Politique de service de signature électronique simple

Version 1.3 | Diffusion : public |

OID n° 1.3.6.1.4.1.58553.1.7.1.1

Historique du document

Version	Date de version	Rédacteur(s)	Approbateur(s)	Modifications
1.0	16/03/2023	Fatimazahrae Jalal	Zouhair Hamdaoui	Création de la PC et DPC
1.1	03/01/2024	Fatimazahrae Jalal	Zouhair Hamdaoui	Ajouter les profils des certificats
1.2	23/09/2024	Fatimazahrae Jalal	Zouhair Hamdaoui	Renommage du document
1.3	27/02/2025	Fatimazahrae Jalal	Zouhair Hamdaoui	Nouvelle autorité de signature

Table des matières

1 Introduction

1.1 Présentation générale

Le présent document est la politique de signature du service de signature simple mis en œuvre par Damanesign. Lorsqu'une fonction de signature est mise à disposition d'utilisateurs, il est important que ces derniers 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 rendue disponible pour vérification.

L'objet de la présente politique de signature est justement de décrire :

- Les conditions dans lesquelles sont réalisées, traitées, conservées ces signatures électroniques
- Les conditions et contextes dans lesquels ces signatures électroniques seront ultérieurement consultables, utilisables et vérifiables.

Ce document est destiné aux :

- Signataires, pour leur permettre de comprendre la portée et le sens de l'engagement pris en signant
- Destinataires des documents signés, qui doivent non seulement s'assurer du sens de ces signatures, mais aussi d'avoir les moyens de s'assurer de leur validité (technique et juridique)

2 Politique de signature

2.1 Champ d'application

Le présent document, Politique de signature simple de la plate-forme Damanesign, s'applique aux transactions électroniques entre les partenaires de la société Damanesign et les clients de ces derniers, signataires des documents. Le service de signature simple de Damanesign permet aux signataires de réaliser une signature électronique à l'aide d'un scellement électronique garantissant l'intégrité des données signées

La signature électronique permet donc :

- De garantir l'intégrité des données signées,
- D'identifier celui qui l'appose
- De manifester son consentement aux obligations qui découlent de cet acte de signature

2.2 Identification du document

La présente P.C. est dénommé Politique et déclaration des pratiques de certification de service de signature simple. Elle est identifiée par son numéro d'identifiant d'objet, ainsi que par le nom, numéro de version, la date de mise à jour.

Le numéro d'OID de la présente P.C. est : 1.3.6.1.4.1.58553.1.7.1.1

2.3 Publication de document

Avant toute publication officielle, la Politique de Signature est validée par l'autorité de certification de Damanesign.

La présente Politique de Signature est :

- Disponible sur le service de signature et accessible par le signataire au moment de la signature électronique simple en ligne.

- Et publiée sur l'URL suivante : https://pki.damanesign.ma/

2.4 Processus de mise à jour

2.4.1 Circonstance rendant une mise à jour nécessaire

La mise à jour d'une Politique de Signature est une procédure impliquant tous les acteurs et faisant l'objet d'une démarche rigoureuse. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique ou combler des lacunes.
La présente politique est réexaminée lors de toute modification majeure.

2.4.2 Prise en compte des mises à jour

Avant toute publication officielle, la politique de signature est validée par l'autorité de certification Damanesign. Ce comité est placé sous la responsabilité du responsable des services de confiance Damanesign. Tous les remarques ou souhaits d'évolutions sur la présente politique sont à adresser au point de contact mentionné ci-après.

Damanesign	
Personne à contacter	IGC Information contact
Adresse postale	Adresse : 4 RUE OUED ZIZ 3EME ETAGE APPT 7 AGDAL, Rabat
Numéro de téléphone	+212 5 37 68 68 01
Adresse électronique	contact@damanesign.ma
Site internet :	https://damanesign.ma/

Ces remarques et souhaits d'évolution sont examinés par l'autorité de certification, qui engage si nécessaire le processus de mise à jour de la présente politique de signature. Toutes les versions des politiques de signature et leurs durées respectives de validité sont conservées par Damanesign et accessibles sur demande à l'adresse e-mail précédente.

