Politique de signature
ADRIA Digitrust

Objet :	**Politique de Signature De l'application Métier « Contractualisation en ligne » Au profit « de Clients et Prospects »**
OID	**1.2.504.1.2.2.30**

Date	Version	Rédacteur
15/07/2021	**1.0**	**ADRIA Digitrust**
19/06/2024	**1.1**	**Adria DigiTrust**

Table des matières

1. Contexte et objectif

Dans le contexte de l'évolution vers la transformation numérique, la signature électronique est de plus en plus utilisée de manière généralisée dans diverses opérations commerciales. Lorsque les fonctions de signature électronique sont mises à disposition des signataires, il est important qu'ils aient connaissance du contexte dans lequel cette signature électronique est produite, des rôles, obligations que chaque acteur endosse, et des conditions dans lesquelles cette signature sera ultérieurement traitée, conservée, et disponible pour vérification. Cette compréhension est essentielle pour assurer une utilisation sécurisée et efficace de la signature électronique dans les opérations commerciales en pleine transformation numérique.

L'application « ADT eSign» permet au signataire de signer électroniquement les documents : des contrats, des opérations de Guichet, des ordres, etc et toutes opérations de gestion, en agence ou en ligne. Ces documents sont ensuite vérifiables et lisibles par les signataires via des outils de lecture de fichiers PDF.

Cette contractualisation en ligne est conforme aux dispositions légales en vigueur, notamment :

- La loi n° 43-20 relative aux services de confiance pour les transactions électroniques ;
- La loi n°09-08 relative à la protection des données personnelles ;

L'application « ADT eSign» se base sur la plateforme du prestataire des services de confiance numérique Adria DigiTrust qui assure en mode SaaS les services de confiances suivants :

- Emission des certificats à la volée pour les personnes physiques ;
- Emission des certificats cachet serveur pour les personnes morales ;
- Signature électronique ;
- Cachetage électronique ;
- Intégration du jeton d'horodatage électronique ;
- Gestion de la preuve électronique.

La présente politique de signature (PS) décrit :

- Les conditions dans lesquelles sont réalisées, traitées, conservées ces signatures électroniques, dans le cadre de l'application « ADT eSign », pour le profil de signataire ;
- Les conditions et contexte dans lesquels ces signatures électroniques seront ultérieurement consultables, utilisables, vérifiables.

La présente politique de signature (PS) est destinée aux :

- Signataires personne physique ;

- Signataires personne morale ;

La structure de la présente politique de signature (PS) est conforme à la norme « *ETSI TR 102 041 V1.1.1 (2002-02) : Signature Policies Report ».*

2. Politique de signature

2.1 Champ d'application

La présente politique de signature (PS) s'applique aux transactions électroniques réalisées à travers l'application «ADT eSign» pour signer des documents en ligne.

Lorsque des fonctions de signature électronique sont mises à disposition d'une population ou d'une entité, il est important que celle-ci ait connaissance du contexte dans lequel cette signature électronique est produite, des rôles, obligations que chaque acteur endosse, et des conditions dans lesquelles cette signature sera ultérieurement traitée, conservée et rendue disponible pour vérification.

La signature électronique apposée sur un ensemble de données permet de garantir :

- L'identité du signataire,
- L'intégrité du document signé,
- Le lien entre le document signé et la signature.

La signature électronique traduit ainsi la manifestation du consentement du signataire quant au contenu des données signées.

