Article 1 : PREAMBULE

Damanesign met à la disposition du Porteur et/ou du Client ou de son Mandataire et de l'Utilisateur du Certificat, tels que définis ci-après, des services de certification électronique qualifiée. Toute utilisation des services proposés suppose la consultation et l'acceptation préalable et sans réserve des présentes Conditions Générales d'Utilisation.

Article 2 : DEFINITIONS & ACRONYMES

Les termes ci-dessous définis auront entre les parties la signification suivante :

« Authentification » : désigne le processus ayant pour but de vérifier l'identité dont se réclame une personne ou une machine.

« Autorité de Certification » ou « AC » : la personne morale qui, au sein d'un prestataire de service de certification électronique a en charge, au nom et sous la responsabilité de celui-ci, l'application d'une politique de certification et a qualité pour émettre des certificats électroniques au titre de cette politiquede certification.

« Autorité d'Enregistrement » ou « AE » : L'AE est utilisée pour la mise en œuvre des services d'enregistrement de demandes de certificats, service de personnalisation et de gestion des supports de bi-clés, de remise aux porteurs, de révocation de certificats, service de déblocage de support de Porteuret journalisation et d'audit.

« Bi-clé » : désigne le couple de clés composé d'une Clé Publique et d'une Clé Privée, généré dans le cadre d'une infrastructure de type PKI (solutions techniques basées sur la cryptographie à Clés Publiques).

« Cachet électronique » : Les données sous forme électronique, créées par une personne morale, qui sontjointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières.

« Certificat » : désigne le fichier électronique attestant qu'une Bi-clé appartient au Porteur identifié dans le certificat. Le Certificat est signé par l'Autorité de Certification.

« Client » : désigne l'Entité qui contracte avec Damanesign pour bénéficier d'un Certificat. Toute obligation applicable au Client s'applique également à son Représentant Légal, au Mandataire deCertification et au Porteur.

« Compromission » : désigne la divulgation ou suspicion de divulgation ou de perte d'informations confidentielles résultant de la violation d'une mesure de sécurité et conduisant à une possible perte de confidentialité et/ou d'intégrité des données considérées.

« Conditions Générales » ou « CGU » : désigne les présentes conditions générales d'utilisation.

« Données Confidentielles » : désigne la Clé du Certificat, le code de retrait et le code d'activation de la Clé, qui sont des données strictement personnelles au Porteur qui devront être impérativement gardéessecrètes.

« Entité » : désigne toute autorité administrative ou entreprise au sens le plus large, c'est-à-direégalement les personnes morales de droit privé de type associations.

« Infrastructure de Gestion des Clés » ou « IGC » : désigne l'ensemble de composantes, fonctions et procédures dédiées à la gestion des clés cryptographiques et de leurs certificats utilisés par des services de confiance.

« LCR » : désigne la liste des certificats révoqués.

« Mandataire de Certification » : désigne la personne désignée par le Représentant Légal du Client aux fins de recueillir les pièces des dossiers de demande de Certificats, de réaliser la reconnaissance en faceà face avec les Porteurs et d'effectuer les demandes de Révocation des Certificats.

« OID » : désigne le numéro d'identifiant objet désignant la Politique de Certification de l'Autorité de

Certification.

« Politique de Certification » ou « PC » : désigne l'ensemble des règles et exigences, identifiées par un OID, auxquelles Damanesign se conforme dans le cadre des présentes et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes.

« Porteur » : désigne la personne physique identifiée dans le Certificat et qui est le détenteur de la Clécorrespondante.

« Représentant Légal » : désigne le représentant légal du Client.

« Responsable du certificat cachet » ou « **RCC** » : La personne physique, dûment autorisée par le client, en charge des opérations de demande et de révocation de certificat pour le compte du client.

« Révocation » : désigne l'action qui a pour but l'extinction de la validité du Certificat. Un Certificat qui afait l'objet d'une Révocation est inscrit sur la LCR.

« Signature Électronique » : désigne l'usage d'un procédé fiable d'identification garantissant son lienavec l'acte auquel elle s'attache, conformément à la législation applicable.

« Utilisateur du Certificat » : désigne l'entité ou la personne physique qui reçoit un document ou unetransaction ayant utilisé un Certificat et qui s'y fie pour vérifier une valeur d'authentification ou une signature électronique provenant du Porteur.

Article 3 : OBJET

Les présentes conditions générales ont pour objet de préciser les conditions et les modalités d'achat des Certificats de Signature électronique qualifiée et/ou de Cachet électronique qualifié pour les professionnels proposés par l'Autorité de Certification (AC) Damanesign, et d'utilisation de tous les services de certification y afférents quelle que soit l'application pour laquelle un Certificat est utilisé. Elles définissent aussi les engagements et obligations respectifs des différents acteurs concernés. L'adhésion aux présentes conditions générales est effective dès la signature par le demandeur du certificat électronique du formulaire de la demande.

Article 4 : DATE EFFET ET DURÉE DU CONTRAT

Les présentes conditions générales d'utilisation sont opposables au représentant légal, au porteur et au mandataire de certification, le cas échéant, dès leur acceptation par ces derniers. Ils se portent forts du respect de ces conditions générales par l'utilisateur du certificat.

Le Contrat est conclu à compter de la réception et la validation effective du dossier du Client par Damanesign.

Le Contrat est conclu pour une durée correspondant à la durée de vie du Certificat qui est de deux ans à compter de la date de génération du certificat.

Paraphes

Le Contrat est constitué de :
- Le présent document ;
- Contrat PSCO-Client : Délivrance de Certificats Électroniques Qualifiés

Article 5 : DEMANDE DE CERTIFICATS ET RENOUVELLEMENT

5.1 Enregistrement des dossiers de demande de certificat :

Le dossier de demande de certificat déposé auprès de Damanesign

Pour la signature électronique qualifiée comprend les éléments suivants :
- Une demande de certificat écrite signée, et datée de moins de trois mois, par le futur porteur et, s'il est différent, par le représentant légal ou son délégataire ou le mandataire de certification ;
- Un document officiel d'identité en cours de validité du futur porteur comportant une photographie d'identité présenté à Damanesign qui en conserve une copie ;
- Les conditions générales d'utilisation signées et légalisées.
- Le porteur ou le représentant légal de l'entité ainsi que le mandataire peuvent faire une demande de certificat en téléchargeant le formulaire de demande de certificat depuis le site Internet de Damanesign : https://guichet.damanesign.ma
- Ils envoient ensuite les pièces justificatives nécessaires en se présentant directement à l'Autorité d'Enregistrement de Damanesign
- Les pièces justificatives à joindre lors d'une demande initiale de certificat sont précisées sur le formulaire d'abonnement
- Lettre de demande du dispositif de signature électronique légalisée, signée et cachetée par le représentant légale de l'entité et qui contient le domaine d'application, c'est-à-dire de préciser dans quel cadre sera utilisé ledit dispositif de signature électronique.

Pour un certificat qualifié de cachet électronique, sous la responsabilité d'une personne morale, le dossier d'enregistrement doit au moins comprendre :
- Une demande de certificat manuscrite datée de moins de 3 mois et signée par un représentant autorisé de la personne morale, comprenant l'ensemble des éléments nécessaires à la délivrance du certificat ;
- Les conditions générales d'utilisation, dans leur version en vigueur, datées et signées ;

5.2 Pour une entreprise :
- Registre du commerce contenant un numéro d'immatriculation officiel modèle J7;
- Attestation d'inscription à la taxe professionnelle ;
- Une fiche de poste et une attestation de travail qui démontrent la qualité du demandeur de certificat signée et cachetée
- Une habilitation du responsable du certificat cachet (RCC) à demander des certificats pour le compte d'un service de l'entité, signée par le représentant légal ou une personne autorisée.
- Si le responsable du certificat cachet n'est pas le représentant légal de l'entité, l'AE vérifie l'habilitation du responsable du certificat pour réaliser cette demande de certificat par le contrôle d'un document signé par le Représentant Légal ou une personne autorisée de l'entité pour laquelle est établie le certificat.

N. B : Le responsable du certificat cachet ne peut être qu'une personne physique. Il est responsable de l'utilisation du certificat (et de la clé privée associée) dans lequel est identifié le service applicatif, et également l'entité pour le compte de laquelle il utilise le certificat et avec laquelle il entretient un lien contractuel/hiérarchique/réglementaire. Le certificat est rattaché au service applicatif et non au responsable du certificat cachet.

