantir leur intégrité et leur authenticité.
- **Prestataire de services de Confiance Numérique (PSCN)** : Toute personne ou entité qui est responsable de la mise en œuvre et la gestion un et\ou plusieurs service(s) de confiance numérique(s) tels qu'ils sont définis dans la loi 43-20 relative aux services de confiance pour les transactions électroniques.
- **Autorité d'Enregistrement (AE)** : Au sein d'un PSCN, une entité a en charge la prise en compte des demandes de certificats et éventuellement des demandes de révocation des certificats.
- **Autorité de Certification (AC)** : Au sein d'un PSCN, une entité a en charge l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification.
- **AC Racine** : Une Autorité de Certification située au sommet d'une hiérarchie d'ACs.
- **AC Déléguée** : Autorité dont le certificat a été signé par AC Racine.
- **Demande de certificat** : ensemble constitué du formulaire d'obtention du certificat signé (acceptant les présentes conditions générales) accompagné des pièces justificatives et du paiement.
- **Client** : personne morale lié avec l'AC par un Contrat pour l'acquisition d'un Certificat Cachet serveur en son nom
- **Représentant Légal** : personne physique disposant des pouvoirs de représenter la personne morale de par la loi. Elle dispose de la faculté de procéder à des demandes d'émission et de révocation de certificats Cachet Serveur au bénéfice de la personne morale. Elle peut mandater un responsable du certificat pour assumer ces responsabilités.
- **Responsable du certificat Cachet Serveur (RCCS)** : Personne physique en charge et responsable au nom d'une personne morale du certificat électronique Cachet Serveur. En particulier, elle fait la demande de génération, révocation du certificat Cachet Serveur. C'est à lui que Adria DigiTrust remet le certificat Cachet Serveur et le code d'activation.

- **Contrat** : relation entre l'AC et le client, représenté par le RCCS.
- **LCR** : Liste des Certificats Révoqués.
- **OID** : identifiant d'objet (Object IDentifier).
- **Révocation** : opération consistant à anticiper la fin de validité d'un Certificat initialement prévue et dont la date est inscrite dans le Certificat.
- **PC/DPC** : Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.
- **Applications métier utilisatrices** : Services applicatifs en ligne liées par voie contractuelle avec la plateforme Adria DigiTrust pour exploitation des certificats émis par l'Autorité de Certification pour des besoins de cachetage électronique.

3. Champs d'application

Les Certificats cachets serveurs générés par l'AC sont destinés à des personnes morales et sont utilisés Uniquement dans la plateforme de cachetage électronique Adria DigiTrust lors d'une transaction de cachetage.
Ces Certificats ne peuvent pas être utilisés dans d'autres plateformes.
Ces Certificats sont stockés dans un module de sécurité sous contrôle de l'AC et ne sont utilisables que durant la transaction de cachetage, à chaque transaction de cachetage via notre portail, le RCCS doit fournir son code d'activation pour passer ces transactions via notre portail en toute sécurité en passant via un module d'authentification forte.
Le prestataire Adria DigiTrust conserve pendant 10 ans les journaux et les traces concernant la délivrance et l'utilisation des clés privées des porteurs, ainsi que les contrats et CGUs validés par le RCCS.

4. Documents de références

- La Politique de certification et Déclaration des pratiques de certification (PC/DPC) de l'Autorité déléguée des certificats Cachet Serveur avancé Adria DigiTrust disponible à l'adresse : https://pki.adria-digitrust.com/cp.html et enregistrée sous l'OID : 1.2.504.1.2.2.1.2
- La politique de gestion de preuve (PGP) du prestataire de signature électronique Adria DigiTrust disponible à l'adresse https://pki.adria-digitrust.com/cgu.html et enregistrée sous l'OID : 1.2.504.1.2.2.4

5. Durée

- La durée de vie du Certificat peut être 1 an, 2ans, ou 3ans, selon le choix du RCCS.
- Le Contrat entre l'AC et RCCS démarre le jour de la notification du RCCS de la disponibilité de son certificat par l'AE.

Le prestataire Adria DigiTrust conserve pendant 10 ans les journaux et les traces concernant la délivrance et l'utilisation des clés privées du certificat, ainsi que le contrat et les CGUs validés par le RCCS.

