DOCUMENT DE RÉFÉRENCE À L'ATTENTION DES INTÉGRATEURS

Fiche technique destinée aux clients souhaitant intégrer Pixel Sceau dans leur propre système d'information.

PIXEL SCEAU

Intégration API B2B
pour signature électronique
en environnement applicatif

Intégration API B2B

Trois modes de signature, trois niveaux d'authentification, un modèle de tarification cohérent

VERSION

Version 1.0 — Mai 2026

ÉMETTEUR

Pixel AI SARLU — en cours d'immatriculation au RCCM d'Abidjan
conçu par Honoré DEMBÉLÉ, 10 BP 3333 Abidjan 10, Cocody

DOCUMENT PARENT

Mémoire technique Pixel Sceau v1.5
https://cipixel.com/sceau-specifications

Document auto-signé électroniquement par Pixel Sceau, ancré sur Bitcoin via OpenTimestamps.

Sommaire

1. Objet du document

Ce document s'adresse aux entreprises qui souhaitent intégrer le service Pixel Sceau dans leur propre système d'information, pour produire des signatures électroniques de façon programmatique. Il complète le Mémoire technique de référence v1.5, qui décrit l'architecture cryptographique sous-jacente.

Pixel Sceau est principalement conçu pour un usage individuel par des professionnels du droit (notaires, huissiers, avocats, etc.) au moyen de l'interface web `cipixel.com/signer`, avec authentification à deux facteurs personnels (mot de passe et code TOTP). Cet usage demeure le mode par défaut.

Cependant, certaines organisations (compagnies d'assurance, établissements bancaires, plateformes immobilières, services de l'État, éditeurs SaaS) ont des besoins de signature en volume qui ne peuvent être satisfaits par l'intervention manuelle d'un opérateur humain. À titre d'exemple, une compagnie d'assurance émettant 500 polices par jour ne peut raisonnablement demander à un cadre désigné de saisir 500 codes TOTP. C'est l'objet de l'**API B2B** décrite ici.

Trois questions structurent cette fiche :

1. **Qui signe**, lorsque c'est un système qui appelle l'API ? Trois modes sont proposés (chapitre 2), au choix du client selon la nature des actes.
2. **Comment authentifier le système** client lui-même, en l'absence d'opérateur humain ? Trois niveaux d'authentification API sont proposés (chapitre 3), du plus simple au plus strict.
3. **Combien cela coûte-t-il** ? Un modèle de tarification à trois paliers est exposé (chapitre 4).

2. Les trois modes de signature

La question de savoir qui est juridiquement signataire d'un acte produit par voie d'API est essentielle. La réponse ne peut pas être « l'API » : une personne morale ou un système informatique ne peuvent former une volonté juridique. Pixel Sceau propose donc trois architectures qui correspondent à trois cas d'usage distincts.

2.1 Mode Système — signature au nom de la personne morale

Le client se voit attribuer un identifiant Pixel dédié à son système d'information, sous la forme `09S-XXXXXXXX-X` (S = System). Toutes les signatures émises par l'API au moyen

de cet identifiant portent la mention de la personne morale (« Atlanta Assurances — système de production »).

Cas d'usage : attestations standardisées, accusés de réception, certificats de garantie automatiques, bordereaux récurrents.

Limite : ce mode ne convient pas aux actes qui exigent l'engagement personnel d'un dirigeant ou d'un mandataire identifié.

2.2 Mode Déléguée nominative — signature au nom d'une personne physique pré-autorisée

Un dirigeant ou un mandataire de l'entreprise (par exemple le Directeur Général) délivre, par voie électronique signée, une délégation d'usage à son système : « j'autorise mon système d'information à signer en mon nom les polices d'assurance d'un montant inférieur à 5 millions de francs CFA, du lundi au vendredi de 8 heures à 18 heures ». Toute signature qui respecte cette enveloppe est apposée au nom du dirigeant ; toute signature qui en sort est refusée et fait l'objet d'une notification.

Cas d'usage : actes routiniers dont l'enveloppe est précisément définie et tracée.

Avantage : la responsabilité juridique du signataire personne physique est préservée, mais sans la friction d'une saisie manuelle pour chaque acte.

2.3 Mode Humaine déclenchée par API — l'API prépare, l'humain signe

Le système client appelle l'API pour préparer un acte ; une notification est aussitôt adressée au signataire désigné, qui consulte le document, valide son authentification à deux facteurs, et appose effectivement sa signature. L'API ne signe pas elle-même : elle orchestre.