En cas de changement du responsable de certificat cachet, l'entité doit le signaler à l'AC et lui désigner un successeur. L'AC révoque les certificats pour lesquels il n'y a plus de responsable du certificat cachet explicitement identifié.
- Si le responsable du certificat cachet n'est pas le représentant légale de la société, un mandat du représentant légale l'autorisent à réaliser la demande.
- La vérification des informations du responsable du certificat cachet et du service applicatif ainsi que de leur entité de rattachement afin de garantir la validité des informations contenues dans le certificat.
- L'enregistrement du futur responsable du certificat cachet nécessite la validation de l'identité "personne morale" de l'entité de rattachement du futur responsable du certificat, de l'identité "personne physique" du futur responsable du certificat cachet, de son habilitation à être responsable du certificat cachet pour le service considéré et pour l'entité considérée.
- Pièce d'identité officielle du responsable du certificat cachet qui sera valide au moment de l'enregistrement.
- Lettre de demande du dispositif de cachet électronique légalisée, signée et cachetée par le représentant légale de l'entité et qui contient le domaine d'application, c'est-à-dire de mentionner dans quel cadre sera utilisé ledit dispositif de cachet électronique, et de préciser pour quel département dans le cas où l'entreprise contient plusieurs départements ;

Pour une personne morale de droit public (administration, établissement public ...) :
- Un document de délégation de pouvoir valide au moment de l'enregistrement, portant délégation de l'autorité responsable de la structure administrative ou de l'établissement public. L'enregistrement d'un titulaire (personne physique ou morale) de certificat peut se faire soit directementauprès de l'autorité d'enregistrement, soit via un mandataire de certification de l'entité cliente dont il dépend.

En cas de recours à un mandataire, celui-ci doit être formellement désigné par un représentant légal de l'entité concernée et doit être enregistré par l'autorité d'enregistrement.

Le dossier d'enregistrement d'un mandataire doit au moins comprendre :
- Une copie de la carte nationale d'identité électronique en cours de validité du mandataire ou tout document valide justifiant son identité (comportant une photo d'identité et délivré par une autorité compétente) ;
- Un mandat daté de moins de 3 mois co-signé par un représentant légal de l'entité désignant le mandataire et par le mandataire pour acceptation ;
- Une attestation d'engagement datée de moins de 3 mois et signée par le mandataire, qui atteste de l'engament du mandataire auprès de l'AC à respecter ses obligations.
- Pour l'entité cliente :
  - [Entreprise] Fournir le document de registre de commerce modèle J7 et l'attestation d'inscription à la taxe professionnelle ;
  - [Administration] Un document de délégation de pouvoir valide au moment de l'enregistrement, portant délégation de l'autorité responsable de la structure administrative.

Le dossier d'enregistrement d'un (futur) titulaire via un mandataire, doit au moins comprendre :
- Une demande de certificat, datée de moins de 3 mois, indiquant l'identité du titulaire, cosigné par le mandataire et le titulaire (ou le représentant légal de l'entité titulaire dans le cas d'une personne morale) ;
- Une copie de la carte nationale d'identité électronique en cours de validité du futur titulaire (ou le représentant légal de l'entité titulaire dans le

Paraphes

cas d'une personne morale) ou tout document valide justifiant son identité délivré (comportant une photo d'identité et délivré par une autorité compétente) ;
- Les conditions générales d'utilisation signées par le titulaire (ou le représentant légal de l'entité titulaire dans le cas d'une personne morale) ;
- L'adresse postale et / ou l'adresse mail permettant à l'autorité de certification de contacter le titulaire (ou le représentant légal de l'entité titulaire dans le cas d'une personne morale).

La vérification de l'identité du mandataire est réalisée conformément aux dispositions relatives à lavérification de l'identité au vu de la délivrance d'un certificat qualifié.

5.3 Vérification de la demande :

L'Autorité d'Enregistrement réalise les opérations suivantes :
- Vérifie et valide l'identité du futur porteur ;
- Vérifie la cohérence des justificatifs présentés ;
- S'assure que le futur porteur a pris connaissance des modalités applicables pour l'utilisation du certificat déterminées par les présentes.

L'identité du porteur ou du responsable de certificats est vérifiée au travers de la vérification de documents officiels d'identité effectuée lors d'un face-à-face.

Les informations concernant la structure à laquelle le porteur est rattaché font l'objet de vérification lorsde l'enregistrement (existence, validité, …)

5.4 Rejet de la demande :

En cas de pièces manquantes et après relance quant à la communication de ces pièces, dans un délai de 2 mois, l'Autorité d'Enregistrement se réserve le droit de rejeter la demande de certificat. Il en informe leporteur, le mandataire de certification ou le représentant légal de l'entité par mail et lettre recommandéeen justifiant la raison du rejet. En cas de résiliation anticipée, pour quelque cause que ce soit, de la Commande, le prix payé par le Client à la souscription reste acquis à Damanesign.

5.5 Délivrance du certificat :

Après authentification de l'origine et vérification de l'intégrité de la demande provenant de l'Autorité d'Enregistrement, Damanesign génère le certificat, la bi-clé du porteur, son dispositif de signature et les codes d'activation.

Selon le cas, le porteur ou le représentant légale reçoit dans le cas d'une personne morale à son domicile personnel un courrier contenant le code d'activation (PIN) qui l'invite à retirer son supportcryptographique auprès de Damanesign sous présentation d'une pièce d'identité originale. Le cas échéant le mandataire reçoit une invitation par courriel pour récupérer le support cryptographique.

L'autorité de certification fait signer une attestation de délivrance (Document Papier) par le porteur ou le mandataire. Par ailleurs, le mandataire ne peut avoir accès à des moyens qui lui permettraient d'activeret d'utiliser la clé privée associée à la clé publique contenue dans le certificat délivré au titulaire.

En cas d'absence de réponse, l'autorité de certification rappelle le porteur par l'envoie d'une lettre recommandée après 3 mois d'absence du porteur, suite à cela le certificat est révoqué par cette autorité.

5.6 Acceptation du certificat :

Le porteur, le mandataire ou le représentant légale doit vérifier que les informations qui sont inscrites surle certificat sont conformes à ses données personnelles préalablement à son utilisation suite à cela il signel'attestation d'acceptation du certificat pour prendre possession du support cryptographique.

Vérification que le certificat est bien associé à la clé privée correspondante et acceptation explicite du certificat par le porteur.

Le porteur dispose d'un délai de 15 jours pour signer le formulaire d'acceptation de certificat dans le cas échéant le certificat sera révoqué.

L'attestation d'acceptation est signée à l'aide de la signature électronique par la clé cryptographique.

L'attestation d'acceptation du certificat est renvoyée à l'AC qui la conserve.

5.7 Assistance :

Afin d'accompagner le client, une assistance téléphonique ou hot line est mise à sa disposition au 05 3768 68 01 de 08h30 à 13h00 et de 14h00 à 18h00 les jours ouvrés.

5.8 Renouvellement :

La cause principale de la délivrance d'un nouveau certificat et de la bi-clé correspondante est la fin devalidité du certificat ou une révocation.

La durée de validité des certificats qualifiés Damanesign pour signature électronique est de deux (2) ans. Damanesign informera le client par courriel deux mois avant la date d'expiration de la validité de soncertificat, de l'échéance de celui-ci et l'invitera à le renouveler.

Les bi-clés doivent être en effet périodiquement renouvelées afin de minimiser les risques d'attaque cryptographique. Un renouvellement peut être aussi réalisé de manière anticipée, par suite d'un événement ou un incident déclaré par le porteur ou le responsable de certificats, les plus fréquents étantla perte, le vol ou le dysfonctionnement du support cryptographique. Dans ce cas le renouvellement consiste pour le porteur ou le responsable de certificats à refaire une demande initiale. Une modificationdes informations contenues dans le certificat entraîne également la délivrance d'un nouveau certificat (avec renouvellement de la bi-clé). En cas de déqualification du support physique du Certificat pendant sa période de validité initiale, notamment due à un changement de PC ou de réglementation, le renouvellement du Certificat pourra être effectué uniquement sur un nouveau support physique. Le renouvellement d'un Certificat en fin de validité implique le renvoi des pièces justificatives qui ne sont plus valables ou qui ont subi des modifications, conformément au Contrat d'abonnement. Tout Porteur est averti par message électronique de l'arrivée à expiration de son Certificat. S'il souhaite le renouveler,il formule une demande de renouvellement avant la date d'expiration en téléchargeant des formulaires depuis le Guichet Electronique Damanesign et en les remplissant. La délivrance d'un nouveau certificat est réalisée de manière identique au processus de délivrance initiale mais le client va devoir payer pour lecertificat et garde le même support cryptographique sauf en cas de dysfonctionnement de ce dernier.