6. Modalité d'obtention du Certificat cachet serveur

L'AE procède à la vérification de dossier d'enregistrement avec les pièces justificatives. Le RCSS fournit obligatoirement son numéro de téléphone GSM et son adresse mail pour des fins de notification.
Après la validation de dossier d'enregistrement, l'AC procède à la génération du Certificat.

Pour plus de détails, voir la PC/DPC de l'Autorité déléguée des certificats Cachet Serveur avancé Adria DigiTrust disponible à l'adresse : https://pki.adria-digitrust.com/cp.html et enregistrée sous l'OID : 1.2.504.1.2.2.1.2

7. 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 du prestataire PSCN Adria DigiTrust. Le prix du certificat est payable à la commande (envoi règlement avec le dossier de demande), sauf accord explicite.

8. Engagements du RCCS

Lors de sa Demande de Certificat, le RCCS doit être vigilant dans la fourniture des informations d'enregistrement, un Certificat n'étant pas modifiable. Il transmet à l'AE, en main propre ou par voie postale/électronique, le formulaire d'obtention du certificat cachet serveur, (le formulaire ext disponible en ligne sur le portail https://pki.adria-digitrust.com/publications.html ou via notre point de contact : contact@adria-digitrust.com), le moyen de paiement correspondant au règlement du montant, ainsi que les pièces justificatives. L'AE accuse par mail de la réception de la demande électronique. Il appartient au RCCS de se rapprocher de l'AE en cas de non transmission par cette dernière de cet accusé de réception.

Le RCCS accepte explicitement le Certificat dans les 7 jours calendaires suivant sa réception auprès de l'AE ou au moment de sa première utilisation, selon celle de ces deux dates qui sera la plus proche dans le temps.

Une fois le certificat généré, le responsable en est informé par un message électronique envoyé à l'adresse indiquée, lui signalant la disponibilité du certificat. Toutefois, les moyens d'activation du cachet serveur resteront sous le contrôle exclusif du responsable du cachet serveur et lui seront transmis au moment du cachetage via un canal SMS sur son numéro de téléphone personnel ainsi que par email.

Le certificat cachet serveur est généré et stockée d'une manière sécurisée par la plateforme Adria Digitrust après l'aboutissement du processus de la validation d'identité du demandeur par l'AE. La génération des clés publique et privée du certificat cachet serveur se fait dans le module cryptographique de la plateforme d'Adria DigiTrust certifié Critères Communs *EAL4+*.

En cas d'une non-acceptation par le RCCS, le Certificat est automatiquement révoqué par l'AE.

Le RCCS est responsable de la confidentialité des codes d'activation du certificat qui lui ont été envoyés pour le cachetage des documents.

En cas de changement de RCCS pendant la validité du Certificat, le nouveau RCCS doit être obligatoirement enregistré auprès de l'AE.

Le Certificat doit être utilisé uniquement pour les usages décrits dans la PC/DPC correspondante et repris également dans le chapitre Conditions d'usage des certificats et des clés privées associées.

Le RCCS s'engage à ne plus utiliser un Certificat suite à l'expiration ou à la révocation de ce dernier.

9. Engagements propres à l'AE et à l'AC

A la réception complète de la Demande de certificat, l'AE vérifie la conformité de la demande. En cas de conformité de la demande, l'AE informe par mail le RCCS que sa Demande de Certificat est validée. Puis, L'Autorité de Certification (AC) génère le certificat dans un délai de cinq jours ouvrés. Ensuite, les codes d'activation seront transmis au RCCS par les canaux de communication, accompagné d'un e-mail détaillant les modalités d'utilisation de son propre certificat cachet serveur.

En cas de non-conformité de la demande ou en cas de dossier incomplet, l'AE demandera par mail au RCCS d'effectuer les modifications sous 7 jours calendaires, le cas échéant elle pourra rejeter la demande et le paiement sera restitué.

L'AC est tenu 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/email aux heures de bureau. Elle fournit également un service de consultation en ligne sur le site https://pki.adria-digitrust.com/crl.html permettant à tout moment aux tiers de vérifier la validité des Certificats émis par elle.

