

Politique de signature électronique

Varel Capital — Version 1.0

Cette politique décrit le dispositif de signature électronique mis en œuvre par Varel Capital pour la souscription de devis, contrats, mandats et conventions de co-courtage, ainsi que les preuves techniques conservées pour démontrer son intégrité.

1. Niveau de signature et cadre juridique

Le dispositif relève de la **signature électronique avancée** au sens de l'**article 26 du règlement (UE) n° 910/2014 (eIDAS)** et a valeur probante au titre des **articles 1366 et 1367 du Code civil**.

Il satisfait les quatre exigences cumulatives de l'article 26 : lien univoque avec le signataire, identification, contrôle exclusif du dispositif de création, et détection de toute modification ultérieure du document.

2. Conformité aux quatre critères de l'article 26 eIDAS

Critère eIDAS (Art. 26)	Mise en œuvre Varel Capital
a) Lien univoque avec le signataire	Compte utilisateur authentifié (email vérifié) + code OTP à 6 chiffres envoyé sur le numéro personnel + tracé graphique manuscrit capturé sur l'appareil.
b) Identification du signataire	Email vérifié, numéro vérifié par OTP, adresse IP, User-Agent et empreinte de session horodatées.
c) Contrôle exclusif du signataire	OTP à usage unique transmis sur le numéro personnel vérifié, session courte (10 min, 5 tentatives maximum), code stocké uniquement sous forme d'empreinte cryptographique avec sel aléatoire. Le tracé manuscrit est capturé en temps réel sur le terminal du signataire.
d) Détection de toute modification ultérieure	Empreinte SHA-256 du document original et du document scellé, sceau serveur HMAC-SHA256, horodatage qualifié RFC 3161 (FreeTSA). Toute altération invalide le sceau.

3. Procédé technique

1. Préparation. Le PDF est généré côté serveur à partir d'un modèle versionné. Empreinte SHA-256 calculée et conservée.

2. Identification. Authentification du signataire (email + mot de passe) puis OTP SMS envoyé au numéro enregistré.

3. Consentement. Tracé manuscrit dans le canevas dédié + saisie de l'OTP. Transmission chiffrée TLS 1.3.

4. Scellement. Signature apposée dans les champs AcroForm puis aplatie. Nouvelle empreinte SHA-256 + sceau HMAC-SHA256 serveur.

5. Horodatage qualifié. Jeton RFC 3161 demandé à FreeTSA et conservé avec le document.

6. Contresignature. Pour les conventions de co-courtage, un administrateur Varel Capital contresigne par le même procédé, puis le document est re-scellé et re-horodaté.

4. Éléments de preuve conservés

Pour chaque acte signé sont conservés : identifiant signataire, email, téléphone vérifié, IP, User-Agent, horodatages OTP, image PNG de la signature manuscrite, empreintes SHA-256 (original + scellé), sceau HMAC-SHA256, jeton RFC 3161, identifiant unique de session.

Conservation : 10 ans à compter de la fin du contrat (article L.114-1 du Code des assurances). Accès restreint par Row Level Security.

5. Vérification par un tiers

Tout tiers (client, assureur, juge, expert) peut vérifier l'intégrité d'un document signé en : (i) téléchargeant le PDF scellé, (ii) recalculant son empreinte SHA-256 et en la comparant à celle journalisée, (iii) validant le sceau HMAC-SHA256 sur demande, (iv) vérifiant indépendamment le jeton RFC 3161 auprès de FreeTSA.

6. Contact

Pour toute question relative à la présente politique : **contact@varelcapital.fr** — Varel Capital, courtier en assurances, ORIAS 18003377.

Document maintenu par Varel Capital — Version 1.0.