Vous allez recevoir un autre pin par la suite dédié à la création d'un nouveau certificat.

5.9 Demande de renouvellement via un formulaire pour obtenir un certificat relatif à la signature électronique qualifiée et au cachet électronique qualifié :

Le renouvellement du certificat constitue une procédure allégée de demande de certificat. Prenez bien en compte les conditions générales d'utilisation.

Le Porteur, le représentant légal ou le mandataire doit télécharger et remplir les formulaires de renouvellement disponibles dans notre Site web Damanesign, pour la vérification des données du nouveau certificat.

Paraphes

Ensuite le porteur/Mandataire doit déposer chez Damanesign toutes les pièces administratives nécessaires ainsi que le support cryptographique pour le renouvellement.

Le porteur reçoit à son domicile personnel un courrier contenant le code d'activation (PIN) qui l'invite à retirer son support cryptographique auprès du local de Damanesign en présentant une pièce d'identité comportant une photographie.

La délivrance d'un nouveau certificat est réalisée de manière identique au processus de délivrance initiale.

Le support cryptographique contenant le certificat est remis en mains propres au porteur ou au mandataire lors d'un face-à- face au niveau du bureau de distribution sur présentation d'une pièce d'identité originale.

Le porteur ou le mandataire doit vérifier que les informations qui sont inscrites sur le certificat sont

Conformes à ses données personnelles suite à cela, il signe l'attestation d'acceptation du certificat.

5.10 Pièces à fournir pour une demande de renouvellement de certificat :

Certificat qualifié de signature électronique

- Justificatifs d'identité des personnes :
  - Les formulaires d'abonnement dûment datés de moins de trois mois et signés par les personnes nommément désignées incluant le formulaire de demande de certificat électronique qui doit contenir l'adresse professionnelle, le numéro de téléphone, l'adressee-mail professionnelle du futur porteur. Le formulaire doit comporter également le cachetde l'organisme ;
  - Une (1) copie certifiée conforme de la CIN (Carte d'Identité Nationale) ou passeport du bénéficiaire valide ou bien carte de séjour valide pour les étrangers résidents ;
  - Bon de commande signé et cacheté par l'organisme ;
  - Un justificatif de paiement (reçu de paiement, chèque) ;
  - Une enveloppe par porteur contenant le formulaire des réponses aux questions secrètes fermée et cachetée par l'organisme ;
  - Les conditions générales qui doivent être co-signées et légalisées par le mandataire et leporteur avec mention d'approbation du mandataire et cachetées par le cachet de l'organisme ;
  - Si nécessaire, Procuration signée et cachetée, conférant mandat à une personne physiquepour la gestion des certificats de la personne morale.
  - Contrat PSCO – Client signé et légalisé
- Justificatifs d'identité de l'organisme :

  - **Société de toute forme juridique - Personne Moral :**
  - Attestation récente qui contient le Numéro ICE, à savoir l'attestation de l'inscription à la taxe professionnelle, (et/ou) le Bulletin De Notification Du N° D'identification Fiscale ou une copie récente et certifiée conforme de l'un des dits documents ;
  - Copie certifiée conforme actualisé de l'extrait du registre de commerce modèle J7 ;
  - Copie certifiée conforme d'un document (s) justifiant la qualité de la personne signataire en tant que représentant légal de l'organisme (délégation de pouvoir, Procès-Verbal de nomination, Statut, …) actualisée ;

  - **Ministère / Établissement public :**
  - Copie certifiée conforme d'un document (s) justifiant la qualité de la personne signataire en tant que représentant légal de l'organisme actualisée ;

  - **Association :**
  - Copie certifiée conforme des Statuts revêtus de la signature légalisée du président ;
  - Copie certifiée conforme du procès-verbal légalisé de l'assemblée générale constitutive ou modificative ;
  - Liste timbrée et légalisée des membres du bureau ;
  - Copie certifiée conforme du récépissé de dépôt ;

  - **Pour les entreprises individuelles et les fonctions réglementées (commerçant, professionslibérales...) - Personne Physique :**

Attestation récente qui contient le Numéro ICE, à savoir :

  - L'attestation de l'inscription à la taxe professionnelle, (et/ou)
  - Le Bulletin De Notification Du N° D'identification Fiscale ou une copie récente et certifiée conforme de l'un des dits documents.

Certificat qualifié de cachet électronique :

- Justificatifs d'identité des personnes :
  - Une demande de certificat manuscrite datée de moins de 3 mois et signée par un représentant autorisé de la personne morale, comprenant l'ensemble des éléments nécessaires à la délivrance du certificat à savoir : Nom, Prénom, l'adresse professionnelle, le numéro de téléphone, l'adresse e-mail professionnelle du représentant.
  - Les conditions générales d'utilisation, dans leur version en vigueur, datées et signées.
- Pour une entreprise :
  - Numéro d'immatriculation officiel de l'entité titulaire du certificat (ICE, numéro d'inscription au registre du commerce, …)
  - Dénomination officielle ou raison sociale de l'entité titulaire du certificat telle qu'enregistrée auprès des autorités compétentes et telle que déclarée auprès de l'Autorité nationale ;
  - Nom du pays d'activité de l'entité titulaire du certificat
  - Tout document attestant de la qualité du demandeur de certificat
- Pour une personne morale de droit public (administration, établissement public ...) :
  - Un document, valide au moment de l'enregistrement, portant délégation de l'autorité responsable de la structure administrative ou de l'établissement public

5.11 Procédure de procuration dans le cas où le mandataire de certification n'est pas le représentant légal :

Le mandataire de certification a pour mission de :

- Demander des certificats électroniques Damanesign ;
- Signer les contrats y correspondants, au nom et pour le compte de l'organisme ;
- Accomplir tous actes nécessaires à l'émission, la gestion et la révocation de tous certificats électroniques qui auront été émis à sa demande et sous sa responsabilité.

Le mandataire de certification désigné s'engage à respecter et à faire respecter l'ensemble des dispositions contractuelles et les procédures Damanesign.

Paraphes

La procuration prend effet à compter de la date de sa signature par le représentant légal de l'organismeet son mandataire et sera valable jusqu'à l'expiration du dernier certificat en cours de validité détenu par l'organisme et demandé par le mandataire, sauf substitution du mandataire de certification par une autre personne dument signalée par le représentant légal et portée à la connaissance de Damanesign.

A cet effet, le représentant légal, s'engage à signaler tout changement concernant le mandataire decertification ou concernant l'organisme, dans les plus brefs délais, et fournir les pièces justificatives nécessaires.

5.12 Modification du certificat :

En cas de modification des informations contenues dans le Certificat, le Certificat devra être révoqué et une nouvelle demande de Certificat devra être faite, selon les modalités définies par les CGU. Damanesign ne procède à aucune modification de Certificat.

5.13 Déblocage du certificat :

En cas de blocage du support cryptographique, notamment dû à une erreur de code PIN, tout déblocage devra être fait par l'intermédiaire de Damanesign.

Toute tentative de déblocage effectuée directement par l'utilisateur, pourrait donner lieu à un dysfonctionnement du support physique du Certificat à la charge du Client.

Article 6 : CONDITIONS D'USAGE DES CERTIFICATS ET LIMITES

6.1 Pour la délivrance de certificats électroniques qualifiés pour la signature électronique :

L'usage est la signature électronique de données par le porteur du certificat (signataire). Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

L'AC fournit le support matériel au porteur, directement, et s'assure que La préparation des dispositifs de création de signature est contrôlée de façon sécurisée par le prestataire de service et que les supports matériels sont stockés et distribués de façon sécurisée.

L'utilisation de la Clé du Porteur et du Certificat doit rester strictement limitée au service de Signature électronique.

En tout état de cause, le Client est pleinement responsable vis-à-vis de Damanesign de l'utilisation du Certificat faite par le Porteur.

6.2 Pour la délivrance de certificats électroniques qualifiés pour le cachet électronique :

L'usage consiste en l'utilisation d'un cachet électronique d'un document par le représentant légale de la personne morale. Un tel cachet électronique apporte, outre l'authenticité et l'intégrité des données ainsicachetées, la manifestation du consentement du représentant légale de la personne morale quant au contenu de ces données.