10. 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 de la personne morale des informations contenues dans le Certificat ;
- Non-respect des engagements du RCCS (notamment sur les conditions d'usage du Certificat), engagements découlant de la PC/DPC de l'AC ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- Pour des raisons techniques ;
- Destruction ou altération du support de remise de Certificat ;
- L'arrêt définitif de l'application métier ou la cessation d'activité de l'entité du RCCS ;

En cas de connaissance d'une des précédentes conditions, le RCCS s'engage à demander immédiatement la révocation du Certificat auprès de l'AE. En conséquence, l'AC révoquera de fait le Certificat.

La demande de révocation peut être effectuée par :

- Le RCCS ;
- Le représentant légal de personne moral ;
- L'AC ou l'AE.

La demande de révocation peut être effectuée :

- Par demande papier signée (par le représentant légal ou le RCCS) ;
- En ligne, par l'envoi d'un courriel électronique à l'adresse de contact Adria DigiTrust contact@adria-digitrust.com (uniquement pour le RCCS).

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. Pour les demandes en ligne, le demandeur doit fournir des informations personnelles (renseignées dans le formulaire d'obtention de certificat) et/ou signer ´électroniquement la demande.

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 Révocation, le prix versé par la personne morale reste acquis à l'AC.

11. Conditions d'usage des certificats et des clés privées associées

Le Certificat est utilisé pour vérifier la signature des documents transmis par l'application métier de la personne morale. L'utilisation de la clé privée et du certificat Cachet Serveur associée est strictement limitée pour réaliser des transactions de cachetage électronique sur des documents électroniques. Les responsables des certificats doivent respecter strictement les usages autorisés des certificats Cachet Serveur. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'utilisation de la clé privée est strictement limitée à cet usage. En cas de non-respect de l'usage de la clé privée, la responsabilité du RCCS pourrait être engagée.

L'usage autorisé de la bi-clé et du certificat associé est indiqué dans le certificat lui-même via l'extension critique « keyUsage ».

12. Méthode pour inviter le RCCS à activer sa clé privée pour le cachetage

La transaction de cachetage électronique se déroule sur la plateforme Adria DigiTrust. Cette plateforme offre au RCCS un portail sécurisé et intuitif, lui permettant d'initier le processus de cachetage des documents qu'il souhaite traiter.

Pour activer sa clé privée liée au certificat de cachet serveur doit passer par un processus d'authentification forte, le RCCS dispose de deux méthodes d'activation:

- La saisie d'un code secret OTP, créé et envoyé au moment du cachetage au RCCS via les canaux SMS et/ou e-mail. Ce code OTP est à usage unique et a une durée de validité limitée.

- Utilisation d'une clé secrète (secret key) généré par Adria DigiTrust. Ce secret respecte rigoureusement les recommandations de sécurité en matière de taille et de complexité. Ce secret est fourni au RCCS pour qu'il puisse l'utiliser au moment de cachetage de ces documents.

La clé privée peut être activée par l'une des deux méthodes selon le contrat signé avec le client.

Le RCCS peut récupérer les documents cachetés soit à partir de l'interface de résultats de la transaction électronique, soit depuis son espace dédié sur le portail Adria DigiTrust.

La clé privée est strictement liée au RCCS, qui est le seul à posséder le code d'activation associé. En effet, pour utiliser sa clé privée, le RCCS doit entrer son code d'activation sur la plateforme. Sans cette étape, la transaction ne peut pas débuter.

13. Engagements et obligations du RCCS

Le RCCS a l'obligation de :

- Communiquer des informations exactes et à jour lors de la demande du Certificat.
- Veillez à la confidentialité des codes d'activation.
- Accepter les présentes conditions générales d'utilisation ;
- Vérifier que les données présentes dans le certificat qui lui est remis sont correctes ;
- Faire, sans délai, une demande de révocation de son certificat auprès du client et\ou l'AC en cas de vol ou perte du code d'activation de la clé privée du Certificat.
- L'acceptation du Certificat émis par l'AC est tacite dès la signature/cachetage du porteur dans la plateforme de signature/cachetage du prestataire Adria DigiTrust.

14. Engagement du client ou de l'autorité d'enregistrement délégué

L'AE est gérée et opérée par Adria DigiTrust. Elle peut fait l'objet d'une délégation par voie contractuelle au responsable d'une application Métier qui utilise la plateforme Adria Digitrust.

