RÉPUBLIQUE DE CÔTE D'IVOIRE · ORGANISATION AFRICAINE DE LA PROPRIÉTÉ INTELLECTUELLE

Mémoire technique rédigé par le concepteur, à l'intention exclusive des notaires, en accompagnement du dépôt OIPI/OAPI parent du 24 mars 2026. Document distinct de toute procédure d'agrément ARTCI, non encore initiée.

PIXEL SCEAU

Service de signature électronique avancée et d'horodatage

Mémoire technique de référence

À l'attention des Notaires et de l'Ordre des Notaires de Côte d'Ivoire

VERSION

Version 1.5 — Mai 2026

CONCEPTEUR ET DÉPOSANT

Honoré DEMBÉLÉ, Ivoirien

10 BP 3333 Abidjan 10, Cocody · Abidjan, Côte d'Ivoire

DÉPÔT PARENT

OIPI / OAPI · 24 mars 2026 · Couverture 17 pays

Document signé électroniquement par son propre service et horodaté sur Bitcoin (OpenTimestamps).

Sommaire

1. Objet du présent mémoire

Ce document expose, à l'intention des notaires de Côte d'Ivoire, de leur Ordre et de l'autorité de régulation, l'architecture technique du service Pixel Sceau. Il décrit les algorithmes, les normes, les garanties opérationnelles et les modalités de vérification indépendante. Il ne constitue pas un argument commercial. Il constitue un dossier de référence.

Pixel Sceau a pour vocation d'offrir aux praticiens du droit un outil d'apposition d'une signature électronique avancée sur tout document numérique, accompagné d'un horodatage à valeur probante renforcée. Le service est conçu comme un auxiliaire de l'écrit authentique notarié et ne prétend en aucune manière s'y substituer.

La conformité revendiquée est celle de la **signature électronique avancée** au sens des normes ETSI EN 319 142 et du droit ivoirien des transactions électroniques. Le service relève à ce stade du régime de fait : il offre les garanties techniques d'une signature avancée sans encore disposer de l'agrément formel de l'ARTCI. L'obtention du statut de **signature électronique qualifiée**, qui impliquera un audit préalable par l'ARTCI selon une procédure dont le concepteur prend l'entière responsabilité, fait l'objet du chapitre 9 du présent mémoire.

2. Identification du prestataire et responsabilité

Élément	Valeur
Concepteur, inventeur, déposant	Honoré DEMBÉLÉ, ressortissant ivoirien
Adresse postale	10 BP 3333 Abidjan 10, Quartier Cocody, Abidjan, République de Côte d'Ivoire
Numéro de carte nationale d'identité	CI 002 896 764 (NNI : 117 477 548 71)
Lieu de naissance	Commune de Gagnoa, République de Côte d'Ivoire
Dépôt OIPI/OAPI parent	Dossier déposé le 24 mars 2026, conforme à l'Annexe I de l'Accord de Bangui, 12 revendications, couverture 17 États membres
Entité juridique titulaire envisagée	Pixel AI SARLU, société à responsabilité limitée unipersonnelle de droit ivoirien, en cours d'immatriculation au RCCM d'Abidjan
Adresse courriel professionnelle	contact@cipixel.com
Site institutionnel	https://cipixel.com

Pixel AI SARLU est l'entité titulaire et opératrice du service. La société est en cours d'immatriculation au Registre du Commerce et du Crédit Mobilier d'Abidjan ; dès son immatriculation effective, elle reprend à son compte l'ensemble des actes et engagements pris durant la phase de constitution. La cession formelle des droits de propriété intellectuelle du concepteur vers la société sera elle-même horodatée sur Bitcoin (bloc dit « PIXEL-1 », successeur de PIXEL-0 actuellement ancré).

La **responsabilité civile et juridique** du service est portée par la société, dans la limite de son capital social, conformément au régime de la société à responsabilité limitée unipersonnelle de droit OHADA. En aucun cas la responsabilité personnelle du concepteur, du gérant ou de tout collaborateur de la société n'est engagée à raison de l'usage normal du service.

3. Cadre normatif applicable

3.1 Droit ivoirien des transactions électroniques

Le service est conçu pour respecter les exigences de la **loi ivoirienne sur les transactions électroniques** (loi n° 2013-546 du 30 juillet 2013) et de ses textes d'application, en particulier les dispositions relatives à la valeur probante de l'écrit et de la signature sous forme électronique.

3.2 Règlement UEMOA

Le service s'inscrit dans le cadre régional défini par les actes additionnels de l'UEMOA relatifs aux transactions électroniques et à la cybersécurité, et entend obtenir, par anticipation, le statut équivalent à celui de prestataire qualifié.