L'AC fournit le support matériel au représentant légale, directement, et s'assure que La préparation des dispositifs de création de cachet est contrôlée de façon sécurisée par le prestataire de service et que les supports matériels sont stockés et distribués de façon sécurisée.

L'utilisation de la Clé du représentant légale et du Certificat doit rester strictement limitée au service de Cachet électronique.

En tout état de cause, le client est pleinement responsable vis-à-vis de Damanesign de l'utilisation du certificat faite par le représentant légal.

Article 7 : REVOCATION DU CERTIFICAT

La révocation d'un certificat consiste à annuler et à résilier le certificat avant la date de son expiration effective pour qu'il ne soit plus utilisable et qu'il n'engage plus votre responsabilité en casd'utilisation. Après révocation, le certificat n'est plus utilisable et change de statut. Il passe de valide à révoquer.

La révocation peut être effectuée à la suite d'un incident couvrant en particulier l'un des cas suivants :

- Incident sur le support cryptographique le rendant indisponible (Perte ou Vol de votre certificat)
- Incident sur le support cryptographique le rendant inutilisable (dégradation / panne…)
- Changement de fonction du porteur au sein de son organisation
- Le décès du porteur ou la cessation d'activité de l'entité à qui il appartient
- Non-respect du porteur des modalités applicables d'utilisation du certificat

Le service de révocation en ligne est accessible 24h/24h et 7j/7j sur le guichet électronique de Damanesign, et l'entité chargée du traitement est joignable de 8h30 à 18h et 7J/7J.

7.1 La demande de révocation peut émaner des personnes suivantes :

- Le porteur du certificat
- Le mandataire du certificat d'un porteur
- Le représentant légal
- Le responsable du certificat cachet (RCC)
- Une personne autorisée (L'AC, L'AE)

7.2 Le porteur du certificat dispose de quatre moyens pour révoquer le certificat :

1ère méthode : Révocation en ligne du certificat Damanesign

- Dans votre navigateur accédez à la page : « https://guichet.damanesign.ma » pour effectuer la révocation du certificat en ligne ;
- Accédez au menu "Services" ensuite veuillez choisir "Révocation du Certificat" ;
- Renseigner l'adresse courriel et le numéro de CIN du porteur de certificat ou RCC.
- Cette étape est protégée par un mécanisme CAPTCHA qui permet de réduire les risques associés aux attaques par des automates, cliquer sur « Continuer » ;
- Saisir les réponses aux questions secrètes (se référer à la copie du formulaire des réponses aux questions secrètes) ;
- Entrer le code OTP reçu par SMS ;
- Si vous avez plusieurs certificats, Cliquer sur le numéro (N°) correspondant au certificat à révoquer, s'assurer bien que les informations affichées correspondent au certificat que vous souhaitez révoquer ;
- Choisir la raison de la révocation et renseigner un commentaire puis cliquer sur le bouton
- « Révocation du certificat » pour terminer l'opération de révocation ;
- Quand l'opération de révocation est réalisée, le porteur ou RCC sera notifié par un courriel de confirmation

2éme méthode : Révocation du certificat via un appel téléphonique

- Le porteur du certificat ou RCC a la possibilité de contacter le département de Révocation de Damanesign sur le numéro suivant +212 5 37 68 68 01 qui est joignable et disponible de 8h30 à 18h et 7j/7j ;

Paraphes

- Dans le cadre d'une démarche de sécurité, le porteur du certificat ou RCC va devoir répondre à une série de questions qui seront posées par l'équipe Damanesign afin de l'authentifier et de s'assurer de son identité ;
- Entrer le code OTP reçu par SMS ;
- En dernier lieu, le porteur du certificat ou RCC va devoir préciser le certificat à révoquer et communiquer la raison de révocation du certificat ;
- Quand l'opération de révocation est réalisée, le porteur ou RCC sera notifié par un courriel de confirmation

3éme méthode : Révocation du certificat en ligne, sur la base de la pièce d'identité et la reconnaissance faciale

Dans le cas d'oubli des réponses aux questions secrètes, le Porteur ou RCC, peut utiliser sa pièce d'identité pour d'authentifier et pouvoir révoquer son certificat en ligne, grâce au service de l'identité numérique de la D.G.S.N. (Direction générale de la Sûreté nationale) https://www.identitenumerique.ma

- Dans votre navigateur accédez à la page : « https://guichet.damanesign.ma » pour effectuer la révocation du certificat en ligne ;
- Accédez au menu "Services" ensuite veuillez choisir "Révocation du Certificat" ;
- Renseignez l'adresse courriel et le numéro de CIN du porteur de certificat ou RCC ;
- Cette étape est protégée par un mécanisme CAPTCHA qui permet de réduire les risques associés aux attaques par des automates, cliquer sur « Continuer » ;
- Cliquez sur le lien « Questions secrètes oubliées ? » ;
- Le porteur ou RCC sera redirigé vers le Portail Identité Numérique Maroc, https://www.identitenumerique.ma de la DGSN (Direction générale de la Sûreté nationale).
- Une fois l'identification terminé sur la base de la pièce d'identité et la reconnaissance faciale
- Le porteur ou RCC est redirigé à nouveau sur https://guichet.damanesign.ma
- Le guichet vérifie l'identité renvoyé par le portail Identité Numérique Maroc et les informations (Nom, prénom, CIN, Date de validité) du porteur ou RCC
- Entrer le code OTP reçu par SMS ;
- Si vous avez plusieurs certificats, Cliquer sur le numéro (N°) correspondant au certificat à révoquer, s'assurer bien que les informations affichées correspondent au certificat que vous souhaitez révoquer ;
- Choisir la raison de la révocation et renseigner un commentaire puis cliquer sur le bouton « Révocation du certificat » pour terminer l'opération de révocation.
- Quand l'opération de révocation est réalisée, le porteur ou RCC sera notifié par un courriel de confirmation.

4éme méthode : Prise de rendez-vous aux bureaux de Damanesign pour la révocation du certificat en face à face

Dans le cas d'oubli des réponses aux questions secrétées, le Porteur ou RCC a la possibilité de se déplacer aux bureaux de Damanesign, ouvert 8h30 à 18h et 7j/7j.

- Le porteur du certificat ou RCC contact le département de Révocation de Damanesign au numéro suivant +212 5 37 68 68 01 qui est joignable et disponible de 8h30 à 18h et 7j/7j ;
- Le chargé de Révocation invite le porteur ou RCC à se présenter dans les bureaux de Damanesign dans la journée ou lendemain en respectant le délai de révocation de moins de 24 heures ;
- Le chargé de Révocation vérifie la pièce d'identité du porteur ou RCC ;
- Le chargé de Révocation, demande au porteur ou RCC de remplir et signer, le formulaire de révocation ;
- Le chargé de Révocation procède à la révocation de certificat via le backoffice du guichet électronique ;
- Quand l'opération de révocation est réalisée, le RCC sera notifié par un courriel de confirmation

7.3 Modalités de révocation d'un certificat par le mandataire du certificat d'un porteur :

Le mandataire dispose de la possibilité de révoquer le certificat d'un porteur par courrier recommandé :

Il est invité à envoyer la demande de révocation de certificat signée et cachetée par courrier à l'adresse suivante :

Damanesign, Service Enregistrement et Relation Clients

Direction développement

4 RUE OUED ZIZ 3EME ETAG E APPT 7 AGDAL, 10080, Rabat.

Le service de révocation Damanesign procède à vérifier l'identité du Mandataire et du certificat à révoquer en rappelant le mandataire sur le n° de téléphone de révocation renseigné sur le formulaire d'enregistrement afin de l'authentifier.

Un courriel de confirmation est envoyé au mandataire et au porteur notifiant la révocation effective du certificat.

7.4 Modalités de révocation d'un certificat par le représentant légal :

Les demandeurs de certificats électroniques qualifiés ont la possibilité de faire des demandes de révocation dans le futur en remplissant le formulaire de demande de révocation et en suivant les modalités de révocation du certificat mentionnées ci-dessus.

Pour le service du cachet électronique qualifié, la révocation d'un certificat peut être aussi demandé par le Responsable du certificat cachet "RCC" ou le représentant légal de l'entité pour laquelle est établie le certificat.

