

I. PREAMBULE

1. Vialink propose à ses Clients
 - a. Un service de Signature électronique permettant à des Porteurs de signer des documents contractuels. A cette occasion, des Certificats numériques sont émis aux Porteurs par Vialink.
 - b. Un service de Cachet permettant à des clients personnes morales de créer des cachets électroniques afin de garantir l'origine et l'intégrité des documents.
2. Vialink porte l'Autorité de Certification (AC) « VIALINK EU STANDARD CA » habilitée, à ce titre, à délivrer, à renouveler, et à révoquer des Certificats numériques.
3. Les Certificats numériques sont émis
 - a. Pour des personnes physiques, agissant à titre personnel, à l'occasion de la signature d'un ou plusieurs documents avec un Client.
 - b. Pour des clients personne morale, afin de leur permettre de sceller leurs documents à l'aide d'un cachet avancé.
4. Le Porteur ou le Responsable du Certificat Cachet serveur (RCCS) déclare être parfaitement informé de l'ensemble des fonctionnalités du Service de Certification, de ses limitations et des obligations qui y sont rattachées.

II. DEFINITIONS

Pour les besoins des présentes, les termes et expressions suivantes ont le sens qui leur est donné ci-dessous :

« Autorité de Certification (AC) »

Entité responsable notamment de la génération, du renouvellement et de la révocation des Certificats de l'Autorité de Certification « VIALINK EU STANDARD CA », suivant les engagements figurant dans la Politique de Certification de cette Autorité de Certification.

« Autorité d'Enregistrement (AE) »

Entité responsable notamment de la collecte et de la vérification des informations du Porteur ou du RCCS, de l'établissement de la demande de certificat, et le cas échéant de la conservation de pièces justificatives du Porteur ou du RCCS.

L'Autorité d'Enregistrement se conforme à ses obligations dans le respect de la Politique de Certification. Le Client assume directement cette responsabilité ou la délègue contractuellement à une tierce partie sous réserve du respect des dispositions de la Politique de Certification et s'il en a fait état dans les Conditions Particulières. Vialink peut également cette responsabilité pour le compte du Client conformément aux Conditions Particulières.

« Certificat »

Désigne l'identité numérique délivrée par Vialink à une personne physique dûment désignée par l'Autorité d'Enregistrement et agissant en son nom propre. Le Certificat dont les caractéristiques sont décrites dans la Politique de Certification lie la signature au signataire.

« Client »

Société contractant avec Vialink pour son compte et/ou celui de ses filiales majoritairement contrôlées à plus de 50 % et l'ayant mandatée dans le cadre des présentes.

« Informations »

Ensemble des informations fournies à Vialink par le Client.

« Politique de Certification »

Document émis par Vialink pour l'Autorité de Certification « VIALINK EU STANDARD CA » dans lequel sont précisées les exigences relatives à la gestion du cycle de vie des Certificats, les

applications autorisées pour les Certificats, et les obligations des intervenants.

« Porteur »

Désigne la personne physique désignée par le Client et à qui un Certificat est délivré, sous la responsabilité de l'Autorité d'Enregistrement. Le Porteur doit se conformer aux obligations qui le concernent et qui sont définies dans la Politique de Certification.

« Responsable du Certificat Cachet Serveur (RCCS) »

La personne physique, dûment autorisée par le client, en charge des opérations de demande et de révocation de certificat pour le compte du client.

« Service de Certification »

Ensemble de prestations comprenant la délivrance, le renouvellement et la révocation de Certificats destinés à être utilisés conformément à la Politique de Certification.

« Utilisateur »

Désigne toute personne physique ou morale utilisant un Certificat, par exemple pour vérifier la Signature ou le Cachet d'un document. L'Utilisateur doit se conformer aux obligations qui le concernent et qui sont définies dans la Politique de Certification.

III. OBJET

Ce document a pour objet de définir les conditions générales d'utilisation des Certificats émis par l'Autorité de Certification « VIALINK EU STANDARD CA » selon la Politique de Certification identifiée ci-dessous.

IV. USAGE DES CERTIFICATS

1. Les Certificats numériques émis par l'AC « VIALINK EU STANDARD CA » sont destinés exclusivement
 - a. A la Signature électronique par le Porteur de documents qui lui sont proposés par le Client. Tout autre usage est explicitement interdit.
 - b. Au Cachet électronique par une personne morale de ses documents à travers les personnes physiques qu'elle désigne sous sa seule responsabilité.
 Tout autre usage est explicitement interdit.
2. Le certificat n'est valide que pendant la durée indiquée dans celui-ci.