3.3 Standards internationaux retenus

Le choix des algorithmes et des formats s'aligne sur les standards internationaux en vigueur, retenus pour leur stabilité, leur publication ouverte et leur reconnaissance par les autorités de régulation européennes et nord-américaines :

- **ETSI EN 319 142-1 et 319 122-1** — formats de signature électronique avancée PAdES et CAdES, publiés par l'European Telecommunications Standards Institute.
- **RFC 3161** — protocole d'horodatage par autorité tierce (Time-Stamp Protocol).
- **RFC 5280, RFC 5652, RFC 6238, RFC 4226** — infrastructure à clés publiques X.509, Cryptographic Message Syntax, mot de passe à usage unique fondé sur le temps.
- **NIST FIPS 186-4 et FIPS 180-4** — Digital Signature Standard et Secure Hash Standard, publiés par le National Institute of Standards and Technology des États-Unis.

> **Pourquoi ces choix sont opposables à tout tiers.** Les normes ETSI et les RFC sont publiques, librement consultables, et leur conformité peut être vérifiée par tout expert indépendant disposant des outils open source de référence (pyHanko, OpenSSL, opentimestamps-client). Le notaire conserve donc la maîtrise complète de la vérification, sans avoir à faire confiance au prestataire.

4. Architecture cryptographique

4.1 Authentification à deux facteurs

Avant toute apposition de signature, l'identité du signataire est vérifiée par **deux facteurs indépendants** :

1. Facteur de connaissance : mot de passe haché par bcrypt (paramètre de coût 12).
2. Facteur de possession : code à usage unique généré sur l'appareil personnel du signataire au moyen d'une application d'authentification standard (RFC 6238). Le code est valide trente secondes et utilisé une seule fois.

Le secret partagé est chiffré au repos par algorithme symétrique authentifié. La défaillance répétée d'authentification entraîne un verrouillage temporaire progressif (cinq tentatives — quinze minutes ; dix — une heure ; vingt — vingt-quatre heures). L'ensemble des tentatives est consigné dans un journal d'audit horodaté et conservé.

4.2 Génération de la clé du signataire

À l'enrôlement, le signataire se voit attribuer une paire de clés asymétrique sur **courbe elliptique NIST P-384 (secp384r1)**, conforme à FIPS 186-4. Cette courbe est recommandée pour les usages réglementaires post-2025. Le niveau de sécurité offert est équivalent à une clé RSA de 7 680 bits, tout en réduisant la taille des signatures.

La clé privée du signataire est chiffrée au format PKCS#8 et n'est jamais transmise ; elle est descellée le temps d'une signature au moyen d'une passphrase détenue par le système, puis détruite en mémoire.

4.3 Certification de la clé du signataire

La clé publique du signataire est attestée par un certificat X.509 émis par l'Autorité de Certification interne Pixel Sceau. Cette autorité est constituée d'une clé RSA de 3 072 bits, conservée chiffrée et destinée à être migrée sur module matériel de sécurité (HSM) certifié FIPS 140-2 niveau 3 dans le cadre de l'agrément qualifié.

Le certificat du signataire mentionne, dans son SerialNumber, l'identifiant Pixel à neuf caractères (code 09) du signataire ; le CommonName porte son nom et son prénom tels qu'inscrits à son acte de naissance ou à sa carte nationale d'identité. La validité du certificat est de deux années renouvelables.

4.4 Format de signature

Pour les documents au format PDF, la signature est apposée selon le format **PAdES baseline B-LT** (ETSI EN 319 142-1), sous-type CMS détaché `/ETSI.CAdES.detached`. L'empreinte du document est calculée en **SHA-384**, cohérente avec la courbe P-384 retenue. Une zone de signature visible, dite « cartouche », est apposée sur la dernière page du document ; elle indique le nom du signataire, son identifiant Pixel, la date et l'heure, ainsi que la mention « Pixel Sceau ».

Les documents au format OOXML (Microsoft Word, Excel, PowerPoint) sont signés selon le format XAdES embarqué dans le paquet, conformément à ETSI EN 319 132-1. Les autres types de fichiers reçoivent une signature CMS détachée encapsulée dans un conteneur ASiC-S (ETSI EN 319 162-1).

4.5 Horodatage à valeur probante

Chaque signature est accompagnée d'un horodatage RFC 3161 délivré par une autorité d'horodatage tierce. À ce jour, l'autorité retenue est DigiCert SHA384 RSA4096 Timestamp Responder 2025, dont les certificats sont reconnus par les principaux distributeurs de confiance (Microsoft, Mozilla, Apple). L'horodatage est intégré à la signature et permet d'établir, de manière indépendante du serveur Pixel, que le document existait dans son état signé à une date donnée.