La demande doit être réalisée par courrier papier. Il est invité à envoyer la demande de révocation de certificat signée et cachetée par courrier recommandé à l'adresse suivante :

Damanesign, Service Enregistrement et Relation Clients

Direction développement

4 RUE OUED ZIZ 3EME ETAG E APPT 7 AGDAL, 10080, Rabat.

La demande doit comporter :

- Le nom et le prénom du demandeur de la révocation ;
- L'adresse courriel du demandeur ;
- Une copie certifiée conforme de la pièce d'identité du demandeur ;
- Le nom du service et de l'entité tels qu'ils apparaissent dans le certificat ;
- La signature du demandeur.

En effet, il suffit juste de remplir le formulaire de révocation mis à disposition sur le site web du guichet électronique Damanesign via le lien suivant https://guichet.damanesign.ma/downloads/forms

L'AE vérifie les éléments de la demande et l'identité du demandeur en le contactant grâce aux informations recueillies au moment de la demande du

Paraphes

certificat (téléphone, email…)

Un courriel de confirmation est envoyé au représentant légal ou bien au responsable du certificat cachet notifiant la révocation effective du certificat.

Pour le service de signature électronique qualifiée, la révocation d'un certificat peut être aussi demandé par le représentant légal de l'entité pour laquelle est établie le certificat.

La demande doit être réalisée par courrier papier. Il est invité à envoyer la demande de révocation de certificat signée et cachetée par courrier recommandé à l'adresse suivante :

Damanesign, Service Enregistrement et Relation Clients

Direction développement

4 RUE OUED ZIZ 3EME ETAG E APPT 7 AGDAL, 10080, Rabat.

La demande doit comporter :

- Le nom et le prénom du demandeur de la révocation ;
- L'adresse courriel du demandeur ;
- Une copie certifiée conforme de la pièce d'identité du demandeur ;
- Le nom de l'entité tels qu'il apparait dans le certificat ;
- La signature du demandeur.

En effet, il suffit juste de remplir le formulaire de révocation mis à disposition sur le site web du guichet électronique Damanesign via le lien suivant https://guichet.damanesign.ma/downloads/forms

L'AE vérifie les éléments de la demande et l'identité du demandeur en le contactant grâce aux informations recueillies au moment de la demande du certificat (téléphone, email…).

Un courriel de confirmation est envoyé au représentant légal notifiant la révocation effective du certificat.

Article 8 : OBLIGATIONS DE DAMANESIGN

Damanesign attribue à sa PC un OID qui est porté dans les Certificats correspondants qu'elle s'engage àfaire évoluer en cas d'évolution de sa PC.

Elle s'engage au contrôle par l'Autorité d'Enregistrement de l'identification du Porteur, du Représentant

Légal et le cas échéant, du Mandataire de Certification, se présentant pour obtenir un Certificat.

Damanesign s'engage à réaliser les prestations de Certification selon les modalités et dans les limites des CGU.

Damanesign s'engage à démontrer à l'Utilisateur du Certificat qui en fait la demande qu'elle a émis un

Certificat pour un Porteur donné et que ce Porteur a accepté le Certificat.

Damanesign s'engage à tout mettre en œuvre pour créer et émettre des Certificats contenant des informations réputées exactes.

Pour cela, Damanesign s'engage à s'assurer que le dossier de demande de Certificat est complet, que lespièces fournies sont apparemment conformes.

Damanesign s'engage à ce que le Certificat soit prêt à la délivrance pour le Porteur dans un délai de 7jours maximum à compter de la remise d'un dossier complet à l'Autorité d'Enregistrement.

Damanesign s'engage à établir, par l'émission d'un Certificat, un lien entre l'identité d'une personne et les informations contenues dans ledit Certificat.

Dans l'hypothèse où le Représentant Légal du Client aurait recours aux services d'un délégataire, l'autorité d'enregistrement s'engage à effectuer le contrôle de l'identité du délégataire et la vérification de l'existence du contrat de mandat entre le Représentant Légal du Client et le délégataire.

Le délégataire sera tenu de s'assurer de la validité du mandat qui lui a été conféré par le Client ou son Représentant Légal.

Damanesign prend toutes les mesures raisonnables pour s'assurer que les Porteurs sont au courant de leurs droits et obligations concernant l'utilisation et la gestion des clés, des Certificats et de l'équipementet des logiciels utilisés aux fins de l'IGC.

Damanesign prend les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformitéavec la PC.

Damanesign a un devoir général de surveillance quant à la sécurité et l'intégrité des Certificats délivrés par elle-même ou l'une de ses composantes.

Damanesign s'engage sur le bon fonctionnement des Certificats qu'elle délivre.

Damanesign s'engage à ce que les bi-clés des porteurs sont générées directement dans le dispositif decréation de signature destiné au porteur.

Damanesign interdit à ses employées faisant partie de son entité organisationnelle de souscrire aux certificats de Damanesign. Pour cela, les employés de Damanesign s'engagent à signer le document desconflits d'intérêt.

Article 9 : OBLIGATIONS DU CLIENT

Le Client et son Représentant Légal s'engagent à respecter les stipulations des présentes CGU.

Le Client et son Représentant Légal sont responsables de la gestion des Certificats délivrés aux employés,délégataires ou agents du Client dans le cadre du contrat d'abonnement de façon, et s'engage à faire ensorte que tout Porteur de Certificat respecte les obligations prévues par les présentes CGU et qu'aucunefraude ou erreur n'est commise. A ce titre, le Client et son Représentant Légal s'assurent notamment quele Porteur :

- Communique les informations utiles à la création du Certificat et les éventuelles modifications pendant toute la durée du Certificat ;
- Respecte la procédure de révocation décrite à l'article relatif à la révocation du Certificat ;
- Conserve secrètes et de manière sécurisée, les données confidentielles et le support physique du Certificat.

Le Client et son Représentant Légal s'engagent à informer l'Autorité d'Enregistrement de rattachement de toute modification des informations contenues dans le Certificat, par courrier avec les pièces justificatives requises, sans délais.

Le Client et son Représentant légal s'engagent à fournir toutes informations utiles, exactes et à jour pour la création et la gestion des certificats.

Le Client et le Mandataire sont garants de l'exactitude des informations fournies et de l'exhaustivité despièces justificatives nécessaires à l'enregistrement des certificats.

Paraphes

Le Client et le Mandataire reconnaissent et acceptent que les informations fournies à ce titre soient conservées et utilisées par Damanesign pour gérer les Certificats dans les conditions prévues par la loi eten particulier celles relatives à la protection des données personnelles.

Le Client et le Mandataire reconnaissent être informés des conditions d'installation des Certificats de Damanesign.

Lors du recours à un mandataire, celui-ci doit être formellement désigné par un représentant légal de l'entité concernée et doit être enregistré par l'autorité d'enregistrement.

Le Mandataire de Certification désigné par le Client doit assurer sa mission en toute rigueur.

Le porteur ou le responsable de certificats est tenu de vérifier la validité du certificat et la conformité deson utilisation.

Article 10 : OBLIGATIONS DU PORTEUR

Le Porteur s'engage à fournir toutes informations utiles, exactes et à jour pour la création et la gestion des Certificats pendant toute la durée du contrat.

Le Porteur est garant de l'exactitude des informations fournies et de l'exhaustivité des pièces justificatives nécessaires à l'enregistrement des Certificats.

Il reconnaît et accepte que les informations fournies à ce titre soient conservées et utilisées par Damanesign pour gérer les Certificats dans les conditions prévues par la loi et en particulier celles relativesà la protection des données personnelles.

Le Porteur informe immédiatement Damanesign de toute modification concernant les informations contenues dans son Certificat.

Damanesign se réserve la faculté de procéder à des vérifications aléatoires concernant l'actualité des informations contenues dans le Certificat.

Le Porteur s'engage à informer l'Autorité d'Enregistrement de rattachement de toute modification des informations contenues dans le Certificat, par courrier avec les pièces justificatives requises, sans délais.

Le Porteur reconnaît être informé des conditions d'installation des Certificats et du tutoriel disponible sur

Le site Internet de Damanesign.

Le Porteur s'engage à respecter les usages autorisés des Bi-clés et des Certificats.

Le Porteur protège sa Clé par des moyens appropriés à son environnement. Il s'engage notamment à ne pas communiquer à un tiers son code PIN ou les réponses à ses questions de sécurité.

Le Porteur protège ses données d'activation et, le cas échéant, les met en œuvre.Le Porteur protège l'accès à sa base de Certificats.

Le Porteur respecte les conditions d'utilisation de sa Clé et du Certificat correspondant.