La vérification de l'identité du RCCS et son organisation, au vu de la création du certificat cachet serveur avancée peut être déléguée par Adria DigiTrust à une autorité d'enregistrement tierce ou à un partenaire tiers (sous-traitant) en charge uniquement de la vérification de l'identité.

Dans ce cas, une convention à part entre les deux parties décrit obligatoirement les pointes suivantes :

- Les relations, les missions et les obligations et rôles et responsabilités du client vis-à-vis l'AE Adria DigiTrust.
- Précise les moyens de contrôle mis en place pour permettre au l'AE Adria Digitrust de vérifier la
- Conformité et le respect des engagements du tiers ;
- Les modalités d'établissement des preuves de vérification de l'identité.

La présence convention donne le droit et la capacité à l'AE Adria digiTrust de :

- Contrôler, à tout moment, les procédés utilisés par le tiers
- Contrôler le respect de sens engagements contractuels dans le cadre de la fourniture du service de confiance ;
- Apporter les preuves/garanties du respect des exigences du référentiel relatif aux services de confiance non qualifiés et aux prestataires fournissant ces services.

15. Engagements propres à l'AE et à l'AC

A la réception de la demande de certificat, l'AE vérifie la conformité de la demande. En cas de conformité de la demande, l'AC crée le Certificat immédiatement et envoie au RCCS une notification de disponibilité de son certificat sur son adresse email.

L'AC est tenu 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://pki.adria-digitrust.com/crl.html permettant à tout moment aux tiers de vérifier la validité des Certificats émis par elle.

16. Vérification des Certificats

Afin de vérifier la chaîne de certification par le client et les applications Métier utilisatrices, les certificats des ACs du PSCN Adria DigiTrust (AC Racine et AC Déléguée) sont téléchargeables depuis le site : https://pki.adria-digitrust.com/cc.html
Afin de vérifier le statut de Révocation d'un Certificat, l'AC publie de façon périodique la LCR et offre un service d'information sur le statut de Révocation des Certificats (service OCSP, pour On-line Certificate Status Protocol). Cette liste des certificats révoqués et ce service OCSP sont accessibles pour les applications utilisant les certificats aux adresses contenues dans les CERTIFICATS :

- PDL, Point de Distribution des LCR : adresses https://pki.adria-digitrust.com/crl.html pour télécharger les LCR
- Adresse https://adt-ocp.adria-digitrust.com du service OCSP pour interrogation sur le statut du Certificat

Pour des questions de disponibilité, une configuration redondante est garantie pour ces services
Les différentes adresses sont les suivantes :

- Pour accéder à la LCR https://pki.adria-digitrust.com/crl.html ;
- Pour accéder au service OCSP https://adt-ocp.adria-digitrust.com

17. Compromission de la clé privée

Pour les certificats de RCCS, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.
Le portail AdriaDigiTrust surveille les listes de révocation des certificats (CRL) pour vérifier l'état de révocation des certificats associés à la clé privée. Un certificat révoqué peut indiquer une compromission.

Le portail AdriadigiTrust met à disposition des règles techniques de contrôle pour suivre l'utilisation des clés privées. Surveillez les schémas d'utilisation des clés et recherchez toute activité inhabituelle ou non autorisée, telle que des opérations de décryptage ou de signature inattendues.
Dès la confirmation de la compromission d'une clé privée, cessez immédiatement de l'utiliser à toutes fins, sauf pour le déchiffrement de la clé, si nécessaire. Cela peut impliquer la révocation du certificat de la clé, de même notre portail Adria DigiTrust ne permet pas l'utilisation d'un certificat révoqué.

18. Etendue de responsabilité

La responsabilité de l'AC ne peut être engagée en cas de compromission de la clé privée du Certificat cachet Serveur. L'AC ne sera en aucun cas responsable des éventuels dommages ayant leur origine dans l'utilisation du Certificat. L'AC ne pourra pas être impliqué par des retards ou pertes que pourraient subir les données transmises sur lesquelles est apposée la signature du Certificat cachet serveur.