4.6 Ancrage Bitcoin (preuve temporelle décentralisée)

En complément de l'horodatage par autorité tierce, l'empreinte SHA-256 du document signé est soumise au protocole ouvert OpenTimestamps. Celui-ci agrège les empreintes reçues et publie, à intervalles réguliers, une racine de Merkle dans une transaction Bitcoin. La preuve d'inclusion qui en résulte permet à tout vérificateur de constater, sans recourir à aucun serveur Pixel ni DigiCert, que le document existait avant un bloc Bitcoin donné. Cette preuve survit à la disparition de tous les acteurs intermédiaires.

4.7 Anticipation de la menace quantique post-RSA / ECDSA

Les algorithmes asymétriques classiques fondés sur le problème du logarithme discret (ECDSA) ou sur la factorisation (RSA) sont théoriquement vulnérables à un ordinateur quantique cryptographiquement pertinent (cryptographically relevant quantum computer, CRQC) au moyen de l'algorithme de Shor (1994). À la date du présent mémoire, aucun CRQC n'est en opération ; les estimations académiques convergentes situent le seuil de pertinence cryptographique entre 2030 et 2040.

Le concepteur prend toutefois acte que le National Institute of Standards and Technology (NIST) a publié en août 2024 trois standards de cryptographie post-quantique :

- **FIPS 203** — ML-KEM (anciennement CRYSTALS-Kyber), encapsulation de clé ;
- **FIPS 204** — ML-DSA (anciennement CRYSTALS-Dilithium), signature numérique ;
- **FIPS 205** — SLH-DSA (anciennement SPHINCS+), signature numérique sans état.

Pour le service de signature électronique, le risque dit « récolte aujourd'hui, déchiffrement demain » (harvest now, decrypt later) ne s'applique pas : un acte signé aujourd'hui ne peut être resigné rétroactivement par un attaquant disposant d'un CRQC futur. La signature passée reste opposable, son antériorité étant garantie par l'horodatage Bitcoin indépendant du chiffrement.

La feuille de route inclut, à l'horizon 2027-2028 et en cohérence avec le calendrier ETSI / ANSSI, l'adoption d'un schéma de **signature hybride** — ECDSA P-384 (sécurité classique) doublée de ML-DSA FIPS 204 (sécurité post-quantique) — afin que les actes signés à compter de cette transition restent vérifiables dans les deux régimes cryptographiques, sans avoir à choisir entre rétro-compatibilité et résistance quantique.

5. Procédure de vérification indépendante par le notaire

Tout notaire peut vérifier l'authenticité d'une signature Pixel Sceau par **trois voies parallèles**, dont aucune ne dépend de la disponibilité du serveur Pixel.

5.1 Vérification au moyen d'Adobe Acrobat Reader

Le document signé étant un PDF conforme à PAdES, son panneau « Signatures » dans Adobe Acrobat Reader expose l'identité du signataire, la chaîne de certificats, l'algorithme cryptographique et la date du timestamp DigiCert. Tant que l'Autorité de Certification Pixel n'est pas inscrite à la Adobe Approved Trust List, le statut indiqué sera « Validity Unknown » ; le notaire peut, en toute simplicité, ajouter la CA Pixel à son magasin de certificats de confiance pour obtenir le statut « Signature Valid ». La démarche d'inscription à la AATL ou à l'EUTL fait partie de la feuille de route d'agrément exposée au chapitre 8.

5.2 Vérification en ligne de commande, outils libres

À l'intention des notaires qui souhaitent procéder à un contrôle approfondi, les outils libres suivants permettent une vérification autonome :

- `pyhanko sign validate` — vérification complète PAdES, chaîne de certificats et timestamp.
- `openssl dgst -sha384` — recalcul de l'empreinte du document.
- `ots verify` — confirmation de l'ancrage Bitcoin du document.

5.3 Vérification publique sur cipixel.com

Le service expose un point d'accès public, accessible sans authentification, à l'adresse **https://cipixel.com/verifier-signature**. Le notaire y dépose le document à vérifier ; le service retourne, sans conserver le document, le statut d'authenticité et le détail des éléments cryptographiques.

> **Principe directeur.** Le notaire n'a, à aucun moment, à faire confiance au prestataire. Il est mis en mesure d'établir lui-même, par des outils standards et publics, que la signature et l'horodatage sont mathématiquement valides.

6. Garanties de pérennité et de continuité

6.1 Validation à long terme

Le format PAdES B-LT retenu embarque, dans la signature elle-même, les listes de révocation (CRL) et les réponses OCSP au moment de la signature. Ainsi, la signature reste vérifiable même après expiration des certificats. La feuille de route prévoit le passage au niveau B-LTA, qui ajoute un horodatage périodique d'archivage permettant une validation au-delà de dix années.

6.2 Conservation des éléments cryptographiques

Les certificats émis, ainsi que les empreintes des signatures et les preuves Bitcoin associées, sont conservés dans une base de données chiffrée au repos et sauvegardés quotidiennement, sous forme chiffrée par algorithme AES-256-CBC, sur infrastructure tierce indépendante (Cloudflare R2). Une copie supplémentaire est conservée par le concepteur en archive personnelle chiffrée.