Le Porteur doit faire, sans délai, une demande de révocation de son Certificat en cas de Compromission ou de suspicion de Compromission de sa Clé (ou de ses données d'activations).

Le Porteur s'engage à ne pas délivrer le Certificat qui lui est attribué ni les codes de protection de ceCertificat.

Le Porteur est informé que les informations personnelles d'identité pourront être utilisées commeéléments d'authentification lors de la demande de révocation.

Article 11 : OBLIGATIONS DES UTILISATEURS DE CERTIFICATS

Les Utilisateurs de Certificats sont informés de la nature et de la qualification du Certificat tel qu'indiquéà l'article 2 Définitions & Acronymes, en particulier que celui-ci ne peut être utilisé que pour des servicesd'Authentification et de Signature électronique.

Les Utilisateurs de Certificats vérifient et respectent l'usage pour lequel un Certificat a été émis.

Les Utilisateurs de Certificats Vérifient que le certificat utilisé a bien été émis par l'AC " Damanesign".

Les Utilisateurs de Certificats contrôlent que le Certificat émis par Damanesign est référencé au niveaude sécurité et pour le service de confiance requis par l'application du règlement, du dahir et de la loi marocaine en vigueur.

Vérifier si le Certificat est conforme aux exigences techniques, fonctionnelles, légales, règlementaires ou normatives appropriées à l'usage qu'il souhaite en faire de signature électronique ou de cachet électronique selon le cas.

Utiliser les logiciels et matériels adéquats pour vérifier le bon fonctionnement du dispositif de signature électronique une fois récupéré physiquement depuis le local Damanesign.

Lorsque le Porteur n'est pas le Représentant Légal de l'Entité, l'Utilisateur du Certificat vérifie que le Porteur dispose, à la date de signature, des pouvoirs nécessaires pour engager l'Entité pour l'acte concerné.

Vérifier que le certificat n'est pas présent dans les listes de révocation de l'AC Damanesign. La liste de révocation des certificats émis par l'AC Damanesign est disponible à l'adresse suivante : https://pki.damanesign.ma/

Pour chacun des Certificats de la chaîne de Certification, du Certificat du Porteur jusqu'à l'Autorité de Certification racine, les Utilisateurs du Certificat vérifient le dispositif de signature électronique, l'état du Certificat et notamment la signature numérique de Damanesign, émettrice du Certificat considéré, et contrôlent la validité de ce Certificat.

Les Utilisateurs de Certificats vérifient et respectent les obligations des Utilisateurs de Certificats exprimés dans la PC applicable.

Les Utilisateurs de Certificats sont obligés de n'utiliser la clef privée qu'au travers du dispositif de création de signature.

Article 12 : POLITIQUE DE CERTIFICATION (PC)

Le document dans lequel est décrit l'ensemble de règles, définissant les exigences auxquelles un 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, consultable sur http://pki.damanesign.ma/cps.html

L'OID de la PC applicable à ces présentes Conditions générales d'utilisation pour le service de signature électronique qualifiée est ***OID n° 1.3.6.1.4.1.58553.1.3.1.3***

Et L'OID de la PC applicable à ces présentes Conditions générales d'utilisation pour le service de cachet électronique qualifié est ***OID n° 1.3.6.1.4.1.58553.1.2.1.1 / 1.3.6.1.4.1.58553.1.2.1.2***

Paraphes

Article 13 : PRIX – PAIEMENT DU PRIX

Le prix mentionné dans l'offre commerciale est payable à la commande d'un certificat de durée de vie de 2 ans selon le contrat signé avec le client.

Les modes de règlement acceptés sont les suivants : Espèce/Virement Bancaire/Chèque.

Le Client accepte que Damanesign encaisse le prix dès la validation de son dossier d'enregistrement.

Le Client reconnait expressément que le prix du service est dû en totalité nonobstant la Révocation duCertificat avant son terme, quelle que soit la cause de la Révocation.

Article 14 : ÉTENDUE DES RESPONSABILITES

Le Client demeure à l'égard de Damanesign l'unique responsable du respect des droits du Mandataire et des porteurs au titre des documents contractuels ainsi que du bon accomplissement de leurs obligations.

Le Client garantit en outre Damanesign contre toute action, réclamation ou demande qui pourrait être introduite à son encontre et tout dommage en résultant, ayant directement ou indirectement comme origine ou fondement le non-respect par le Client, un mandataire ou un porteur de l'un quelconque des termes des documents contractuels.

La responsabilité de Damanesign est limitée aux dommages matériels découlant directement d'un manquement de Damanesign à ses obligations aux termes des documents contractuels, à l'exclusion de tout indirect et/ou connexes inhérents à l'utilisation des CERTIFICATS. Et de toute perte de chiffre d'affaires, de bénéfice, de profit, d'exploitation, de renommée ou de réputation de clientèle, du préjudice commercial, économique et autre perte de revenus ou de chance.

Damanesign ne pourrait en aucun cas être tenue responsable dans le cas d'un non-respect par le Client,le Mandataire ou le porteur de leurs obligations notamment en cas de :

- Demande de révocation tardive auprès de l'AE ;
- Utilisation d'un certificat expiré ;
- Utilisation d'un certificat dans le cadre d'une application ou transaction autre que celles prévues aux termes de la PC et des documents contractuels ;
- Usage détourné du Certificat autre que celui spécifié explicitement dans la PC.

Dans le cas où la responsabilité de Damanesign serait retenue, les dommages et intérêts et indemnités àsa charge, toutes causes confondues et toutes sommes confondues, ne sauraient en aucun cas dépasserle prix d'achat du Certificat particulier et le prix d'achat pour le certificat professionnel.

En tout état de cause, la responsabilité totale cumulée de Damanesign au titre d'un service donné pendant toute sa durée, quelle que soit la cause ou la forme de l'action intentée, n'excédera pas la totalitédes sommes versées par le Client au titre du Service.

Damanesign n'assume aucune responsabilité quant aux conséquences des retards, altérations ou pertes que pourrait subir le Client dans la transmission de tous messages électroniques, lettres ou documents.

De même, Damanesign n'assume aucune responsabilité quant aux conséquences liées à la Révocationd'un Certificat.

Le Client dispose d'un délai de trois (3) jours à compter de la survenance du fait à l'origine du dommagepour engager la responsabilité de Damanesign au titre des Conditions Générales.

Article 15 : FORCE MAJEURE

Damanesign ne saurait être tenue responsable des pertes, dommages, retards ou manquement à l'exécution d'obligations résultant des Conditions Générales lorsque les circonstances y donnant lieu relèvent de la force majeure.

Dans l'hypothèse où le cas de force majeure empêche l'exécution par l'une des Parties de ses obligationspour une durée supérieure à deux (2) mois, chacune des Parties pourra résilier les Conditions Générales de plein droit et sans formalité judiciaire, sans que le Client ne puisse prétendre à aucune indemnité.

Article 16 : RESILIATION

Au cas où l'une des parties n'exécuterait pas l'une des obligations découlant des présentes conditions générales, l'autre partie lui notifiera d'exécuter ladite obligation.

A défaut pour la partie défaillante d'avoir exécuté dans les trente (30) jours de cette notification, l'autre partie pourra résilier le Contrat sans préjudice des dommages-intérêts.

Si la partie défaillante exécute dans les trente jours, il pourra être tenu au règlement de dommages- intérêts de retard. En cas de résiliation anticipée, pour quelque cause que ce soit, de la commande, le prixpayé par le client à la souscription reste acquis à Damanesign.

Le client peut demander la résiliation par lettre recommandée papier ou électronique.

Article 17 : CONSERVATION

Le client consent à ce que Damanesign conserve les documents relatifs à la preuve du contrôle d'identification des Porteurs pendant les délais prévus dans la Politique de Certification ainsi que les documents relatifs à la conclusion du présent contrat.

Les données relatives à la fourniture des services de confiance qualifiés (signature/cachet électronique qualifié) sont conservées sur site pendant une durée de trente (30) jours. Après leur génération, ils sont archivés et conservés pendant une durée minimale de 12 ans de manière sécurisée avec accès contrôlé et limité. En effet, la durée de validité du certificat est de deux ans et les certificats sont archivés pendant une période minimum de 12 ans après leur expiration.

Il appartient au client de conserver une copie du présent contrat préalablement imprimé par ses soins, dele signer de manière manuscrite et de retourner l'entier dossier à l'Autorité d'Enregistrement. Les dossiersd'enregistrement sont archivés pour une durée de 12 ans au minimum.