V. POLITIQUE DE CERTIFICATION

1. Les Certificats de signature sont émis conformément à la Politique de Certification de l'AC « VIALINK EU STANDARD CA », disponible sur le site de Vialink à l'adresse :

<https://app.vialink.fr/tsp/>

L'OID des certificats traités dans cette Politique de certification rattachée aux présentes Conditions Générales sont les suivants :

OID associé :

Usage du certificat	OID de la PC
Certificat de Signature Personne Physique à la volée	1.2.250.1.198.4.1.2.2.0.1
Certificat d'authentification et de Signature Personne Physique 3 ans	1.2.250.1.198.4.3.2.5.0.1
Certificat de Signature Personne Physique en lien avec une personne morale à la volée	1.2.250.1.198.4.1.3.2.0.1
Certificat d'authentification et de Signature Personne Physique en lien avec une personne morale 3 ans	1.2.250.1.198.4.3.3.5.0.1
Certificat de Cachet serveur 3 ans	1.2.250.1.198.4.4.1.5.0.1
Certificat de Cachet serveur 5 ans	1.2.250.1.198.4.4.1.6.0.1

Autorités de Certification de Vialink	CONDITIONS GENERALES D'UTILISATION DES CERTIFICATS DE SIGNATURE EMIS PAR L'AC "VIALINK EU STANDARD CA"	Version 1.6 Août 2022
---------------------------------------	---	--------------------------

L'OID est indiqué au niveau des informations de stratégies relatives aux certificats présentes dans les détails du certificat associé.

- Les Certificats sont signés l'AC « VIALINK EU STANDARD CA », elle-même disposant d'un certificat signé par l'AC Racine Vialink nommée « VIALINK EU ROOT CA ». Les certificats de ces AC sont accessibles sur le site de Vialink à l'adresse : <https://app.vialink.fr/tsp/>

VI. DELIVRANCE DU CERTIFICAT DE SIGNATURE (personne physique)

- La demande de certificat est initiée par l'Autorité d'Enregistrement au cours du processus de signature.
- Le Porteur pourra fournir à l'Autorité d'Enregistrement une pièce d'identité valide parmi les titres acceptés par l'Autorité de Certification pour prouver l'exactitude des informations de son identité.
- Le Client, en sa qualité d'Autorité d'Enregistrement, valide l'identité du Porteur en vérifiant si possible une pièce d'identité valide parmi les titres acceptés par l'Autorité de Certification.
- L'Autorité d'Enregistrement transmet la demande de certificat validée à l'Autorité de Certification.
- La clé publique et la clé privée du Porteur sont générées par Vialink, utilisées pour la signature et détruites immédiatement après. Vialink garantit par des mesures organisationnelles et techniques que le certificat du Porteur n'est utilisé que pour cette unique signature.
- Le Certificat est émis par Vialink sur la base des informations transmises par l'Autorité d'Enregistrement.
- Le Certificat est inséré dans les documents signés. Ce Certificat n'est pas publié par Vialink sur un autre support.

VII. DELIVRANCE DU CERTIFICAT DE CACHET (personne morale)

- La demande de certificat est initiée par le Client qui précisera l'identité du Responsable du Certificat Cacher Serveur (RCCS). Le Client, en sa qualité d'Autorité d'Enregistrement, valide l'identité du RCCS en vérifiant une pièce d'identité valide parmi les titres acceptés par l'Autorité de Certification.
- Le Client, en sa qualité d'Autorité d'Enregistrement, fournira à Vialink les informations nécessaires à la génération du certificat. Il doit notamment valider les documents suivants :
 - Une pièce justificative de l'existence de la personne morale (par exemple extrait de KBIS pour une société française).
 - Si le RCCS n'est pas le responsable de la société, un mandat l'autorisant à réaliser la demande.
- Le Client, en sa qualité d'Autorité d'Enregistrement, valide les Informations du RCCS et transmet la demande de certificat à l'Autorité de Certification.
- La clé publique et la clé privée du Certificat sont générées par Vialink, et mis à disposition du Client pour le cachet après authentification du Client sur une interface dédiée. Vialink garantit par des mesures organisationnelles et techniques que le certificat du Client n'est utilisé que pour cet unique usage.
- Le Certificat est inséré dans les documents scellés. Ce Certificat n'est pas publié par Vialink sur un autre support.

