Conditions Générales d'Utilisation du certificat à la volée

AC Adria DigiTrust Signature

Signature avancée

Objet	**Conditions Générales d'Utilisation du certificat à la volée délivré par Adria DigiTrust Signature avancée**
OID	**1.2.504.1.2.2.18**

Date	Version	Rédacteur	Evolutions
11/12/2023	**1.0**	**Adria Digitrust**	Création de document
19/03/2024	**1.1**	**Adria Digitrust**	• Mise à jour de la partie eKYC • Mise à jour de la partie champs d'application
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 des clés privées pour le signataire et compromission de sa clé • Introduction de l'engagement de l'Autorité d'Enregistrement Déléguée (AED). • Mise à jour de la partie sur la protection des données personnelles et identification des signataires. • Intégration de la section Conformité à la norme ETSI EN 319 411-1 LCP

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**

Table des matières

1. Objet

Modalités d'utilisation d'un certificat à la volée délivrée par l'Autorité de certification pour la réalisation d'une transaction de signature électronique à travers la plateforme de signature électronique en mode SaaS Adria DigiTrust.
Les présentes CGUs définissent les engagements et obligations respectifs des parties liées aux présentes. Elles découlent de la Politique de certification et Déclaration des pratiques de certification (PC/DPC) de l'Autorité déléguée des certificats à la volée Adria DigiTrust disponible à l'adresse : https://pki.adria-digitrust.com/cp.html et enregistrée sous l'OID : 1.2.504.1.2.2.1.1
Le porteur de certificat à la volée est une personne physique.
Le porteur de certificat accepte les présentes CGUs au moment de la réalisation de l'opération de signature dans la plateforme de signature électronique en mode SaaS Adria DigiTrust.

2. Définitions

- **Certificat** : certificat Adria DigiTrust à la volée constitué d'un fichier de données électroniques signé numériquement, conforme à la norme X.509 v3, contenant des informations sur le porteur, lui permettant de signer des documents lors d'une transaction de signature électronique via la plateforme de signature Adria DigiTrust.
- **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.
- **Porteur** : Personne physique à qui l'AC émet le certificat à la volée et son code d'activation pour signer électroniquement des documents électroniques.
- **Client :** entité légale responsable d'une application Métier, et ayant une relation contractuelle avec Adria DigiTrust pour faire appel à la plateforme Adria DigiTrust pour la signature électronique par le porteur des documents générés par cette application Métier.
- **LCR** : Liste des Certificats Révoqués.
- **OID** : identifiant d'objet (Object IDentifier).
- **DGSN :** Direction Générale de la Sûreté Nationale.
- **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.

- **KYC** : dispositif de sécurité permettant la vérification en ligne de l'identité des clients lors d'une transaction électrique. Le but derrière ce dispositif d'éviter l'usurpation d'identité des clients réalisant des transactions en ligne, et de s'assurer de la conformité vis-à-vis les législations et les réglementations sectorielles.

3. Champs d'application

Les Certificats à la volée générés par l'AC sont destinés à des personnes physiques et sont utilisés Uniquement dans la plateforme de signature électronique Adria DigiTrust lors d'une transaction de signature.
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 signature.
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 signataire.

4. Documents de références

- La Politique de certification et Déclaration des pratiques de certification (PC/DPC) de l'Autorité déléguée des certificats à la volée « Adria DigiTrust Signature » disponible à l'adresse : https://pki.adria-digitrust.com/cp.html et enregistrée sous l'OID : 1.2.504.1.2.2.1.1
- 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 de validité

La durée de vie du Certificat à la volée est entre 5 minutes et 2 heures.
Le Certificat est révoqué juste après l'opération de la signature électronique et cesse d'être valable.