6.3 Hypothèse de cessation d'activité du prestataire

En cas de cessation d'activité de Pixel Sceau, le notaire conserve la pleine capacité de vérifier les signatures antérieurement produites :

1. Le document signé est auto-portant : il embarque la signature, le certificat, le timestamp DigiCert et les éléments de validation.
2. L'empreinte du document est inscrite dans la chaîne Bitcoin et reste vérifiable indépendamment de tout serveur.
3. L'Autorité de Certification Pixel sera, à l'horizon de l'agrément qualifié, déposée auprès d'un tiers séquestre de confiance pour assurer sa pérennité au-delà de la durée de vie du prestataire.

6.4 Continuité institutionnelle au-delà du fondateur

Le service est porté par une société commerciale, Pixel AI SARLU, et non par une personne physique. Cette construction juridique a pour effet :

1. De limiter la responsabilité aux actifs sociaux, conformément au régime OHADA de la SARLU ; aucune personne physique n'engage son patrimoine personnel.
2. De permettre la transmission de la fonction d'opérateur : décès, incapacité, retrait ou cession du fondateur entraînent la désignation d'un nouveau gérant selon les statuts, sans interruption du service ni perte de la qualité d'opérateur.
3. D'isoler le service de toute considération personnelle : un notaire qui utilise Pixel Sceau ne contracte pas avec une personne, il contracte avec une institution organisée pour durer.

En complément, le plan de continuité prévoit le dépôt de la clé maître de l'Autorité de Certification, des codes sources du service et des procédures d'exploitation auprès d'un tiers séquestre, opposable à toute reprise de l'activité par un successeur. Ce dispositif est cohérent avec les exigences attendues au titre de l'agrément PSCE qualifié.

6.5 Protection de l'Autorité de Certification et politique de révocation

La compromission de l'Autorité de Certification interne Pixel Sceau constituerait, en théorie, la faille la plus grave envisageable : un attaquant disposant de la clé privée de la CA pourrait émettre frauduleusement des certificats au nom de signataires arbitraires. Le concepteur prend acte de cette menace structurelle et applique, à proportion du niveau de service revendiqué (avancé, non encore qualifié), les mesures suivantes :

1. La clé privée de la CA est conservée au format PKCS#8 chiffré, sur volume serveur en permission restrictive (700/600), accessible uniquement au compte de service

applicatif. La passphrase de descellement est isolée du processus et chargée en variable d'environnement éphémère.

2. Aucune signature de certificat n'est effectuée sans descellement explicite de la clé ; à l'issue de l'opération, la clé est purgée de la mémoire.
3. Les opérations sensibles sur la CA (émission, révocation, rotation) sont journalisées dans la table pixel.audit_log et conservées de manière indélébile.

À l'horizon de l'agrément qualifié, le dispositif est renforcé :

1. Migration de la clé privée de la CA sur **module matériel de sécurité (HSM)** certifié FIPS 140-2 niveau 3, sans extraction possible.
2. Séparation en Root CA hors ligne et Intermediate CA en ligne, afin que la compromission de l'IC ne contraigne pas à la révocation de toute la chaîne.
3. Dépôt de la clé Root CA auprès d'un tiers séquestre de confiance indépendant.
4. Publication des certificats émis dans des journaux de transparence (Certificate Transparency logs) inspirés de la norme RFC 6962, permettant à tout tiers de surveiller l'activité de l'autorité.

Politique de révocation. La révocation d'un certificat de signataire peut être déclenchée selon trois voies :

- À la demande du titulaire, sur preuve d'identité (compromission de moyen d'authentification, départ de l'étude, cessation d'activité notariale) ;
- À l'initiative du prestataire, sur détection automatique ou signalement de compromission ;
- Sur ordre judiciaire dûment notifié.

L'effet de la révocation est immédiat : le certificat est marqué revoque dans la base, et toute tentative ultérieure de signature ou de vérification renvoie un échec d'authentification. Les signatures antérieures à la révocation conservent leur validité, conformément au principe de la signature électronique avancée : la révocation produit ses effets ex nunc, non ex tunc.

La publication d'un répondeur OCSP (RFC 6960) sous `ocsp.cipixel.com` et d'une liste de révocation publique (CRL, RFC 5280) sous `crl.cipixel.com` est inscrite à la feuille de route d'agrément (cf. chapitre 9). Dans l'intervalle, la liste interne tient lieu de référence et est consultable sur demande motivée de l'Ordre.