VIII. REVOCATION DU CERTIFICAT

- Le Porteur (Certificat de personne physique) ou le RCCS (Certificat de personne morale) peut demander la révocation

de son Certificat pendant la période de validité du Certificat en cas d'erreur dans les informations contenues en s'adressant au Service Client Vialink (coordonnées ci-après) ou en se connectant sur le site : <https://app.vialink.fr/tsp/>

- Le Demandeur devra s'authentifier avant que la révocation du Certificat ne soit réalisée par l'Autorité de Certification.
- La révocation du Certificat n'est possible que pendant la durée de validité de celui-ci, limitée à quelques minutes pour les certificats de personnes physiques. Au-delà, le certificat est expiré et ne peut plus, sous aucune condition, être révoqué.
- Le site mis à disposition par Vialink pour effectuer la révocation est disponible 24h/24 et 7j/7, Vialink met en œuvre les mesures appropriées pour en assurer sa disponibilité.
- En cas de compromission de la clé privée, ou d'un incident de sécurité majeur, Vialink peut procéder, unilatéralement et sans tarder, à la révocation d'un Certificat. Dans ce cas, le Porteur ou RCCS est prévenu sans délai.

IX. VERIFICATION DES CERTIFICATS

- Vialink met à disposition des Utilisateurs des mécanismes permettant de vérifier la validité d'un Certificat en termes de date, d'usage indiqué dans la politique de certification applicable (cachet électronique) et d'état de révocation, pour l'ensemble de la chaîne de certification. La suspension des certificats n'est pas autorisée. Les Utilisateurs sont tenus de vérifier un Certificat avant de l'utiliser. La méthode de vérification est laissée à leur appréciation.
- Vialink indiquera aux Utilisateurs les contraintes spécifiques (ajouts ou suppressions) à travers les politiques de certification applicables.
- Pour vérifier la chaîne de certification, l'Utilisateur d'un Certificat peut télécharger les certificats de l'AC Racine et des AC subordonnées sur le site de Vialink <https://app.vialink.fr/tsp/>
- Pour vérifier le statut de révocation d'un Certificat, l'AC publie périodiquement avec une disponibilité de 24h/24 et 7j/7 :
 - la Liste des Certificats Révoqués : <http://crl.vialink.fr/vialink/crl-vialink-eu-standard-ca.crl>
 - la liste des certificats d'AC révoqués : <http://crl.vialink.fr/vialink/crl-vialink-eu-root-ca.crl>
L'AC fournit également un service OCSF à l'URL suivante : <http://crl.vialink.fr/ocsp/standard>

X. OBLIGATIONS DES PORTEURS ET RCCS

Les Porteurs et RCCS s'engagent à :

- Communiquer des informations exactes et à jour lors de la demande de Certificat ;
- Vérifier avec précaution les informations destinées à être intégrées dans le Certificat avant de donner leur accord. Cet accord vaut acceptation du Certificat ;
- Lire, comprendre et accepter les présentes avant de déclencher la signature du ou des documents soumis par le Client ;
- Demander sans délai la révocation de leur Certificat s'ils découvraient une erreur dans les informations transmises à Vialink pour la demande de Certificat ;
- Respecter les pratiques de gestion du dispositif de création de signature transmises par l'AC.

Respecter les engagements qui leur incombent, tels que stipulés dans la Politique de Certification.

Autorités de Certification de Vialink	CONDITIONS GENERALES D'UTILISATION DES CERTIFICATS DE SIGNATURE EMIS PAR L'AC "VIALINK EU STANDARD CA"	Version 1.6 Août 2022
---------------------------------------	---	--------------------------

XI. CONSERVATION DES DONNEES

1. Les enregistrements informatiques relatifs à l'émission, à la gestion et à la révocation de Certificats, objet des présentes, seront conservés par Vialink dans des conditions raisonnables de sécurité durant 10 ans après leur enregistrement.
2. Les documents contractuels ainsi que les justificatifs fournis à l'Autorité d'Enregistrement et/ou à Vialink dans le cadre de la délivrance ou de la révocation d'un certificat sont conservés durant 10 ans, selon les liens contractuels entre Vialink et cette Autorité d'Enregistrement.