6. Modalité d'obtention du Certificat

L'AE procède à la vérification de l'identité du futur porteur, ainsi que les pièces justificatives de son identité via le mécanisme KYC.
Le porteur fournit obligatoirement son numéro de téléphone GSM et son adresse mail.
Après la validation de l'identité du porteur, l'AC procède à la génération du Certificat.
Pour plus de détails, voir la PC/DPC de l'Autorité déléguée des certificats à la volée Adria DigiTrust disponible à l'adresse : https://pki.adria-digitrust.com/cp.html et enregistrée sous l'OID : 1.2.504.1.2.2.1.1

7. Utilisation de la clé privée du Certificat pour signature

La clé privée du Certificat est stockée et protégée par l'infrastructure du prestataire PSCN Adria DigiTrust.
Des moyens techniques et organisationnels sont mis en œuvre afin d'assurer que la clé privée ne sera utilisée que par le porteur. En aucun cas le prestataire Adira DigiTrust pourra utiliser cette clé pour son propre usage ou pour le compte d'une autre personne que le porteur.

8. Méthode pour inviter le porteur à signer par sa clé privée

La signature électronique par la clé privée se fait dans la plateforme de signature électronique. Cette dernière offre deux possibilités pour signer :

- Soit de façon transparente pour le porteur lorsque le processus de signature est adossé à l'application métier au Client.
- Soit en recevant un lien URL dans son adresse email l'invitant à procéder à la signature électronique.
- Le signataire sera invité à s'authentifier et à s'identifier sur le portail de la DGSN. Cette étape est transparente pour le signataire, car il sera automatiquement redirigé depuis notre portail vers le portail de la DGSN. De même, une fois que le signataire est identifié sur le portail de la DGSN, le même mécanisme sera adopté pour le rediriger automatiquement vers notre portail Adria DigiTrust.
- Ensuite, le signataire accède à un espace de consentement pour visualiser les documents à signer, avec différentes options telles que les ouvrir dans une fenêtre contextuelle, les télécharger, etc.
- Par la suite, le signataire accepte les conditions générales d'utilisation en exprimant son consentement via une case à cocher qu'il doit sélectionner pour confirmer son consentement, de même il possède la possibilité de consulter les CGUs de signature. Sinon, peut annuler la transaction via une option dédiée sur le portail.
- Ensuite, le portail Adria DigiTrust redirige le signataire vers un espace d'authentification où il doit saisir son code d'activation, qui lui sera envoyé soit par e-mail, soit par SMS sur les coordonnées GSM ou l'adresse e-mail fournies lors de l'initialisation de la transaction de signature.
- À la fin du processus, le signataire peut récupérer les documents signés ou se référer au portail Adria DigiTrust pour consulter les détails de la transaction de signature.

La clé privée est associée de manière logique au porteur et ce dernier est le seul à posséder le code de son activation.
En effet, pour pouvoir utiliser sa clé privée, le porteur devra saisir dans la plateforme de signature le code OTP qu'il a reçu sur son portable GSM et/ou sur son adresse mail.

9. Modalités de renouvellement

Le renouvellement des Certificats n'est pas autorisé.

10. Modalités de révocation

Le Certificat est révoqué une fois la clé privée associée est utilisée par le porteur en saisissant le code d'activation OTP qu'il lui a été transmis par SMS et/ou mail.
Le porteur et\ou l'application métier peut demander la révocation du Certificat dans les cas suivants :

- Le porteur a désisté et\ou a abandonné la transaction de signature,

- Les informations figurant dans le Certificat ne sont pas conformes avec l'identité du porteur.
- Le code d'activation transmis au porteur par GSM/MAIL est perdu ou volé.

La durée de vie du Certificat est très courte (Maximum 2 heures), cela entraîne que le recours aux demandes de révocation de la part du porteur et/ou l'application métier du Client est extrêmement rare.

11. Tarif

Sauf accord de l'AC, le prix de vente du Certificat à la volée est inclus dans le prix de la signature électronique de l'offre SaaS de la plateforme de signature de Adria DigiTrust. Il est fixé dans la grille tarifaire disponible sur demande auprès du service commercial du prestataire PSCN Adria DigiTrust.