2.4.3 Information des acteurs pour donner suite à une mise à jour

Lorsqu'une mise à jour a été planifiée, les informations relatives à cette évolution sont mises en ligne sur les lieux de publication. Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du point de contact susmentionné pour obtenir plus d'informations.
La publication d'une nouvelle version de la politique de signature consiste à archiver la version précédente et mettre en ligne dans le répertoire prévu à cet effet les éléments suivants :

- Document au format PDF,
- OID du document,
- Empreinte du document,
- Algorithme de hachage utilisé (condensat SHA-256 pour cette version),
- Date et heure exacte d'entrée en vigueur.

2.4.4 Entrée en vigueur de la nouvelle version et période de validité

Lorsqu'une nouvelle version de la Politique de Signature est mise en ligne, celle-ci est présentée et mise à disposition des signataires lors des transactions électroniques suivant la publication.

La date et l'heure exacte d'entrée en vigueur de la nouvelle Politique de Signature sont précisées sur le site de publication.
La nouvelle version de la Politique de Signature entre en vigueur dès sa publication sur le lieu de publication identifié au chapitre 2.3 et reste valide jusqu'à la publication d'une nouvelle version.

3 Acteurs et rôles

3.1 Listes des acteurs

3.1.1 Signataires

Les signataires des documents sont des personnes physiques clients du service de signature électronique de Damanesign, disposant de l'autorisation de l'entité qu'elles représentent le cas échéant pour signer des documents.
L'utilisateur a un niveau d'identification simple (l'identité du signataire est vérifiée par rapport aux informations déclaratif) avant de commencer le processus de signature.

3.1.2 Damanesign

Damanesign développe et opère le service de signature utilisé par les signataires.
Damanesign est responsable de la réalisation, de l'hébergement et de la maintenance du service de signature utilisé par les signataires.
Par ailleurs, Damanesign :

- Conserve le document électronique signé dans des conditions de sécurité permettant de garantir sa confidentialité et son intégrité dans le temps.

3.1.3 Destinataire

Les destinataires des documents signés électroniquement sont les clients eux-mêmes qui conservent ces documents dont la signature électronique matérialise leur consentement par rapport au contenu des documents.

3.2 Rôles et obligations du signataire

3.2.1 Environnement du signataire

L'opération de création de la signature doit être réalisée sur un équipement informatique (ordinateur, tablette, smartphone) connecté au réseau internet.
Le processus de signature ne dépend pas de l'équipement du client, par conséquent, aucun outil lié aux opérations de signature n'est à installer sur l'équipement informatique des signataires.
Le signataire doit toutefois s'assurer que cet équipement est protégé, notamment contre l'utilisation frauduleuse de son identité.
Il est donc nécessaire de protéger l'accès physique et technique à ce poste et aux informations confidentielles qui s'y trouvent.

3.2.2 Outil de signature utilisé

Les clients doivent contrôler les données qu'ils vont signer avant d'y apposer leur signature électronique.
Ils utilisent pour cela le service de signature mis à disposition par Damanesign et dont les différentes étapes du processus de signature les amènent à :

- Contrôler les éléments du document à signer,
- Accepter les Conditions Générales de service de signature,
- Accepter explicitement l'opération de signature.

3.2.3 Type de certificat utilisé

Aucun certificat électronique n'est délivré au signataire pour réaliser l'opération de signature.
La signature électronique réalisée par le signataire est de niveau « simple ».
Toutefois, un scellement électronique est réalisé par Damanesign pour toute signature

3.2.4 Protection du support du certificat

Non applicable. Aucun certificat n'est délivré au signataire.

3.2.5 Révocation du certificat

Non applicable. Aucun certificat n'est délivré au signataire.

3.3 Rôles et obligations de Damanesign

3.3.1 Environnement technique

Des mesures de sécurité permettant de protéger l'accès au service de signature sont mises en œuvre, notamment :

- La surveillance de l'accès physique et logique au système et la protection contre les intrusions,
- Une limitation d'accès et d'administration du service à un minimum de personnes de confiance, ayant les compétences nécessaires.

3.3.2 Outil de signature utilisé

Damanesign s'appuie sur son service de signature :

- Pour réaliser un scellement pour chaque signature électronique « simple » réalisée,

Type de certificat utilisé

Damanesign utilise un certificat de scellement délivré par l'Autorité de Certification de Damanesign conformément à la Politique de Certification identifiée par l'OID suivant : 1.3.6.1.4.1.58553.1.7.1.1

3.3.3 Révocation du certificat

Damanesign s'engage à demander la révocation de son certificat de scellement en cas de perte, de vol, de compromission ou de simple suspicion de compromission de sa clé privée et se conformer ainsi aux Conditions Générales d'Utilisation émises par l'Autorité de Certification de Damanesign.

