Politique de service de cachet électronique simple

Version 1.1 | Diffusion : public | ***OID n 1.3.6.1.4.1.58553.1.8.1.10***

Historique du document

Version	Date de version	Rédacteur(s)	Approbateur(s)	Modifications
1.0	21/02/2025	Fatimazahrae Jalal	Zouhair Hamdaoui	Création de la politique
1.1	04/03/2025	Fatimazahrae Jalal	Zouhair Hamdaoui	Nouvelle autorité de cachet

Table des matières

1 Introduction 5
1.1 Présentation générale 5
2 Politique de signature 5
2.1 Champ d'application 5
2.2 Identification du document 6
2.3 Publication de document 6
2.4 Processus de mise à jour 6
2.4.1 Circonstance rendant une mise à jour nécessaire 6
2.4.2 Prise en compte des mises à jour 6
2.4.3 Information des acteurs pour donner suite à une mise à jour 7
2.4.4 Entrée en vigueur de la nouvelle version et période de validité 7
3 Acteurs et rôles 7
3.1 Listes des acteurs 7
3.1.1 Clients 7
3.1.2 Damanesign 7
3.1.3 Destinataire 7
3.2 Rôles et obligations du utilisateurs 8
3.2.1 Environnement des utilisateurs 8
3.2.2 Outil de cachet utilisé 8
3.2.3 Type de certificat utilisé 8
3.2.4 Protection du support du certificat 8
3.2.5 Révocation du certificat 8
3.3 Rôles et obligations de Damanesign 8
3.3.1 Environnement technique 8
3.3.2 Outil de cachet utilisé 8
3.3.3 Type de certificat utilisé 9
3.3.4 Révocation du certificat 9
3.3.5 Données de vérification du cachet électronique 9
3.3.6 Protection des moyens 9
3.3.7 Journalisation 9
3.3.8 Reprise en cas d'interruption de service 9
3.3.9 Assistance aux utilisateurs 9
3.4 Rôles et obligations des destinataires 10
3.4.1 Limitation des responsabilités de Damanesign 10
4 Cachet électronique et validation 10
4.1 Caractéristiques de l'équipement de l'utilisateur 10
4.2 Données sellées 10
4.3 Opération de cachet électronique 10
4.4 Caractéristiques des cachets électroniques 11
4.5 Algorithmes utilisables 11
4.5.1 Algorithme de condensation 11
4.5.2 Algorithme de chiffrement 11
4.6 Vérification du cachet 11
5 Profil des certificats et des LCR 11
5.1 Profils de certificats 11
5.1.1 Certificats de l'AC Racine 11
5.1.2 Certificats de l'AC « Damanesign Seal2 CA » 12
5.1.3 Certificats de cachet simple (1.3.6.1.4.1.58553.1.8.1.1) 13

5.2 Liste de Certificats Révoqués 13
6 Politique de confidentialité 14
6.1 Classification des informations 14
6.2 Communication des informations à un tiers 14
7 Dispositions juridiques 14
7.1 Droit applicable 14
7.2 Règlement des différends 14
7.3 Propriété intellectuelle de l'infrastructure de création et de validation des signataires 14
7.4 Données personnelles 15

1 Introduction

1.1 Présentation générale

Le cachet électronique apposé sur un ensemble de données permet de garantir leur origine et leur intégrité. Une politique de cachet électronique définit les conditions de recevabilité d'un document portant un ou plusieurs cachets électroniques dans le cadre d'échanges électroniques prédéfinis.

Le présent document, intitulé **« Politique de service de cachet électronique Damanesign »**, décrit ces conditions dans le cadre de l'utilisation d'un service de création de cachet électronique simple. Il s'adresse à toute entité souhaitant sécuriser et garantir la valeur juridique des documents et données produits dans le cadre de son activité, notamment en vue de leur stockage dans l'application de production. Ces conditions s'appliquent également à l'utilisation du service de vérification des cachets électroniques.

L'objet de cette politique est de préciser :

- Les conditions dans lesquelles les cachets électroniques sont apposés, traités et conservés.
- Les modalités et contextes dans lesquels ces cachets électroniques pourront être consultés, utilisés et vérifiés ultérieurement.

Ce document est destiné :

- Aux utilisateurs et aux entités cachetantes, afin de leur permettre de comprendre la portée et la valeur de l'apposition d'un cachet électronique.
- Aux destinataires des documents cachetés, qui doivent s'assurer de la signification du cachet et disposer des moyens nécessaires pour en vérifier la validité technique et juridique.