Les dossiers (en version papier et électronique) sont archivés chez Damanesign, sur des sites sécurisés et dont les données sont accessibles qu'aux personnes autorisées.

Les Certificats et les LCR sont archivés pendant une durée minimale de 12 ans après leur expiration.

Si le Client souhaite que les dossiers d'enregistrement, les Certificats ou les LCR soient conservés pour une durée d'archivage supérieure, il devra en faire le nécessaire et en prendre le coût lui-même à sa charge.

Paraphes

Les clés privées des porteurs ne font l'objet d'aucun séquestre et d'aucune sauvegarde.

Les données pertinentes qui doivent être conservées sont toutes les informations relatives à la fourniture d'un service de confiance ou échangés avec Damanesign dans le cadre de la réalisation d'une transactionélectronique, et qui peuvent servir pour :

- Assurer la disponibilité et la continuité du service de confiance fourni y compris en cas d'arrêt de service ;
- Fournir des preuves suffisantes notamment en cas de litige
  - Des preuves de fiabilité du service confiance ;
  - Des preuves d'intégrité et de non-répudiation et de la transaction réalisée par le biais duservice de confiance.

Cela comprend :

- Les conventions acceptées par l'utilisateur du service de confiance en particulier :
  - Les conventions de preuve ;
  - Les conditions d'utilisation du service ;
- Les éléments techniques du service de confiance qui ont servi à conclure la transaction électronique associée :
  - Le cas échéant, les certificats électroniques utilisés, l'ensemble des chaînes de certification mises en œuvre – certificats, jeton d'horodatage … ; les listes de révocation des certificats électroniquesutilisées.
- Les politiques relatives aux services de confiance engagées (exemple : politique de certification, politique de signature …) ;
- Le descriptif des processus d'identification et d'enregistrement des clients ;
- Le cas échéant, les documents objet de la transaction après signature ou cachetage électroniquement, ou a minima les empreintes numériques de ces documents.

Article 18 : PREUVE

Les Parties conviennent expressément que dans le cadre de leurs relations contractuelles, les messagesélectroniques datés et signés valent preuve entre elles et justifient que la notification est imputable à lapartie émettrice dudit message.

Il est expressément convenu que pour la preuve des échanges entre l'Autorité de Certification et le Client,le mandataire, le représentant légal ou le porteur du certificat, seules les archives de l'Autorité de Certification et de l'Autorité d'Enregistrement font foi entre les parties.

Article 19 : SOUS TRAITANCE

Le Client, le mandataire et les porteurs autorisent expressément l'Autorité de Certification (AC) à communiquer à ses partenaires auxquels elle pourrait sous-traiter certains travaux, les données, notamment celles à caractère personnel les concernant ou concernant leur entreprise, nécessaires à l'exécution de ceux-ci.

Article 20 : INTEGRALITÉ DU CONTRAT

Les parties reconnaissent que La version en vigueur des Conditions générales, le formulaire de demandede CERTIFICAT ou celui de son renouvellement ainsi que la version en vigueur de la PC et toutes les procédures organisationnelles constituent l'intégralité des accords entre elles en ce qui concerne la réalisation de des présentes, et annulent et remplacent tous accords et propositions antérieurs ayant le même objet quelle qu'en soit la forme, sous réserve des avenants ou annexes qui viendraient en modifier ou compléter les dispositions.

Article 21 : NULLITÉ

Si une ou plusieurs clauses des CGU sont tenues pour non valables ou déclarées comme telles par une loi,un règlement ou par suite d'une décision définitive d'une juridiction compétente, les autres clauses conserveront leur pleine validité sauf en cas de caractère indissociable avec la stipulation litigieuse.

Article 22 : INDEPENDANCE DES PARTIES

D'une façon générale, chacune des parties est une personne morale indépendante juridiquement et financièrement, agissant en son nom propre et sous sa seule responsabilité.

Article 23 : COMMUNICATION

Damanesign sollicitera ses clients en vue de pouvoir citer, à titre de référence commerciale, son nom.Toute autre communication sera préalablement soumise au Client pour approbation.

Article 24 : ASSURANCE

Damanesign atteste avoir souscrit une assurance Responsabilité Civile et Professionnelle concernant lesprestations relatives au présent Contrat.

En cas de dommage direct subi par le client suite à une faute professionnelle de Damanesign ou de sespréposés dûment prouvée, le client est dédommagé à la hauteur du prix d'achat du certificat pour les certificats professionnels.

Article 25 : PROPRIETE INTELLECTUELLE

L'acquisition d'un Certificat ne confère aucun droit de propriété aux Clients, aux Mandataires ou aux porteurs. Ces derniers s'engagent à respecter et à faire respecter les droits d'auteur et de propriété intellectuelle et industrielle de Damanesign qui est seul propriétaire des noms, logos, marques ou tout autre signe distinctif lui appartenant. Le Client et le Porteur ne pourront faire état ou usage des marques,logos, documents ou tout autre droit de propriété intellectuelle appartenant à Damanesign qu'avec l'autorisation expresse, écrite et préalable de celle-ci.

Article 26 : MODIFICATION DES DISPOSITIONS CONTRACTUELLES

Damanesign peut être amenée à adapter et à apporter des modifications aux dispositions des présentesconditions générales et des documents contractuels relatifs au Certificat (Politique de Certification et Déclaration des Pratiques de Certification) qui lui apparaîtraient nécessaires pour répondre aux évolutions techniques et commerciales de son offre et pour l'amélioration de la qualité des Services de Certification ou qui seraient rendues nécessaires par la modification de la législation, de la réglementationou des référentiels en vigueur.

Les éventuelles modifications des dispositions contractuelles seront publiées sur le site Internet de l'AC. Les changements apportés à un document contractuel seront portés à la connaissance du Client par un email, au moins un mois avant leur entrée en vigueur, le client ayant alors la possibilité de résilier son Contrat en cas de désaccord sans aucune pénalité. En l'absence de résiliation et si le(s) porteurs continuent à utiliser les Certificats dépassant les un mois prévu, le Client sera réputé tacitement avoir accepté lesdites modifications.

Article 27 : POLITIQUE DE GESTION DES PLAINTES CLIENTS

Paraphes

Damanesign a instauré une politique interne de gestion des plaintes clients qui assure un traitementjuste et équitable dans un délai raisonnable.

Damanesign a adopté des mesures pour traiter les plaintes, qui sont résumées ci-dessous :Toutes les plaintes peuvent être soumises soit :

Par courriel : contact@damanesign.ma

Par courrier postal : 4 RUE OUED ZIZ 3EME ETAGE APPT 7 AGDAL, 10080, Rabat

27.1 Responsable traitement des plaintes :

La personne responsable du traitement des plaintes au sein de Damanesign dispose de l'objectivité et del'indépendance nécessaire pour accomplir cette tâche. Elle bénéficie par ailleurs d'une connaissance suffisante pour exécuter cette mission correctement et dispose des informations suffisantes concernant les procédures internes en vigueur.

27.2Procédures :

En cas de mécontentement vis-à-vis d'un service fourni par Damanesign, chaque client doit prendre directement contact avec le responsable du traitement des plaintes.Damanesign adopte les mesures suivantes :

- Le responsable du traitement des plaintes prend en charge la plainte ;
- Dans les trois jours ouvrables suivant la réception de la plainte, un accusé de réception est envoyé au client ;
- Damanesign procède à un examen initial de la plainte et détermine les éventuelles informations supplémentaires ou documents nécessaires pour mener à bien une enquête ;
- Damanesign peut avoir besoin de contacter le client pour obtenir des informations supplémentaires si nécessaire ;
- Dans un délai en principe de deux semaines suivant l'envoi de l'accusé de réception, une réponse finale doit être donnée au client ;
- Damanesign enregistrera les plaintes pour les processus d'amélioration continue et de surveillance par le biais d'un examen régulier.

27.3Informations requises :

Lorsque Damanesign enquête sur une plainte, elle s'appuie sur les informations fournies par le client et celles dont Damanesign dispose déjà.

Pour un traitement rapide et efficace de la plainte par Damanesign, les informations suivantes sontnécessaires pour considérer la plainte comme étant valide tant au niveau de la forme que du fond :

- Les coordonnées du client (afin de vérifier les informations de la banque de données) ;
- La nature de l'engagement avec Damanesign ;
- La personne en charge responsable ;
- La nature de la plainte ;
- Les détails de toutes les mesures déjà prises pour résoudre le problème ;
- Des copies de toute documentation à l'appui de la plainte.