L'AC ne saurait être tenue responsable de problèmes relevant de la force majeure. Si un cas de force majeure a une durée supérieure à quinze jours, le RCCS sera autorisé à mettre un terme au Contrat et il n'y aura pas de préjudice

Le Client reste seul responsable envers Adria DigiTrust du respect des droits du mandataire conformément aux documents contractuels et de l'exécution satisfaisante de leurs obligations. De plus, le Client s'engage à indemniser Adria digiTrust contre toute action en justice, réclamation ou demande formulée à son encontre, ainsi que contre tout dommage résultant directement ou indirectement du non-respect par le Client, un Mandataire ou un Porteur de l'un quelconque des termes des documents contractuels.
La responsabilité d'Adria DigiTrust se limite aux dommages matériels résultant directement de son défaut d'exécution de ses obligations telles que définies dans les documents contractuels.

Adria DigiTrust décline toute responsabilité en cas de non-respect par le Client, le Mandataire ou le Porteur de leurs obligations, à l'exception de celles explicitement stipulées dans sa PC/DPC de l'Autorité déléguée des certificats Cachet Serveur sous l'OID : 1.2.504.1.2.2.1.2 et les documents contractuels.

Si la responsabilité d'Adria digiTrust est engagée, les dommages et indemnités qui lui incombent, quelle qu'en soit la nature et le montant, ne pourront en aucun cas excéder le prix d'achat du Certificat. Dans tous les cas, la responsabilité cumulée d'Adria digiTrust pour un service spécifique, quelle que soit la cause ou la forme de l'action intentée, ne dépassera pas le montant total payé par le Client pour ledit service, conformément aux limites prévues.

19. Contrat et modifications

Le Contrat annule tout engagement antérieur. Le RCCS convient que, pendant la durée du Contrat, l'AC pourra modifier les conditions générales d'utilisation. Toutefois, les conditions acceptées et signées par le RCCS restent valides pendant toute la durée du Contrat, sauf si le RCCS accepte explicitement les nouvelles conditions émises et publiées par l'AC sur le site https://adria-digitrust.com/cgu.html. 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 approuvée", la date et la signature du RCCS.

20. Preuve

Les Parties conviennent expressément que dans le cadre de leur Contrat, les messages électroniques datés et signés valent preuve entre elles et justifient que la notification est imputable à la partie émettrice dudit message.
Il est expressément convenu que pour la preuve des échanges entre l'AC et le représentant légal ou le RCCS, seules les archives de l'AC et de l'AE font foi entre les parties.

21. Assurance

L'AC Adria DigiTrust atteste avoir souscrit une assurance Responsabilité Civile et Professionnelle concernant les prestations relatives au présent Contrat.
En cas de dommage direct subi par le client suite à une faute professionnelle de l'AC, le Client est dédommagé à la hauteur du prix du Certificat cachet serveur et du Support cumulé..

22. Sous-traitance

Le Client autorise expressément l'AC à communiquer à ses partenaires auxquels elle pourrait sous-traiter certains travaux, les données, notamment celles à caractère personnel le concernant, nécessaires à l'exécution de ceux-ci.

23. 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 (15) jours de cette notification, l'autre partie pourra résilier le Contrat.

24. Données personnelles

Les données personnelles incluent les informations nominatives de l'individu concerné, enregistrées dans le dossier d'enregistrement, sur le certificat électronique et sur tous les supports utilisés pour gérer le cycle de vie du certificat. Des mesures techniques, fonctionnelles et organisationnelles sont mises en œuvre afin de garantir la protection de ces données dès l'enregistrement du dossier et tout au long des différentes étapes de gestion du cycle de vie des Certificats.

Toute collecte de données à caractère personnel dans le cadre de ce Contrat est réalisée dans le strict respect de la loi N° 09-08.
Peuvent seuls, dans les limites de leurs attributions respectives, être destinataires des données collectées précitées : Le personnel chargé de la fourniture du service, la DGSSI, les dispositifs de contrôle interne et externe, et toutes les autorités habilitées conformément à la réglementation en vigueur.

Conformément à la loi n°09-08, Les données à caractère personnel peuvent à tout moment faire l'objet d'un droit d'accès, de modification, de rectification et d'opposition auprès d'Adria DigiTrust :
•Mail : contact@adria-digitrust.com

Les informations suivantes sont considérées comme confidentielles :
- Les données secrètes associées au certificat (clé privée),
- Les journaux de la plateforme AdriadigiTrust
- Les données personnelles du « RCCS » et de son organisation qui sont utilisées pour la génération de certificat cachet serveur et pour le processus d'identification/authentification et de notification.

Adria DigiTrust pourra utiliser les données à caractère personnel pour faire profiter le client d'autres produits et services.