3.3.4 Données de vérification de signature

Damanesign effectue une vérification de la qualité de la signature électronique préalablement à l'archivage du document signé.
Pour effectuer des vérifications des signatures/scellements électroniques, Damanesign utilise les données à sa disposition notamment les données publiques relatives au certificat de Damanesign, telles que les listes de révocation ou encore le certificat de l'Autorité de Certification ayant délivré son certificat.

En cas d'arrêt de la vérification de la signature, l'archivage électronique du document est temporairement suspendu mais n'impacte en rien la validité du document signé.
Damanesign s'assure de mettre en œuvre les procédures et dispositifs techniques permettant de lancer automatiquement une nouvelle vérification du document signé lorsque le service sera de nouveau disponible.

3.3.5 Protection des moyens

Damanesign s'assure de la mise en œuvre des moyens nécessaires à la protection des équipements fournissant le service de signature.
Les mesures prises concernent à la fois :

- La protection des accès physiques et logiques aux équipements aux seules personnes habilitées,
- La disponibilité du service,
- La surveillance et le suivi du service.

3.3.6 Journalisation

Damanesign s'assure de la conservation des traces relatives :

- A la circulation des échanges au sein des réseaux et des équipements informatiques,
- Au traitement des données échangées.

Damanesign s'assure que les preuves de traitement relatives à la vérification des signatures électroniques sont conservées pendant toute la durée règlementaire.

3.3.7 Reprise en cas d'interruption de service

Damanesign s'assure de la mise en œuvre des moyens nécessaires à la reprise d'activité en cas d'interruption de service d'un des composants nécessaires aux tâches dont il a la responsabilité.
Il s'assure en particulier que ces moyens font l'objet de tests à intervalles réguliers.

3.3.8 Assistance aux utilisateurs

Les signataires peuvent s'adresser à Damanesign pour toute information complémentaire ou pour signaler tout dysfonctionnement à l'adresse indiquée au chapitre 2.4.2.

3.4 Rôles et obligations des destinataires

3.4.1 Limitation des responsabilités de Damanesign

3.4.1.1 Mise à jour des informations utilisées

Certaines données, notamment les listes de révocations, ne peuvent être mises à jour en temps réel et il s'écoule plusieurs heures (24 au maximum) avant la publication de ces données par l'Autorité de Certification.

3.4.1.2 Contenu des documents signés

Les clients sont responsables du contenu des informations présentes dans le document signé.

4 Signature électronique et validation

4.1 Caractéristiques de l'équipement du signataire

L'équipement informatique du signataire (ordinateur, tablette, smartphone) fonctionne dans un environnement sous le contrôle du client.

Le processus de signature ne dépend pas de l'équipement du client.
Le certificat utilisé par Damanesign pour la signature du client est un certificat de cachet Damanesign.
Ce certificat est délivré par une Autorité de Certification : Damanesign Signature2 CA.

4.2 Données signées

Les données signées sont des documents convertis au format PDF préalablement à leur signature.

4.3 Opération de signature électronique

Au préalable du processus de signature électronique, le client accède à un ou plusieurs moyens d'authentification suivant le processus d'enrôlement en vigueur.
Pour la signature simple le niveau d'authentification est :
- Authentification de niveau 1 : l'identité du signataire est contrôlée sur la base d'informations déclaratives.

L'opération de signature électronique peut avoir lieu dans différents environnements, selon l'équipement dont dispose le signataire.
Les fonctionnalités minimales suivantes sont assurées par le service de signature, pour permettre au signataire d'avoir connaissance et conscience de l'action qu'il est sur le point d'effectuer :

– **Présentation des documents à signer.**

Les documents à signer sont présentés à l'écran en séquence. Le signataire doit volontairement dérouler l'ensemble du ou des documents à signer pour accéder à la phase de signature.

– **Présentation des attributs de la signature au signataire**

Les « attributs » de la signature suivants sont affichés au signataire pour lui permettre d'avoir connaissance des conditions dans lesquelles sa signature électronique sera réalisée et traitée :
- Lien vers la politique de signature,
- Lien vers les Conditions Générales du Service,

Le signataire doit confirmer qu'il a pris connaissance des Conditions Générales du Service et de la Politique de Signature du service de Damanesign.