2.2 Politique jointe

Eu égard que l'opération de signature électrique est confiée au prestataire de confiance numérique Adria DigiTrust, la présente politique de signature est étroitement liée à la politique de gestion de preuve (PGP) d'Adria DigiTrust enregistré avec le OID : 1.2.504.1.2.2.4 et disponible dans le lien web : https://pki.adria-digitrust.com/cgu.html

2.3 Identification

La présente politique de signature est enregistrée sous l'OID 1.2.504.1.2.2.30

2.4 Point de contact et prise en compte des remarques

Les demandes d'information ou questions concernant la présente politique sont à adresser à :

- **Personne à contacter :** ADT Contact
- **Adresse :** 119, Bd abdelmoumen N° 15 2ème étage Casablanca

- **Email :** contact@adria-digitrust.com
- **Tel :** +212 6 15 13 37 34

2.5 Processus de mise à jour

2.5.1 Circonstances rendant une mise à jour nécessaire

La mise à jour de la présente Politique de signature peut avoir pour origine :

- Intégration d'un nouvel acteur ;
- Evolution du droit ;
- Besoin de s'adapter aux évolutions technologiques ;
- Observations des différents acteurs.

La présente politique est réexaminée lors de toute modification majeure de l'application « ADT eSign ».

2.5.2 Information des acteurs

Lorsqu'une mise à jour a été planifiée, les informations relatives à cette évolution sont mises en ligne sur les lieux de publication. La nouvelle version reste valide jusqu'à la publication de la version suivante.

3. Définitions et acronymes

Les définitions et acronymes sont disponibles dans le document « *la politique de gestion de la preuve (PGP)* » enregistré avec l'OID : 1.2.504.1.2.2.4 et disponible dans le lien web : https://pki.adria-digitrust.com/cgu.html

4. Acteurs et rôles

4.1 Les acteurs

4.1.1 Signataire personne physique

Un signataire personne physique désigne un individu identifié et reconnu en tant que tel, qui appose sa signature manuscrite ou électronique sur un document, contrat ou accord. La signature d'une personne physique engage sa responsabilité personnelle conformément aux termes et conditions de l'accord en question. Les signataires personnes physiques sont souvent désignés par leur nom, leur titre et leur position au sein d'une organisation.

4.1.2 Signataire personne morale

Un signataire personne morale fait référence à une entité juridique distincte de ses membres individuels, telle qu'une société, une entreprise, une association, une fondation ou

toute autre structure organisationnelle dotée de la capacité juridique. Lorsqu'une personne morale signe un document, elle le fait en tant que représentante de l'entité et non au nom d'un individu spécifique. La responsabilité légale qui découle de la signature d'une personne morale incombe à l'organisation elle-même, plutôt qu'à ses employés ou membres individuels.

4.1.3 Le prestataire de confiance numérique Adria DigiTrust

Le prestataire Adria DigiTrust intervient, dans le cadre de la présente politique de signature, en tant que :

- Autorité de certification (AC) : en exploitant une infrastructure de gestion de clés (PKI) pour l'émission des certificats à la volée et des certificats cachet serveur
- Prestataire de signature électronique : en exploitant la plateforme de signature électrique pour la réalisation de l'opération de la signature électronique des contrats et actes, avec intégration d'un jeton d'horodatage.
- Prestataire de la gestion de la preuve : en assurant la création du fichier de preuve associé à une opération de signature électronique et transmission du dossier de la preuve.

4.2 Rôles et obligations du signataire

Le signataire doit contrôler les données qu'il va signer avant d'y apposer sa signature électronique.

La plateforme d'Adria DigiTrust va amener le signataire à respecter ces trois étapes avant de signer électroniquement :

- Visualiser les documents à signer ;
- Valider la lecture et la compréhension des Conditions Générales du service
- Accepter formellement l'opération de signature.

4.2.1 Type de certificat utilisé

Le certificat utilisé par le signataire est un certificat à la volée émis par l'autorité de certification (AC) du prestataire des services de confiance numérique Adria DigiTrust Signature, en respect des exigences de la politique de certification (PC) : « *Politique de certification et Déclaration des pratiques de certification (PC/DPC) De l'Autorité déléguée des certificats à la volée Adria DigiTrust Signature* » enregistré avec l'OID : 1.2.504.1.2.2.1.1 et disponible dans le lien web : https://pki.adria-digitrust.com/cp.html