Cas d'usage : actes engageant fortement la responsabilité personnelle du signataire (contrats supérieurs à un seuil, actes inhabituels, engagements stratégiques).

Avantage : sécurité juridique maximale, sans perte de l'intégration applicative.

2.4 Combinaison recommandée

Dans la pratique, un même client utilise généralement **plusieurs modes** selon le type d'acte. Une compagnie d'assurance utilisera typiquement le mode Système pour les attestations, le mode Déléguée pour les polices courantes, et le mode Humaine déclenchée pour les contrats au-delà d'un seuil contractuel. Ce paramétrage est défini conjointement à l'intégration et formalisé dans une matrice d'autorité revue annuellement.

3. Les trois niveaux d'authentification API

L'authentification d'un système client face à Pixel Sceau est indépendante du mode de signature retenu. Trois niveaux sont proposés, du plus simple au plus strict, selon les exigences du client.

3.1 Niveau A — Clé d'API

Le client se voit délivrer une clé d'API de 256 bits, transmise dans l'en-tête HTTP `X-Identity-API-Key` de chaque requête. La clé est stockée hachée (SHA-256) côté serveur ; sa rotation est possible à tout moment depuis la console d'administration. Cette méthode est suffisante pour un volume modéré et un client ayant maîtrise de son environnement.

3.2 Niveau B — Clé d'API et signature HMAC de la requête

En complément de la clé d'API, chaque requête est signée en HMAC-SHA-256 au moyen d'une clé secrète partagée, distincte de la clé d'API. La signature est calculée sur le corps de la requête, un horodatage (timestamp) et un identifiant unique (nonce), et transmise dans l'en-tête `X-Pixel-Signature`. Cette méthode prévient les attaques par rejeu (replay) et la modification du corps de la requête en transit. Elle est recommandée pour les clients à volume élevé ou soumis à des exigences réglementaires spécifiques.

3.3 Niveau C — TLS mutuel et liste d'adresses IP autorisées

Pour les clients aux exigences les plus strictes (banques, services de l'État, opérateurs critiques), Pixel Sceau émet un certificat client X.509 signé par sa propre Autorité de Certification ; le client présente ce certificat à chaque connexion (mutual TLS). Les adresses IP sources du client sont en outre listées en allocation explicite (allowlist) côté serveur. Toute requête issue d'une autre adresse, ou non accompagnée d'un certificat client valide, est rejetée avant toute tentative d'authentification applicative.

> **Remarque.** Les niveaux d'authentification API et les modes de signature sont orthogonaux. Un même client peut tout à fait combiner une authentification niveau C (TLS mutuel) avec un mode de signature humaine déclenchée par API, pour les actes les plus critiques.

4. Modèle de tarification

Quatre formules sont proposées, adaptées à la taille et à la prévisibilité du besoin du client.

Formule	Cible	Tarif indicatif
Gratuit — Notaires	Notaire individuel inscrit à l'Ordre de Côte d'Ivoire, usage par interface web	Gratuit les 12 premiers mois suivant la première signature
Pay-as-you-go	Petite organisation, volume variable, sans engagement	150 FCFA par signature, facturation mensuelle a posteriori
Forfait mensuel	PME et cabinets prévoyant un volume régulier	25 000 FCFA pour 500 signatures incluses ; 100 FCFA par signature supplémentaire
Enterprise	Grandes organisations (banques, assurances, plateformes nationales, État)	Sur devis : volume, engagement de niveau de service, support dédié, certificat client mTLS, console de pilotage

Les tarifs ci-dessus sont indicatifs au stade de lancement et seront stabilisés après concertation avec les premiers clients de référence. Le service demeure gratuit pour les notaires individuels durant la phase initiale (cf. Mémoire technique v1.5, chapitre 8).

5. Procédure d'intégration

L'intégration d'un client B2B suit un parcours en six étapes, dont la durée totale dépend du niveau d'authentification retenu.

1. **Prise de contact** — Le client adresse une demande à `contact@cipixel.com` en précisant son volume estimé, son cas d'usage et le niveau d'exigence souhaité. Réponse sous deux jours ouvrés.
2. **Cadrage** — Une réunion de cadrage (à distance ou sur site à Abidjan) permet de définir le mode de signature, le niveau d'authentification, la matrice d'autorité et les modalités de facturation.