– **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 déclencher le processus de signature des documents sélectionnés.
Le signataire doit volontairement dérouler l'ensemble du ou des documents à signer. Il ne peut donc en aucun cas contester que ces informations lui aient été présentées lors de la transaction dématérialisée.

– **Authentification**

Une authentification non rejouable par SMS peut être réalisée si elle a été spécifiée par l'expéditeur.
Le client reçoit alors un code à usage unique sur son mobile dont le numéro a été déclaré soit par lui-même soit par l'émetteur du document à signer.
Il est invité à saisir ce code à l'écran pour s'authentifier puis passer à l'étape de signature.

– **Signature**

Une fois signés, les documents sont mis à disposition du client et archivés.

4.4 Caractéristiques des signatures

Les signatures électroniques apposées par les clients sont des signatures PDF. La signature mise en œuvre est basée sur la norme ETSI EN 319 412-1.
Le certificat utilisé pour réaliser cette signature est le certificat de cachet de Damanesign.

4.5 Algorithmes utilisables pour la signature

4.5.1 Algorithme de condensation

Les algorithmes de condensation supportés sont SHA-256.

4.5.2 Algorithme de chiffrement

L'algorithme de chiffrement à utiliser est RSA Encryptions.

4.6 Vérification de la signature

La vérification de la signature est possible pour les destinataires et lecteurs des documents signés. Le cas échéant, elle porte sur :

- La vérification du respect de la norme de signature,
- La vérification du certificat de Damanesign et de tous les certificats de la chaîne de certification,
- Validité temporelle,
- Statut,
- Signature cryptographique,
- La vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue,
- La vérification de la signature électronique apposée sur le fichier en utilisant la clé publique de Damanesign contenue dans le certificat transmis,
- La vérification que le certificat utilisé au moment de la signature n'était pas dans une Liste de Certificats Révoqués. Cela concerne le certificat de cachet de Damanesign,
- La vérification de l'identifiant de la Politique de Signature référencée.

4.7 Gestion de la preuve

Pour conserver une trace de chaque signature, Damanesign constitue une preuve électronique signée, qui recense les éléments associés à la signature effectuée :

- Document signé par l'ensemble des clients,
- Certificat de cachet utilisé par Damanesign pour le compte des clients,
- L'ensemble des chaînes de certification mises en œuvre,

Cette preuve est disponible à tout moment pour les clients et les destinataires.

5 Profil des certificats et des LCR

5.1 Profils de certificats

Les certificats respectent le format décrit par la RFC 5280.

5.1.1 Certificats de l'AC Racine

Champ	Contenu

Version	2, indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	`sha256WithRSAEncryption`
Issuer	CN = Damanesign Root CA OU = 154609 O = Damanesign C = MA
Validity	30 ans
Subject	CN = Damanesign Root CA OU = 154609 O = Damanesign C = MA (certificat auto-signé)
Subject Public Key Info	RSA 4096 bits

Champ	Criticité	Général
Authority Key Identifier	N	Contient l'identifiant de clé de la clé publique de l'AC émettrice (champ *Subject Key Identifier* du certificat de l'AC émettrice). Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Subject Key Identifier	N	Identifiant de la clé du sujet (AC) Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Key Usage	O	`keyCertSign, CRLSign`
Basic Constraints	O	`CA: TRUE`
Certificate Policies	N	AnyPolicy (2.5.29.32.0) PKIX User Notice Qualifier (1.3.6.1.5.5.7.2.2) User Notice:The Damanesign Certification Authority. PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) CPS Pointer : http://pki.damanesign.ma/cps.html
CRL Distribution Points	N	http://pki.damanesign.ma/crl/ca_root_2024.crl

5.1.2 Certificats de l'AC « Damanesign Signature2 CA »

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	`sha256WithRSAEncryption`
Issuer	CN = Damanesign Root CA OU = 154609 O = Damanesign C = MA
Validity	30 ans
Subject	CN = Damanesign Signature2 CA OU = 154609 OI=NTRMA-154609 O = Damanesign C = MA
Subject Public Key Info	RSA 4096 bits

Champ	Criticité	Général
Authority Key Identifier	N	Contient l'identifiant de clé de la clé publique de l'AC émettrice (champ *Subject Key Identifier* du certificat de l'AC émettrice). Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Subject Key Identifier	N	Identifiant de la clé du sujet (AC) Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Key Usage	O	`keyCertSign, CRLSign`