« *Politique de certification et Déclaration des pratiques de certification (PC/DPC) De l'Autorité déléguée des certificats à la volée Adria DigiTrust Signature Simple* » enregistré avec l'OID : 1.2.504.1.2.2.1.3 et disponible dans le lien web : https://pki.adria-digitrust.com/cp.html

4.2.2 Procédé fiable d'identification

Avant l'autorisation de l'opération de signature électronique et la génération du certificat à la volée du signataire, l'autorité d'enregistrement (AE) du prestataire des services de confiance numérique Adria DigiTrust procède à la vérification de l'identité du signataire, comme stipulé par la « *Politique de certification et Déclaration des pratiques de certification (PC/DPC) De l'Autorité déléguée des certificats à la volée Adria DigiTrust Signature* » enregistré avec le OID : 1.2.504.1.2.2.1.1 et disponible dans le lien web : https://pki.adria-digitrust.com/cp.html .

« *Politique de certification et Déclaration des pratiques de certification (PC/DPC) De l'Autorité déléguée des certificats à la volée Adria DigiTrust Signature Simple* » enregistré avec l'OID : 1.2.504.1.2.2.1.3 et disponible dans le lien web : https://pki.adria-digitrust.com/cp.html

4.2.3 Déroulement fonctionnel de l'acte de signature

Dans la plateforme de signature électronique Adria DigiTrust, l'acte de signature se déroule comme suit :

- Un texte explicite est présenté au signataire pour lui expliciter la portée de l'acte qu'il s'apprête à réaliser ;
- Le document que le signataire s'apprête à signer lui est présenté : il a la possibilité de le visualiser entièrement à travers son poste de travail ;
- Le signataire a la possibilité de renoncer et de refuser de signer ;
- Le signataire doit cliquer sur un bouton d'approbation pour valider la signature opérationnel après avoir coché la case « J'ai lu les conditions générales et j'accepte de signer tous les documents » dans toutes les clauses de consentement ;
- Le signataire doit saisir le code « OTP » qui lui a été envoyé dans son téléphone portal GSM ou par Email, et ensuite cliquer sur le bouton « valider » ;
- La plateforme Adria DigiTrust réalise l'opération de signature électronique du contrat ou acte avec le certificat à la volée et intégrations du jeton d'horodatage (l'horodatage est optionnel)
- La plateforme Adria DigiTrust réalise l'opération de signature électronique des documents avec le certificat cachet serveur dans le cas d'un signataire personne morale et intégrations du jeton d'horodatage (l'horodatage est optionnel).

4.2.4 Protection du certificat Client

La bi-clé associée au certificat à la volée du signataire est généré dans un matériel cryptographique de l'autorité de certification (AC) de la plateforme Adria DigiTrust. Aucun support n'est remis signataire.

Après l'opération de signature, l'AC détruit la bi-clé, conformément à la « *Politique de certification et Déclaration des pratiques de certification (PC/DPC) De l'Autorité déléguée des*

certificats à la volée Adria DigiTrust » enregistré avec l'OID : 1.2.504.1.2.2.1.1 et disponible dans le lien web : https://pki.adria-digitrust.com/cp.html et « *Politique de certification et Déclaration des pratiques de certification (PC/DPC) De l'Autorité déléguée des certificats à la volée Adria DigiTrust Signature Simple* » enregistré avec l'OID : 1.2.504.1.2.2.1.3 et disponible dans le lien web : https://pki.adria-digitrust.com/cp.html

4.2.5 Révocation du certificat

Le certificat à la volée du signataire a une durée de validité limitée et il est révoqué par la plateforme de signature suite après la réalisation de l'opération de signature électronique.

4.2.6 Limitation de la responsabilité Adria DigiTrust

Les signataires sont responsables du contenu des informations présentes dans le document signé, et de la bonne utilisation des certificats de signature dans ce cadre.