12. Engagements du porteur

Le porteur a l'obligation de :

- Communiquer des informations exactes et à jour lors de la demande du Certificat.
- Protéger le code d'activation.
- Accepter les présentes conditions générales d'utilisation ;
- Vérifier que les données présentes dans le certificat du document signé 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 du porteur dans la plateforme de signature du prestataire Adria DigiTrust.
- Avant la réalisation de la signature, le porteur peut ne pas utiliser la clé privée associée au Certificat en refusant la saisie du code d'activation, ou en demandant la révocation du Certificat. Dans ce cas, la clé privée générée sera détruite de manière automatique par un processus technique.

13. 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 d'un utilisateur, au vu de la création du certificat électronique de signature électronique 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.

14. 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 le code d'activation au porteur dans son portable GSM et/ou son adresse mail.
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.

15. Vérification des Certificats

Afin de vérifier la chaîne de certification par le client, 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. Cette liste des certificats révoqués est accessible pour les utilisateurs et les applications utilisant les certificats aux adresses contenues dans les Certificats :

- PDL, Point de Distribution des LCR : adresse http pour télécharger les LCR https://pki.adria-digitrust.com/crl.html, pour le téléchargement de CRL de l'AC délégué de signature, il suffit juste de ce référencie au lien suivant : https://pki.adria-digitrust.com/sources/AdriaDigiTrustSignature.crl

Pour des questions de disponibilité, une configuration redondante est garantie pour la LCR.

16. Compromission de la clé privée

Pour les certificats de porteur, 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.

17. Etendue de responsabilité

L'AC ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme des Certificats.
L'AC décline sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes dans 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, L'AC 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 conditions générales d'utilisations.

18. Convention sur la preuve

Pour chaque signature électronique réalisée, L'AC et le Porteur acceptent que :

- Les éléments utilisés afin de procéder à la signature électronique des documents, à savoir le nom et prénom du Porteur, le numéro de portable GSM utilisé, l'adresse e-mail, le Certificat, les pièces justificatives d'identité.
- Les éléments d'horodatage électronique.
- Le code d'activation OTP
- Le dossier de preuves généré par la plateforme Adria DigiTrust à l'issue de l'opération de signature électronique.

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.
Ce dossier de preuve est archivé par le Client comme formalisé dans la PGP du prestataire Adria DigiTrust.

19. Conditions d'indemnisation

Aucune indemnisation n'est possible dans le cadre des présentes conditions générales d'utilisation

20. 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.

21. Données personnelles

Les données collectées par l'AC, notamment celles à caractère personnel, sont nécessaires à la production, la fourniture et la gestion des certificats électroniques et les services y afférents. Tous les champs sont obligatoires, à défaut l'AC ne pourra traiter la demande de certificat.
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 de 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 de signature électronique
- Les données personnelles du « Signataire » qui sont utilisées pour la génération de certificat à la volée et pour le processus d'identification/authentification et la génération de dossier de preuve.

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

22. 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 Signataire et enregistrement dans le Dossier de preuve
- Prénom : Identification du Signataire et enregistrement dans le Dossier de preuve
- Numéro de téléphone : Envoi d'un OTP SMS pour la Signature afin d'authentifier le Signataire et enregistrement dans le Dossier de preuve
- Adresse email : Envoi d'un OTP courriel pour la Signature afin d'authentifier le Signataire et enregistrement dans le Dossier de preuve
- N° document d'identité : Identification de signataire auprès de service DGSN et enregistrement dans le dossier de preuve
- Adresse IP : Enregistrement dans le Dossier de preuve
- Image de signature : Enregistrement dans le Dossier de preuve
- Autres données pouvant se trouver dans un Jeton d'Identité : Vérification/authentification du Signataire et enregistrement dans le Dossier de preuve

23. Règlement des litiges

Les présentes CGUs 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.

24. 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 utilisateurs. 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 seront 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 acceptant nos conditions générales d'utilisation, les utilisateurs consentent à l'utilisation des modules KYC externe DGSN pour la vérification de leur identité.

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

Les présentes Conditions Générales d'Utilisation du certificat à la volée pour la signature avancée, délivré par Adria DigiTrust, sont conformes à la norme ETSI EN 319 411-1 LCP.

26. Coordonnées de la Société Adria DigiTrust

Les coordonnées de Adria DigiTrust sont :

- Email : contact@adria-digitrust.com