2 Politique de signature

2.1 Champ d'application

Le présent document, Politique de cachet électronique simple de la plate-forme Damanesign, régit l'utilisation du service de cachet électronique simple dans le cadre des transactions électroniques effectuées entre les partenaires de la société Damanesign et leurs clients, émetteurs des documents cachetés. Ce service permet aux organisations d'apposer un cachet électronique garantissant l'intégrité et l'authenticité des documents émis, renforçant ainsi la confiance numérique et la sécurité des échanges.

Grâce à son scellement électronique, le cachet électronique simple assure :

- **L'intégrité des documents**, en garantissant qu'aucune altération n'a été apportée après l'apposition du cachet ;
- **L'identification de l'entité émettrice**, en associant de manière unique le cachet à son propriétaire ;
- **L'authenticité et la fiabilité des documents**, en attestant de leur provenance et en renforçant leur valeur juridique.

En apportant une preuve incontestable de l'origine et de l'intégrité des documents, le cachet électronique simple constitue un élément clé de la dématérialisation sécurisée, répondant aux exigences réglementaires et facilitant les échanges numériques en toute confiance

2.2 Identification du document

La présente Politique est dénommée de service de cachet 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 : 1.3.6.1.4.1.58553.1.8.1.10

2.3 Publication de document

Avant toute publication officielle, la Politique de cachet électronique est soumise à la validation de l'autorité de certification de Damanesign.
La présente Politique de cachet électronique est :

- **Disponible sur le service de cachet**, et accessible aux clients lors de leur demande de cachet électronique simple en ligne.
- **Publiée à l'adresse 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 cachet 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 cachet 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. Toutes les versions des politiques de cachet 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 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 cachet 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 Clients

Les demandeurs du cachet sont des personnes physiques, clientes du service de cachet électronique de Damanesign, disposant, le cas échéant, de l'autorisation de l'entité qu'elles représentent pour apposer un cachet sur des documents. L'utilisateur doit avoir un niveau d'identification simple (l'identité est vérifiée par rapport aux informations déclaratives) avant de commencer le processus de cachetage.

3.1.2 Damanesign

Damanesign développe et opère le service de cachet utilisé par les clients.
Damanesign est responsable de la réalisation, de l'hébergement et de la maintenance du service de cachet.

3.1.3 Destinataire

Les destinataires des documents cachetés électroniquement sont les clients eux-mêmes, qui conservent ces documents dont le cachet électronique matérialise leur consentement par rapport au contenu des documents.

3.2 Rôles et obligations du utilisateurs

3.2.1 Environnement des utilisateurs

L'opération de création d'un cachet électronique doit être effectuée sur un équipement informatique (ordinateur, tablette, smartphone) disposant d'une connexion internet.
Le processus étant entièrement en ligne, il ne dépend pas du matériel du client. Par conséquent, aucun logiciel ou outil spécifique n'a besoin d'être installé sur l'équipement informatique de l'utilisateur.
Cependant, l'utilisateur doit veiller à la sécurité de son dispositif afin de prévenir toute utilisation frauduleuse de son identité. Il est donc essentiel de protéger l'accès physique et technique à son équipement, ainsi que les informations confidentielles qu'il contient.

3.2.2 Outil de cachet utilisé

Les clients doivent vérifier attentivement les données avant d'apposer le cachet électronique.

Pour ce faire, ils utilisent le service de cachet électronique mis à disposition par Damanesign, qui les guide à travers les différentes étapes du processus, notamment :

- **Contrôler les éléments du document à cacheter**,
- **Accepter les Conditions Générales du service de cachet**,
- **Valider explicitement l'opération de cachetage**.

3.2.3 Type de certificat utilisé

Aucun certificat électronique n'est attribué au client pour effectuer l'opération de cachetage.
Le cachet électronique apposé est de niveau **« simple »**, conformément aux exigences applicables.

3.2.4 Protection du support du certificat

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

3.2.5 Révocation du certificat

En cas de perte, de vol, de compromission ou de simple suspicion de compromission de la clé privée, le responsable de certificat de cachet doit demander la révocation dans les plus brefs délais du certificat.

3.3 Rôles et obligations de Damanesign

3.3.1 Environnement technique

Des mesures de sécurité permettant de protéger l'accès au service de cachet 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 cachet utilisé

Damanesign s'appuie sur son service de cachet :

- Pour réaliser un scellement simple dans chaque demande de cachet.

3.3.3 Type de certificat utilisé

Damanesign utilise un certificat de cachet à la volé délivré par l'Autorité de Certification de Damanesign conformément à la Politique de Certification identifiée par l'OID suivant : 1.3.6.1.4.1.58553.1.8.1.1

3.3.4 Révocation du certificat

Damanesign s'engage à demander la révocation de son certificat de cachet 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.