7. Sécurité opérationnelle

La signature électronique avancée n'a de valeur que si l'infrastructure qui la produit est elle-même sécurisée. Le présent chapitre expose les mesures de sécurité opérationnelle mises en place ; il est rédigé dans l'esprit des référentiels ISO/IEC 27001, ANSSI et NIST Cybersecurity Framework, et doit pouvoir servir de socle à l'audit indépendant prévu au chapitre 9.

7.1 Hébergement et localisation des données

L'infrastructure de Pixel Sceau est hébergée sur trois serveurs virtuels distincts opérés par DigitalOcean LLC (AS14061), centre de données de **Francfort-sur-le-Main, République fédérale d'Allemagne (Union européenne)**. Le choix de l'Union européenne emporte l'application du Règlement général sur la protection des données (RGPD, règlement UE 2016/679), dont les exigences sont alignées sur celles de la loi ivoirienne n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel et, sur plusieurs points, plus contraignantes. DigitalOcean est certifié SOC 2 Type II et ISO/IEC 27001 ; ses installations de Francfort répondent au niveau Tier 3 de l'Uptime Institute.

La migration de l'infrastructure vers un centre de données situé en Côte d'Ivoire ou dans la zone UEMOA sera envisagée dès qu'une offre éligible (équivalence Tier 3, certifications ISO/IEC 27001, agrément ARTCI pour l'hébergement de données sensibles) sera disponible. À ce stade, aucune offre régionale ne satisfait simultanément ces trois critères.

7.2 Surface d'attaque exposée à l'extérieur

Sur chacun des trois serveurs, seuls les ports strictement nécessaires sont exposés à l'Internet public :

Port	Service	Protocole
80/TCP	HTTP — redirection 301 vers HTTPS	nginx
443/TCP	HTTPS — application	nginx + TLS 1.2 / 1.3
22022/TCP	Administration SSH (par clé exclusivement)	OpenSSH durci

Tous les autres ports (notamment 22, 5432 PostgreSQL, 3306, 6379, 27017, 9200) sont filtrés par le pare-feu UFW avec politique deny incoming par défaut. La translation du

port SSH depuis le port standard 22 vers le port 22022 réduit significativement le bruit des scans automatisés et le volume des tentatives de force brute.

7.3 Protection contre les attaques applicatives

Le service est précédé d'une couche de protection Cloudflare (Web Application Firewall, protection anti-DDoS de couche 3/4 et 7, Bot Fight Mode, filtrage géographique disponible). Au niveau du serveur, nginx applique :

- une politique **HSTS preload** (HTTP Strict Transport Security) avec inclusion des sous-domaines ;
- une politique de sécurité de contenu (**CSP**) restrictive ;
- une politique de référent (Referrer-Policy), une protection contre le détournement de type MIME (X-Content-Type-Options), une protection contre le cadrage abusif (X-Frame-Options) ;
- une limitation de débit (rate limiting) par zone : 30 requêtes par seconde sur l'API générale, 2 par seconde sur les points d'authentification, 5 par minute sur le point d'administration ;
- la résolution réelle de l'adresse du visiteur, traversant les en-têtes CF-Connecting-IP, pour permettre une journalisation et un bannissement fondés sur l'adresse réelle du client.

7.4 Sécurité du système d'exploitation

Les trois serveurs reposent sur Ubuntu Server LTS 24.04 « Noble », mise à jour quotidienne via unattended-upgrades. Un durcissement du noyau est appliqué par sysctl selon les bonnes pratiques NIST et CIS Benchmarks : suppression des redirections ICMP émises, filtrage du chemin de retour (reverse path filter), journalisation des paquets manifestement falsifiés (log_martians), protection contre l'assassinat TIME-WAIT (tcp_rfc1337), restriction de la divulgation des pointeurs noyau (kptr_restrict=2), restriction du traçage de processus (yama.ptrace_scope=2), protection des liens symboliques et physiques.

L'accès administrateur SSH est conditionné à l'authentification par clé Ed25519 (mot de passe désactivé, challenge-response désactivé, ouverture de session par mot de passe interdite y compris pour le compte root). Le service fail2ban assure le bannissement automatique des adresses sources de tentatives d'intrusion répétées, avec quatre filtres actifs : SSH agressif, échecs d'authentification HTTP, scanners de robots nginx, scanners modernes de vulnérabilités (env, .git, phpunit, wp-config, etc.).

7.5 Sécurité de la base de données

La base de données PostgreSQL 16 est accessible exclusivement en boucle locale (`listen_addresses = localhost`). Le pare-feu UFW bloque explicitement le port 5432 en plus de la politique par défaut. Le fichier pg_hba.conf exige l'authentification par peer pour les connexions par socket Unix et par scram-sha-256 pour les connexions TCP locales. Aucun compte ne dispose des droits SUPERUSER en dehors du compte d'administration postgres. Les comptes applicatifs sont strictement limités à leur base et au schéma nécessaire.