3. **Convention de service** — Rédaction et signature d'une convention bilatérale qui formalise l'ensemble des paramètres définis lors du cadrage.
4. **Provisionnement technique** — Émission de la clé d'API (niveau A), de la clé HMAC (niveau B) ou du certificat client (niveau C). Création de l'identifiant Pixel dédié (09S, ou délégation rattachée à un 09 personnel). Le délai est de un à cinq jours ouvrés selon le niveau retenu.
5. **Phase pilote** — Le client procède à ses premiers appels en environnement de production restreint, avec accompagnement technique du concepteur. Cette phase dure typiquement deux à quatre semaines et permet d'ajuster la matrice d'autorité.
6. **Mise en production** — Le service est ouvert au volume nominal du client. Le suivi se poursuit au moyen de la console de pilotage et du dispositif de support défini à l'étape 3.

6. Engagement de niveau de service

Pixel Sceau prend, à l'égard de ses clients B2B, les engagements suivants :

Indicateur	Engagement
Disponibilité mensuelle du service	99,5 % en formule Forfait ; 99,9 % en formule Enterprise
Temps de réponse aux requêtes API	Moins de 800 millisecondes au 95e percentile, hors apposition de signature
Délai d'apposition d'une signature PAdES	Moins de 3 secondes au 95e percentile, horodatage TSA et ancrage Bitcoin compris
Délai de réponse au support	24 heures ouvrées en formule Forfait ; 4 heures ouvrées en formule Enterprise
Notification d'incident	Sous 2 heures sur le canal convenu (courriel, webhook signé)
Temps de reprise après sinistre majeur	RTO 4 heures, RPO 24 heures (formule Enterprise : RTO 1 heure, RPO 1 heure)

Les indicateurs ci-dessus sont mesurés mensuellement et exposés au client dans sa console de pilotage. En cas de dépassement, des avoirs sont accordés selon une grille convenue contractuellement.

7. Annexe — Exemple d'appel API

L'exemple suivant illustre l'apposition d'une signature en mode Système avec authentification de niveau A. Il est volontairement simplifié ; la documentation technique complète (OpenAPI 3.0) sera mise à disposition lors de la phase de provisionnement.

```
POST /api/v1/sceau/b2b/signer HTTP/1.1
Host: api.pixelhelix.net
X-Identity-API-Key: <clé délivrée au client>
Content-Type: application/json

{
  "code_09": "09S-ATLANTASYS-X",
  "nom_signataire": "Atlanta Assurances — système de production",
  "motif": "Attestation de garantie n° 2026-04231",
  "pdf_b64": "<PDF source encodé en base64>",
  "callback_url": "https://atlanta.example.ci/sceau/callback"
}
```

La réponse, encodée en JSON, contient le PDF signé en base64, l'empreinte SHA-256 du document signé, la référence d'horodatage Bitcoin et la durée de traitement. Si l'option callback_url est utilisée, une notification signée HMAC est envoyée au client en cas d'événement ultérieur (confirmation Bitcoin, par exemple).

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "statut": "signe",
  "ref_signature": "SIG-20260524-3F8B7C",
  "pdf_signe_b64": "<PDF signé encodé en base64>",
  "sha256_signe": "67f90d29...",
  "ref_horodatage": "HRD-XXXXXXXX",
  "duree_traitement_ms": 1842
}
```

8. Coordonnées et prise de contact

Élément	Valeur
Émetteur	Pixel AI SARLU (en cours d'immatriculation au RCCM d'Abidjan)
Conception et exploitation	Honoré DEMBÉLÉ, 10 BP 3333 Abidjan 10, Quartier Cocody, Côte d'Ivoire
Demandes commerciales	`contact@cipixel.com`
Support technique	`support@cipixel.com`
Site institutionnel	https://cipixel.com
Document parent	Mémoire technique de référence v1.5 — https://cipixel.com/sceau-specifications
Vérification publique d'une signature	https://cipixel.com/verifier-signature

---

Pixel Sceau — Fiche d'intégration API B2B — version 1.0 — mai 2026.


```
Signe electroniquement par
Honoré DEMBÉLÉ
09P-HFJRVTT2-V
2026-05-24 00:42:36 UTC
Pixel Sceau
```