27.4 Réponse à une plainte :

Damanesign accuse bonne réception de la plainte dans les délais prévus ci-dessus. Damanesign s'efforcera de résoudre la plainte dans les deux semaines suivant la réception pour autant qu'elle soit valide et complète. Si la révision dépasse deux semaines, Damanesign informera le client des raisons du retard.

Une fois que Damanesign a examiné la plainte, elle fournit une réponse écrite sur un support durable. Toutes les écritures au client contiendront la mention des prochaines étapes possibles et des procéduresouvertes.

27.5Registre :

Damanesign conserve et met régulièrement à jour un registre des plaintes comprenant notamment lesdétails suivants :

- Le nom et les coordonnées du plaignant ;
- Les faits de la plainte ;
- Mesures prises à la suite de l'enquête sur la plainte du client ;
- Les communications entre Damanesign et le client.

Les informations contenues dans le registre améliorent la gestion et atténuent les problèmes identifiés.

Article 28 : REGLEMENT DES LITIGES – TRIBUNAL COMPETENT

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'Autorité de Certification.

Article 29 : GESTION DES DONNÉES COLLECTÉES

Les données collectées par Damanesign, 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 Damanesign ne pourra traiter votre demande du certificat.

Toute collecte de données à caractère personnel dans le cadre de l'activité Damanesign est réalisée dansle 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, l'autoritéنationale d'agrément et de surveillance de la certification électronique, les dispositifs de contrôle interneet externe, les donneurs d'ordres pour lesquels le bénéficiaire utilisera son certificat pour exploiter leursservices dématérialisés en cas de besoin et toutes les autorités habilitées conformément à la réglementation en vigueur.

Conformément à la loi n°09-08, vous pouvez accéder aux données à caractère personnel vous concernant, les rectifier ou vous opposer au traitement de vos données à caractère personnel pour desmotifs légitimes, par courrier avec accusé de réception à l'adresse suivante :

Damanesign 4 RUE OUED ZIZ 3EME ETAGE APPT 7 AGDAL, Rabat, ou par courrier électronique à l'adresse : contact@damanesign.ma

Ce traitement a été notifié et autorisé par la CNDP au titre de l'autorisation n° : **A-I-119/2024**

Ci-dessous, vous trouverez la mention relative à la protection des données à caractère personnel, conforme aux dispositions de l'article 5 de la loi 09-08.

29.1 Clause et mention types relatifs à la protection des données personnelles :

Clause :

L'Autorité d'Enregistrement indique l'identité du responsable du traitement qui exploite le site.

Paraphes

Les informations recueillies sur le site www.damanesign.ma font l'objet d'un traitement destiné à la production, la fourniture et la gestion des certificats électroniques et les services y afférents.

Les destinataires des données sont l'Équipe Damanesign, plus précisément l'Autorité d'Enregistrement. Conformément à la loi n° 09-08 promulguée par le Dahir 1-09-15 du 18 février 2009, relative à la protectiondes personnes physiques à l'égard du traitement des données à caractère personnel, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vousadressant à l'adresse courriel suivante : contact@damanesign.ma

Vous pouvez également, pour des motifs légitimes, vous opposer à ce que les données qui vousconcernent fassent l'objet d'un traitement.

Ce traitement a été notifié et autorisé par la CNDP au titre de l'autorisation n° : **A-I-119/2024**

Mention :

Conformément à la loi 09-08, vous disposez d'un droit d'accès, de rectification et d'opposition autraitement de vos données personnelles. Ce traitement a été autorisé par la CNDP sous le n° : **A-I-119/2024**

Article 30 : CONTACT

Adresse postale	Damanesign 4 RUE OUED ZIZ 3e ETAGE APPT 7 AGDAL,Rabat
Adresse courriel	contact@damanesign.ma
Site Web	http://pki.damanesign.ma https://www.damanesign.ma/
Téléphone	+212 5 37 68 68 01

Article 31 : CONFORMITÉ

Damanesign est une autorité de certification qualifiée. Elle a fait l'objet d'une évaluation, d'un contrôle de conformité et d'un audit par la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) pour être conforme avec la politique de service de confiance et est inscrite sur la liste de confiance En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'A.C. et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué marocaine. Cette liste de confiance vous sera utile pour la vérification du statut qualifié d'un certificat qualifié.

- **Lien :** https://www.dgssi.gov.ma/fr/prestations-et-produits-reglementes

Article 32 : RESPONSABILITÉS DE LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES

32.1 Entités chargées de la mise à disposition des informations :

L'A.C. met en œuvre une fonction de publication et une fonction d'information sur l'état des certificats, sur les informations devant être publiées à destination des porteurs et des utilisateurs de certificats. Les méthodes de mise à disposition et les URL correspondantes (annuaire accessible par le protocole LDAP et/ou HTTP, serveur Web, serveur OCSP, etc.) sont précisées ci-après.

32.2 Informations devant être publiées :

L'A.C. a pour obligation de publier au minimum les informations suivantes à destination des porteurs et utilisateurs de certificats :

- La politique de certification, établie par le P.S.Co. et couvrant l'ensemble des rubriques du RFC3647
- La liste des certificats révoqués
- Les certificats de l'A.C., en cours de validité
- Le certificat de l'A.C. Racine et son empreinte cryptographique (SHA-256)
- Les différentes P.C. des A.C.

Ces documents sont publiés à l'adresse https://pki.damanesign.ma/cps.html dont la déclaration de divulgation est prise en considération et il s'agit plus précisément d'un document qui décrit les détails importants et les politiques liées à l'infrastructure de clés publiques mise en place (Certificat Qualifiée de Signature, Certificat Root et les CRLs) ainsi qu'une chaine de confiance qui est respectée et bien ficelée.

32.3 Publication du certificat d'AC :

Le certificat de l'Autorité de Certification est publié à l'adresses suivante : http://pki.damanesign.ma/certs/ca_qsig_2022.crt

32. 4 Publication de la CRL :

La liste de certificats révoqués (CRL) est publiée sur :

http://pki.damanesign.ma/crl/ca_qsig_2022.crl

32.5 Délais et fréquences de publication :

Les informations liées à l'I.G.C. (nouvelle version de la P.C., formulaires, etc.) doivent être publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectives de l'A.C. En particulier, toute nouvelle version doit être communiquée au porteur lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord. Les systèmes publiant ces informations doivent avoir une disponibilité de 24 h sur 24, avec une durée maximale d'interruption d'une heure (et pas plus de quatre heures cumulées par mois).

Les certificats d'A.C. doivent être diffusés préalablement à toute diffusion de certificats de porteurs ou de L.C.R. correspondants et les systèmes les publiant doivent avoir la même disponibilité.

- Révocation d'un certificat de signature :

Toute demande de révocation est traitée en urgence. Il s'écoule au maximum vingt-quatre (24) heures entre la demande de révocation par le porteur et la publication de la nouvelle L.C.R. prenant en compte cette demande. La L.C.R. est mise à jour quotidiennement et publiée via HTTP. Toute L.C.R. est publiée dans un délai moins de 30 minutes après sa génération.

- Révocation d'un certificat d'une composante de l'I.G.C. :

La révocation du certificat d'une A.C. est effectuée immédiatement après la validation de cette procédure par le comité de pilotage et suite à la détection d'une des causes de révocation.

Paraphes

Le point de contact identifié au sein de la DGSSI doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

- Exigences de vérification de la révocation par les utilisateurs de certificats :

L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LCR, OCSP…) est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

- Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats :

La fonction de gestion des révocations est disponible 24h/24 et 7J/7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 30 minutes et une durée maximale totale d'indisponibilité par mois inférieure à 2 heures.

32.6 Contrôle d'accès aux informations publiées :

L'ensemble des informations publiées à destination des utilisateurs de certificats doit être libre d'accès en lecture. L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'I.G.C.

32.7 Fonction d'information sur l'état des certificats :

Caractéristiques opérationnelles :

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de L.C.R. au format V2.

Disponibilité de la fonction :

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24 et 7 jours sur 7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 30 min et une durée maximale totale d'indisponibilité par mois de 2 heures.

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'A.C. et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

Signature, approbation du représentant légal/mandataire de certification avec cachet de l'organisme	**Signature du porteur/RCC avec cachet de l'organisme**
Date :	Date :

Paraphes