Basic Constraints	O	CA:TRUE pathlen :0
Certificate Policies	N	AnyPolicy (2.5.29.32.0) PKIX User Notice Qualifier (1.3.6.1.5.5.7.2.2) User Notice:The Damanesign Certification Authority. PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) CPS Pointer: http://pki.damanesign.ma/cps.html
Subject Alternative Name **Issuer Alternative Name**	N	Non utilisée
CRL Distribution Points	N	http://pki.damanesign.ma/crl/ca_root_2024.crl
Authority Information Access	N	CA: http://pki.damanesign.ma/cert/ca_root_2024.crt

5.1.3 Certificats de signature simple (*1.3.6.1.4.1.58553.1.7.1.1*)

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	sha256WithRSAEncryption
Issuer	CN = Damanesign Signature2 CA OU = 154609 OI=NTRMA-154609 O = Damanesign C = MA
Validity	2 ans
Subject	CN=Damanesign signature service OU=154609 O=Damanesign C=MA
Subject Public Key Info	RSA 2048 bits

Champ	**Criticité**	Général
Authority Key Identifier	N	Contient l'identifiant de clé de la clé publique de l'AC émettrice (champ *Subject Key Identifier* du certificat de l'AC émettrice). Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Subject Key Identifier	N	Identifiant de la clé du sujet (AC) Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Key Usage	O	DigitalSignature
Extended Key usage	O	Document Signing
Basic Constraints	O	CA: FALSE
Certificate Policies	N	PolicyIdentifier: 1.3.6.1.4.1.58553.1.7.1.1 PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) CPS Pointer: https://pki.damanesign.ma/cps.html
Subject Alternative Name **Issuer Alternative Name**	N	Non utilisée
CRL Distribution Points	N	http://pki.damanesign.ma/crl/ca_sign2_2025.crl
Authority Information Access	N	CA: http://pki.damanesign.ma/cert/ca_sign2_2025.crt

5.2 Liste de Certificats Révoqués

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Signature	sha256WithRSAEncryption
Issuer	CN = Damanesign Signature2 CA OU = 154609

	O = Damanesign C = MA
thisUpdate	Date et heure UTC
nextUpdate	Date et heure UTC (7 jours de validité)
RevokedCertificates	Liste des numéros de série des certificats révoqués (Couples *UserCertificate-RevocationDate*)
Numéro de LCR	Entier
AuthorityKeyIdentifier	Identifiant de la clé de l'A.C.

6 Politique de confidentialité

6.1 Classification des informations

Les informations suivantes sont considérées comme confidentielles :

- Les clés privées du service de signature de Damanesign et des composantes du service de signature de Damanesign (clés privées des Autorités de Certification)
- Les informations personnelles des utilisateurs renseignées sur la plateforme de signature
- Les contrats et autres documents manipulés sur la plateforme de signature,
- Les preuves constituées et leur contenu,
- Les journaux de l'application de signature,
- Les procédures internes de gestion des preuves de Damanesign,
- Les rapports d'audit sur l'application de signature de Damanesign et sur les différents composants de l'infrastructure s'il en existe.

Les informations confidentielles sont protégées, et donc non accessibles publiquement.

6.2 Communication des informations à un tiers

On entend par tiers, tout organisme n'étant pas dans la chaîne de traitement des informations de Damanesign.
La diffusion des informations à un tiers ne peut intervenir que si Damanesign en reçoit la demande formelle et accepte la communication (notamment dans le cadre d'un litige et si un juge en formule une demande).

7 Dispositions juridiques

7.1 Droit applicable

La présente politique de signature est régie par le droit marocain.

7.2 Règlement des différends

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux de Rabat.

7.3 Propriété intellectuelle de l'infrastructure de création et de validation des signataires

Damanesign dispose des droits de propriété intellectuelle des services mis en œuvre dans le cadre de son service de signature.
Les signataires ne disposent d'aucun droit de propriété intellectuelle sur les documents signés.
Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent, par quelque procédé que ce soit, est strictement interdite et constitue une contrefaçon sanctionnée par le Code de la propriété intellectuelle.
Damanesign est propriétaire de la politique de signature.

7.4 Données personnelles

Les données personnelles au sens de la loi 09-08 marocain sur la protection des données considérées dans le cadre du service de signature simple de Damanesign sont :

- Le prénom et le nom du signataire,
- L'adresse email du signataire,
- Le numéro de téléphone du signataire.