7.6 Gestion des secrets

Les éléments confidentiels (clés d'API, mots de passe de base de données, passphrase de la CA Pixel Sceau, clé maître de chiffrement des sauvegardes, clé maître de chiffrement des secrets TOTP) sont :

- conservés exclusivement dans des fichiers .env en permission `600`, détenus par le compte utilisateur du service ;
- jamais inscrits dans le code source ni dans les dépôts de version ;
- copiés et conservés par l'administrateur dans un gestionnaire de mots de passe à coffre chiffré (1Password) ;
- soumis à rotation périodique, et systématiquement rotés en cas de soupçon de compromission ou de départ d'un collaborateur.

Le dépôt du code source fait l'objet d'une analyse régulière par l'outil gitleaks visant à détecter toute fuite accidentelle de secret. La détection d'une telle fuite déclenche une procédure de rotation immédiate.

7.7 Chiffrement des sauvegardes et plan de reprise

Les sauvegardes de base de données et de code sont produites quotidiennement, à 3 heures du matin UTC, et déposées sur le stockage objet Cloudflare R2 en mode chiffré : chaque fichier est chiffré par algorithme **AES-256-CBC** avec dérivation de clé par **PBKDF2**, au moyen d'une clé maître BACKUP_ENCRYPT_KEY de 64 caractères, identique sur les trois serveurs pour permettre la restauration croisée. La clé maître est conservée hors ligne par l'administrateur.

La chaîne complète de reprise a été testée de bout en bout (téléchargement du fichier chiffré, déchiffrement, décompression, restauration sous psql) ; le résultat est consigné dans le journal des opérations.

Limite assumée et roadmap. Le mode AES-256-CBC retenu ne fournit pas d'authentification cryptographique d'intégrité (à la différence d'un mode AEAD type

AES-256-GCM ou ChaCha20-Poly1305). L'intégrité du flux déchiffré est vérifiée implicitement par le contrôle de redondance cyclique du conteneur gzip qui précède le chiffrement : toute modification du ciphertext entraîne un échec de décompression, détecté à la restauration. La migration vers un chiffrement authentifié (AEAD), au moyen de l'outil age (X25519 + ChaCha20-Poly1305) en mode paire de clés, est inscrite à la feuille de route ; elle est subordonnée à la mise en place d'une procédure de gestion de clé X25519 conforme aux exigences d'un audit indépendant.

7.8 Authentification administrateur et gestion des accès

Tout accès à l'interface d'administration de Pixel Sceau requiert une authentification à **deux facteurs stricts** : mot de passe haché par bcrypt et code TOTP au sens de RFC 6238 généré sur un appareil tiers (cf. chapitre 4.1). Le compte d'administrateur fait l'objet d'une limitation de débit spécifique au niveau nginx (cinq tentatives par minute, par adresse réelle) et d'un verrouillage progressif côté applicatif. Les opérations sensibles (révocation de certificat, émission manuelle, accès aux journaux d'audit) sont journalisées dans la table pixel.audit_log et conservées de manière indélébile.

7.9 Surveillance, journalisation, audit

Un surveillant horaire (Sentinel) vérifie sur chacun des trois serveurs : la disponibilité des services applicatifs, l'âge de la dernière sauvegarde, les tentatives de force brute SSH, l'activité des filtres fail2ban, l'état du certificat TLS et la date limite de renouvellement. Toute anomalie déclenche l'envoi d'un courriel d'alerte à l'administrateur.

L'ensemble des opérations cryptographiques (apposition de signature, demande et vérification de second facteur, émission ou révocation de certificat, vérification publique) est journalisé. Le journal est conservé en base sur durée alignée avec la durée de conservation légale des actes notariés.

7.10 Gestion des vulnérabilités et des correctifs

Les dépendances logicielles tierces (bibliothèques Python notamment) sont soumises à un audit mensuel automatisé par l'outil pip-audit, dont le résultat est notifié à l'administrateur par courriel si une vulnérabilité connue est détectée. Le dépôt de code est inscrit au programme Dependabot de GitHub, lequel ouvre automatiquement les demandes de mise à jour des dépendances vulnérables. Le système d'exploitation Ubuntu reçoit ses correctifs de sécurité par unattended-upgrades, conformément aux recommandations de Canonical.

7.11 Référentiels normatifs respectés

Référentiel	Application
ISO/IEC 27001:2022	Cadre général de la gestion de la sécurité de l'information ; objectif de certification à l'horizon de l'agrément qualifié.
NIST Cybersecurity Framework 2.0	Six fonctions (gouvernance, identification, protection, détection, réponse, reprise) appliquées dès la conception.
ANSSI — Guide d'hygiène informatique	Mesures de durcissement OS et réseau ; séparation des comptes ; gestion des accès.
OWASP Top 10:2021	Sécurité applicative ; en-têtes, CSP, validation des entrées, authentification, journalisation.
CIS Benchmarks Ubuntu LTS & PostgreSQL 16	Configuration durcie du système d'exploitation et de la base de données.
RGPD (UE 2016/679)	Applicable du fait de l'hébergement européen ; complète la loi ivoirienne 2013-450.
Loi ivoirienne 2013-450	Loi du 19 juin 2013 relative à la protection des données à caractère personnel.