25. Protection des données personnelles

En cas de détection de perte d'intégrité des données ou atteinte à la sécurité qui peuvent porter préjudice au porteur du certificat, Adria DigiTrust informera le porteur dans un délai de 24 heures par écrit à son adresse mail.

La nature des données collectées sont les données d'identification du porteur. En acceptant ces CGU, le client donne son consentement pour l'utilisation de ces données dans le strict respect des mesures légales nécessaires garantissant la protection de ces derniers.

Le client peut accéder aux informations les concernant, les rectifier et s'opposer au traitement de ses données pour motif légitime, en adressant un courrier électronique à l'adresse suivante : contact@adria-digitrust.com.

Les données à caractère personnel traitées sont collectées directement/indirectement auprès du Signataire, voilà la liste des données collectés :

- Nom de la famille : Identification du RCCS et enregistrement dans le Dossier d'enregistrement
- Prénom : Identification du Signataire et enregistrement dans le Dossier d'enregistrement
- Numéro de téléphone : Envoi d'un secret d'activation et pour des fins d'authentification et enregistrement dans le Dossier d'enregistrement
- Adresse email : Envoi des emails de notification et modalités d'utilisations et enregistrement dans le Dossier d'enregistrement.
- N° document d'identité : Identification de RCCS auprès de service DGSN ou de l'AE aDria DigiTrust et enregistrement dans le dossier d'enregistrement
- Adresse IP : Enregistrement dans le Dossier de preuve
- Image de cachetage : Enregistrement dans le Dossier de preuve
- Autres données pouvant se trouver dans un Jeton d'Identité : Vérification/authentification de la transaction de cachetage et enregistrement dans le Dossier de preuve

26. Cession du contrat

Le RCCS ne peut pas céder ses droits liés au Contrat.

27. Règlement des litiges

Le présent Contrat et l'ensemble des documents contractuels sont régis par la Loi marocaine.
Tout litige relatif à la validité, à l'exécution ou à l'interprétation des présentes conditions générales ou des dispositions de l'intégralité des accords entre les parties sera soumis à la compétence des tribunaux marocains du ressort de l'AC.

28. Intégration de Modules eKYC pour la vérification d'Identité

Dans le cadre de nos services, nous avons intégré des modules eKYC (Know Your Customer) pour la vérification d'identité des responsables de cachet serveur au moment de la validation de la demande de certificat. Cette intégration est basée sur le module KYC DGSN Mon e-ID fourni par la **Direction Générale de la Sûreté Nationale** se module est basée sur les briques suivantes :

- Processus de Vérification : Ce module eKYC permet la vérification de l'identité des utilisateurs en temps réel en utilisant les services de la DGSN.
- Engagements des Utilisateurs : Les utilisateurs reconnaissent et acceptent que les informations personnelles fournies dans le cadre du processus eKYC soient soumises à la vérification par la DGSN.
- Utilisation des Informations : Les informations vérifiées peuvent être utilisées dans le cadre de nos services conformément à notre politique de confidentialité.
- Responsabilités : Nous ne sommes pas responsables des erreurs, omissions ou retards résultant du processus de vérification eKYC effectué par la DGSN.
- Conditions d'Utilisation : L'utilisation du module eKYC externe DGSN est sujette aux

En cas échéant, le RCCS passe par le module KYC interne d'ADRIA DigiTrust. À cet effet, le responsable devra disposer d'un document officiel justifiant son identité, comportant son nom, prénom, photo, date et lieu de naissance.

En acceptant nos conditions générales d'utilisation, les utilisateurs consentent à l'utilisation des modules KYC externe DGSN/ interne d'Adria DigiTrust pour la vérification de leur identité.

29. Conformité à la norme ETSI EN 319 411-1 LCP

Les présentes Conditions Générales d'Utilisation du cachet serveur avancé délivré par Adria DigiTrust sont conformes à la norme ETSI EN 319 411-1 LCP.

30. Coordonnées de la Société Adria DigiTrust

Les coordonnées d'Adria DigiTrust sont :

- Email : contact@adria-digitrust.com

31. Signature

En signant ci-dessous, vous confirmez avoir lu, compris et accepté les présentes Conditions Générales d'Utilisation.

Date : _____

Nom:_____

Signature : _____