XII. CONFORMITE

Vialink est un opérateur de services de certification électronique qui délivre des services conforme au règlement eIDAS, l'AC « VIALINK EU STANDARD CA » est gérée par l'opérateur Vialink.

XIII. LIMITES DE RESPONSABILITES

1. Vialink ne pourra pas être tenue pour responsable d'une utilisation non autorisée ou non conforme des données d'authentification, des Certificats, des listes de révocation, ainsi que de tout autre équipement ou logiciel mis à disposition.
2. Vialink décline sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le Porteur ou le RCCS.
3. En aucun cas, Vialink ne peut être tenue responsable des préjudices indirects tels que notamment perte financière, perte de données, dommage indirect lié à l'utilisation du certificat.

XIV. PROTECTION DES DONNEES A CARACTERE PERSONNEL

1. Conformément la réglementation applicable en matière de protection des données à caractère personnel (et en particulier l'article 13 du Règlement Général sur la Protection des Données 2016-679 du 27 avril 2016, le Porteur ou RCCS est informé que :
 - Les informations collectées et traitées par Vialink intervenant en qualité de Responsable de Traitement sont nécessaires à la gestion des accès, à la fourniture du Service de Certification et à la gestion des informations, les traitements de données opérés par Vialink ayant pour fondement juridique l'exécution du présent contrat.
 - Ces informations sont obligatoires pour l'utilisation du Service. Elles peuvent être utilisées comme éléments d'authentification pour une révocation ;
 - Les informations sont destinées à Vialink, Responsable de traitement, à ses sous-traitants ou à ses partenaires, ainsi qu'aux autorités compétentes,
 - Les données sont conservées pour une durée de 10 ans conformément à l'article « **XI. Conservation des données** » ci-dessus.

Le Porteur ou RCCS est également informé qu'il dispose des droits suivants :

- D'un droit d'accès, de rectification des données le concernant ;
- D'un droit à la limitation du traitement de ses données dans certaines conditions ;
- Du droit à la portabilité des données (c'est-à-dire le droit de demander à Vialink de transmettre ses propres

données ou de les transmettre directement à un autre acteur) ;

- Du droit d'introduire une réclamation auprès de l'autorité de contrôle ;

Les demandes doivent être accompagnées d'un justificatif d'identité et peuvent être adressées :

dpo@vialink.fr

Ou

Vialink, Service DPO
18 quai de la Rapée
75012 PARIS

Cas particulier des cookies :

Les Porteurs ou RCCS sont informés que, lors de l'accès au Site hébergeant le service de signature de Vialink, des informations peuvent être temporairement déposées et stockées sur le terminal utilisé pour la connexion au Site. L'objectif est de faciliter la navigation sur le site et également, sous réserve de leur accord, pour personnaliser leur parcours et pour la diffusion sur le site de publicités ciblées ou de communications et de contenus personnalisés et de réaliser des actions de prospection commerciale directe (email, sms...).

Les Porteurs et les RCCS reconnaissent avoir été informés de cette pratique et des moyens dont ils disposent pour s'y opposer.

XV. CONTACT

Pour toute demande concernant le service de certification de l'AC « VIALINK EU STANDARD CA », contacter le service client de VIALINK :

- Par courrier : Vialink, Service Clients, 18 quai de la Râpée, 75012 PARIS
- Par téléphone au +33 (0)1.40.02.91.12 du lundi au vendredi de 9h à 18h.

XVI. CESSION DU CONTRAT

1. Les présentes Conditions Générales d'Utilisation représentent le Contrat entre Vialink et le Porteur de certificat ou le RCCS qui représente la personne morale.
2. Ce Contrat pourra faire l'objet d'une cession totale ou partielle à un tiers par Vialink sans l'accord écrit et préalable du Porteur ou RCCS, mais moyennant information préalable et écrite de Vialink.

XVII. LOI APPLICABLE

Le Contrat est soumis à la loi française. Il en est ainsi pour les règles de forme comme pour les règles de fond.

XVIII. ATTRIBUTION DE COMPETENCE

En cas de litige et à défaut d'accord amiable entre les parties, compétence expresse est donnée au Tribunal de Commerce de Paris, nonobstant pluralité de défendeurs ou appel en garantie, même pour les procédures d'urgence ou les procédures conservatoires en référé ou par requête.

Le Porteur ou RCCS reconnaît avoir pris connaissance des présentes « Conditions Générales d'Utilisation » et s'engage à les respecter.

Signature du Porteur ou RCCS