7.12 Formation et accompagnement des utilisateurs

La sécurité d'un service de signature électronique ne se réduit pas à sa qualité technique : elle dépend tout autant de la bonne compréhension qu'en ont ses utilisateurs. Le concepteur prend les engagements suivants en matière d'accompagnement :

- Mise à disposition, sur `cipixel.com`, d'une documentation utilisateur en français, illustrée, expliquant pas à pas l'enrôlement, l'apposition d'une signature et la vérification d'une signature reçue ;
- Tenue, à la demande de l'Ordre des Notaires de Côte d'Ivoire, de sessions de formation sur la signature électronique avancée, ses garanties et ses limites ; ces sessions ne facturent aucun frais d'inscription ;
- Désignation d'un point de contact unique (`support@cipixel.com`) pour toute question des notaires utilisateurs, avec engagement de réponse sous 24 heures ouvrées ;
- Édition d'une convention d'usage entre Pixel AI SARLU et chaque étude utilisatrice, qui rappelle les bonnes pratiques (confidentialité du second facteur d'authentification, signalement de tout incident, devoir d'information de l'Ordre).

> **Limite assumée.** Aucune certification ISO/IEC 27001 ni audit indépendant n'a, à ce jour, été conduit. Le présent chapitre décrit l'architecture telle qu'elle est construite et exploitée par le concepteur ; sa conformité effective devra être attestée par un cabinet d'audit indépendant dans le cadre de la procédure d'audit préalable à l'agrément ARTCI (cf. chapitre 9).

8. Engagement vis-à-vis de l'Ordre des Notaires

Le concepteur prend, par le présent mémoire, les engagements suivants à l'égard de l'Ordre des Notaires de Côte d'Ivoire :

1. Ne jamais se substituer à l'acte authentique. Pixel Sceau apporte un complément technique de traçabilité ; il ne crée ni n'authentifie aucun droit.
2. Ne diffuser aucun acte signé. Le service n'archive aucun document, ne le transmet à aucun tiers et n'en conserve aucune copie. Seule l'empreinte cryptographique transite par les serveurs, à seule fin de signature.
3. Mettre l'Ordre en capacité de contrôler le service à tout instant, par mise à disposition des journaux d'audit, des spécifications techniques et des codes sources sur demande motivée.
4. Soumettre toute évolution structurelle à l'avis préalable de l'Ordre dès lors que celle-ci serait susceptible d'affecter la valeur probante des signatures déjà délivrées.
5. Garantir la gratuité du service pour les notaires inscrits pendant les douze premiers mois suivant la première signature, à titre de geste de bonne foi et de période de prise en main.

9. Limites assumées et feuille de route d'agrément ARTCI

Le concepteur reconnaît, en toute transparence, les limites du service en son état actuel :

- L'Autorité de Certification Pixel n'est, à ce jour, inscrite ni à l'Adobe Approved Trust List, ni à l'EU Trusted List, ce qui implique une démarche manuelle d'ajout de la CA dans les outils de vérification ;
- La clé privée de l'Autorité de Certification est conservée sur volume serveur chiffré, et non sur module matériel de sécurité ;
- Le point de distribution des listes de révocation et le répondeur OCSP, bien que prévus à l'architecture, ne sont pas encore publiés sous forme accessible au public ;

- Le statut de signature électronique qualifiée au sens ARTCI / UEMOA n'est pas encore obtenu.

Le concepteur prend acte que l'obtention du statut qualifié auprès de l'ARTCI est subordonnée à une procédure d'audit préalable, qui n'est, à la date du présent mémoire, ni demandée ni en cours d'instruction. La séquence prévue, dans l'ordre exact retenu, est la suivante :

1. Immatriculation de la société Pixel AI SARLU au Registre du Commerce d'Abidjan.
2. Acquisition d'un module matériel de sécurité conforme à FIPS 140-2 niveau 3.
3. Publication du point de distribution des listes de révocation et du répondeur OCSP sur `crl.cipixel.com` et `ocsp.cipixel.com`.
4. Constitution du dossier d'audit : documentation des procédures internes (gestion des incidents, gestion des révocations, plan de continuité d'activité, séquestre de clé) et audit de sécurité par un cabinet indépendant ivoirien ou régional.
5. Dépôt officiel de la demande d'agrément, accompagnée du dossier d'audit, auprès de l'ARTCI.
6. Audit ARTCI, prise en compte des remarques et corrections éventuelles.
7. Notification de l'agrément (ou refus motivé) par l'ARTCI.
8. Une fois l'agrément obtenu, inscription à la AATL ou à l'EUTL et passage en mode de signature PAdES B-LTA.