4.3 Rôles et obligations de Adria DigiTrust

4.3.1 Autorité de certification

Les obligations du prestataire de confiance numérique Adria DigiTrust sont détaillées dans les documents :

- « *Politique de certification et Déclaration des pratiques de certification (PC/DPC) De l'Autorité déléguée des certificats à la volée Adria DigiTrust* » enregistré avec l'OID (avancée et simple) : 1.2.504.1.2.2.1.1 et 1.2.504.1.2.2.1.3 et disponible dans le lien web https://pki.adria-digitrust.com/cp.html.
- « *Politique de certification et Déclaration des pratiques de certification (PC/DPC) De l'Autorité déléguée des certificats cachet serveur Adria DigiTrust* » enregistré avec l' OID (avancée et simple) : 1.2.504.1.2.2.1.2 et 1.2.504.1.2.2.1.4 et disponible dans le lien web https://pki.adria-digitrust.com/cp.html.

4.3.2 Prestataire de signature électronique et gestion de la preuve

Les obligations du prestataire de confiance numérique Adria DigiTrust sont détaillés dans le document « la politique de gestion de la preuve (PGP) » enregistré avec le OID : 1.2.504.1.2.2.4 et disponible dans le lien web : https://pki.adria-digitrust.com/cgu.html.

4.3.3 Limitation de la responsabilité Adria DigiTrust

Les signataires sont responsables du contenu des informations présentes dans le document signé, et de la bonne utilisation des certificats de signature dans ce cadre.

5. Signature électronique et validation

5.1 Données signées

Au moment de la signature électronique, le signataire signe électroniquement :

- Les documents visualisés par le signataire

5.2 Opération de signature électronique

La plateforme de signature du prestataire Adria DigiTrust garantit le déroulement des étapes suivantes, pour permettre au signataire d'avoir connaissance et conscience de l'action qu'il est sur le point d'effectuer :

- **Présentation du document à signer :** Le signataire a la possibilité de visualiser les informations du document que l'application de signature lui propose de signer.
- **Présentation des attributs de la signature au signataire :** Les Conditions Générales d'Utilisation du Service de signature du prestataire Adria DigiTrust sont présentées au signataire et précisent notamment les conditions dans lesquelles sa signature électronique sera réalisée et traitée.
- **Interaction avec le signataire (consentement explicite et possibilité d'arrêt du processus de signature) :** Le signataire a les moyens d'exprimer explicitement (c'est-à-dire, de manière volontaire et non ambiguë) son consentement pour sélectionner un document ou plusieurs documents et déclencher le processus de signature des documents sélectionnés.

5.3 Caractéristiques des signatures

5.3.1 Type de signature

L'application ADT eSign prend en charge la signature de tout type de document : PDF, XML, Word, etc

5.3.2 Norme de signature

La signature mise en œuvre est basée sur les normes : PADES, CAdES, XADES, JADES

5.4 Algorithmes utilisables pour la signature

5.4.1 Algorithme de condensation

Les algorithmes et mécanismes cryptographiques mis en œuvre sont conformes aux spécifications définies au niveau de référentiel de la DGSSI et de la norme ETSI TS 119 312 (v1.4.2 ou ultérieure). Le portail Adria DigiTrust utilise les algorithmes de condensation SHA-512/256

5.4.2 Algorithme de chiffrement

Les algorithmes et mécanismes cryptographiques mis en œuvre sont conformes aux spécifications définies au niveau de référentiel de la DGSSI et de la norme ETSI TS 119 312 (v1.4.2 ou ultérieure). Le portail Adria DigiTrust utilise l'algorithme de chiffrement RSA Encryption

5.5 Conditions pour déclarer valide le fichier signé

Un fichier signé est considéré comme valide lorsque les conditions suivantes sont remplies :

- Vérification positive de la signature électronique du signataire ;
- Vérification positive des droits du signataire en fonction des données transmises ;
- Validation de la réception du dossier de preuve associé à la transaction.

6. Dispositions juridiques

6.1 Droit applicable

La présente politique de signature (PS) est régie par la loi marocaine.

6.2 Tribunaux compétents

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre de la présente politique de signature seront soumis à la juridiction des tribunaux de Casablanca.