3.3.5 Données de vérification du cachet électronique

Damanesign effectue une vérification de la qualité du cachet électronique, pour mener à bien ces vérifications, Damanesign s'appuie sur les données disponibles, notamment les informations publiques relatives au certificat utilisé pour le cachetage, telles que les listes de révocation ou encore le certificat de l'Autorité de Certification ayant délivré ce certificat.

3.3.6 Protection des moyens

Damanesign s'assure de la mise en œuvre des moyens nécessaires à la protection des équipements fournissant le service de cachet simple.
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.

3.3.7 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 cachets électroniques sont conservées pendant toute la durée règlementaire.

3.3.8 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.

3.3.9 Assistance aux utilisateurs

Les clients 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 Cachet électronique et validation

4.1 Caractéristiques de l'équipement de l'utilisateur

L'équipement informatique de l'utilisateur (ordinateur, tablette, smartphone) fonctionne dans un environnement sous le contrôle du client.
Le processus de cachet simple ne dépend pas de l'équipement du client.
Le certificat utilisé par Damanesign pour le cachet du client est un certificat de cachet Damanesign.
Ce certificat est délivré par une Autorité de Certification : Damanesign Seal2 CA.

4.2 Données sellées

Les données sellées sont des documents convertis au format PDF.

4.3 Opération de cachet électronique

Avant l'application d'un cachet électronique, le client accède à un ou plusieurs moyens d'authentification conformément au processus d'enrôlement en vigueur.

Pour le cachet électronique simple, le niveau d'authentification requis est :

- **Authentification de niveau 1** : l'identité de l'émetteur est vérifiée sur la base d'informations déclaratives.

Le service de cachet électronique garantit les fonctionnalités minimales suivantes, permettant à l'émetteur d'avoir pleine connaissance et conscience de l'action qu'il s'apprête à réaliser :

- **Présentation des documents à cacheter** : L'utilisateur doit préparer le document à cacheté
- **Présentation des attributs du cachet électronique :** Les informations suivantes sont mises à disposition de l'émetteur afin qu'il puisse prendre connaissance des conditions dans lesquelles son cachet électronique sera appliqué et traité :
  - Lien vers la politique de cachet électronique,
  - Lien vers les Conditions Générales du Service.
  - L'émetteur doit confirmer qu'il a pris connaissance des Conditions Générales du Service ainsi que de la Politique de Cachet du service Damanesign.
- I**nteraction avec l'émetteur :** consentement explicite et possibilité d'arrêt du processus L'émetteur doit exprimer son consentement de manière explicite, volontaire et non ambiguë afin de déclencher l'application du cachet électronique sur les documents sélectionnés.
- **Authentification** : Une authentification non rejouable par clé API est requise.

- **Cachetage** : Une fois le cachet électronique appliqué, les documents sont mis à disposition du client.

4.4 Caractéristiques des cachets électroniques

Les cachets électroniques apposés par les clients sont au format **PDF** et conformes aux standards de signature électronique.

Le cachet électronique utilisé est mis en œuvre selon la norme **ETSI EN 319 412-1**.

4.5 Algorithmes utilisables

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 du cachet

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

- La vérification du respect de la norme de cachet,
- 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 du cachet 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 scellement 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 cachet référencée.

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`
Authority Information Access		`CA:` http://pki.damanesign.ma/cert/ca_root_2024.crt

5.1.2 Certificats de l'AC « Damanesign Seal2 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	29 ans
Subject	CN = Damanesign Seal2 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 cachet simple (1.3.6.1.4.1.58553.1.8.1.1)

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 Seal2 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: 1.3.6.1.4.1.58553.1.8.1.1 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_seal2_2025.crl
Authority Information Access	N	CA:http://pki.damanesign.ma/cert/ca_seal2_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 Seal2 CA OU = 154609 OI=NTRMA-154609 O = Damanesign C = MA
thisUpdate	Date et heure UTC

nextUpdate	Date et heure UTC (1 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 cachet de Damanesign et des composantes du service de cachet de Damanesign (clés privées des Autorités de Certification)
- Les informations personnelles des utilisateurs renseignées sur la plateforme de cachet
- Les contrats et autres documents manipulés sur la plateforme de cachet,
- Les preuves constituées et leur contenu,
- Les journaux de l'application du cachet,
- Les procédures internes de gestion des preuves de Damanesign,
- Les rapports d'audit sur l'application de cachet 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 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 cachet.
Les utilisateurs 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 service cachet.

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 cachet simple de Damanesign sont :

- Le prénom et le nom du client,
- L'adresse email du client,
- Le numéro de téléphone du client.
- Le nom de service su cachet du client