Tant que cette procédure n'est pas menée à son terme, le service ne saurait être présenté comme agréé ni comme en cours d'agrément. Il opère uniquement sous le régime de fait de la signature électronique avancée.

10. Bibliographie normative

Référence	Titre
Loi ivoirienne n° 2013-546	Loi du 30 juillet 2013 portant sur les transactions électroniques en République de Côte d'Ivoire
Accord de Bangui — Annexe I	Brevets d'invention, Organisation Africaine de la Propriété Intellectuelle
ETSI EN 319 142-1	PAdES Baseline Profile (PDF Advanced Electronic Signature)
ETSI EN 319 122-1	CAdES Baseline Profile (Cryptographic Advanced Electronic Signature)
ETSI EN 319 132-1	XAdES Baseline Profile (XML Advanced Electronic Signature)
ETSI EN 319 162-1	ASiC Baseline Profile (Associated Signature Container)
RFC 3161	Internet X.509 Public Key Infrastructure — Time-Stamp Protocol (TSP)
RFC 4226	HOTP — HMAC-Based One-Time Password Algorithm
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile
RFC 5652	Cryptographic Message Syntax (CMS)
RFC 6238	TOTP — Time-Based One-Time Password Algorithm
NIST FIPS 180-4	Secure Hash Standard (SHA-384)
NIST FIPS 186-4	Digital Signature Standard (ECDSA, courbe P-384)
NIST FIPS 140-2 niveau 3	Security Requirements for Cryptographic Modules (cible HSM)
NIST SP 800-63B	Digital Identity Guidelines — Authentication and Lifecycle Management
NIST FIPS 203	Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM, anc. CRYSTALS-Kyber, post-quantique)
NIST FIPS 204	Module-Lattice-Based Digital Signature Standard (ML-DSA, anc. CRYSTALS-Dilithium, post-quantique)
NIST FIPS 205	Stateless Hash-Based Digital Signature Standard (SLH-DSA, anc. SPHINCS+, post-quantique)

RFC 6960	Online Certificate Status Protocol (OCSP)
RFC 6962	Certificate Transparency
OpenTimestamps	Protocole d'horodatage ouvert ancré sur la chaîne Bitcoin

11. Coordonnées du déposant

Élément	Valeur
Nom et prénom	DEMBÉLÉ, Honoré
Adresse postale	10 BP 3333 Abidjan 10, Quartier Cocody, Abidjan, République de Côte d'Ivoire
Adresse courriel	honore@dembele.net · contact@cipixel.com
Site institutionnel	https://cipixel.com
Document de spécifications publiques	https://cipixel.com/sceau-specifications
Vérification publique d'une signature	https://cipixel.com/verifier-signature
Vérification publique d'un horodatage	https://cipixel.com/verifier-horodatage

---

Authenticité du présent mémoire. Le présent document, dans sa version définitive, a été signé électroniquement par le service Pixel Sceau lui-même et son empreinte SHA-256 a été ancrée sur la chaîne Bitcoin par OpenTimestamps. L'empreinte figure en pied de chaque page intérieure ; la preuve d'ancrage est consultable à l'adresse de vérification publique mentionnée ci-dessus.

CONCEPTEUR, DÉPOSANT

Honoré DEMBÉLÉ
Ivoirien, né à Gagnoa
10 BP 3333 Abidjan 10

DATE DU DOCUMENT

Mai 2026 — Abidjan

SIGNATURE ÉLECTRONIQUE

Pixel Sceau (ECDSA P-384, PAdES B-LT, TSA DigiCert, ancrage Bitcoin OpenTimestamps)

Annexe A — Questions souvent posées par les notaires

La présente annexe rassemble, sous forme de questions et de réponses, les interrogations que tout notaire rigoureux est en droit de soulever avant d'envisager l'usage de Pixel Sceau dans son étude. Les réponses sont formulées de manière mesurée, sans visée commerciale ; elles renvoient aux chapitres du mémoire qui en exposent les justifications techniques détaillées.

A.1 — Pourquoi utiliser ce service alors qu'il existe des logiciels libres de signature électronique ?

Il est exact que des bibliothèques libres telles que OpenSSL, GnuPG, pyHanko ou LibreOffice savent produire des signatures cryptographiquement valides. Pixel Sceau s'appuie d'ailleurs lui-même sur la bibliothèque libre pyHanko pour la signature PAdES. Ces bibliothèques sont des outils destinés à des techniciens.

Pixel Sceau est un service. Sa raison d'être tient en ce que la signature électronique d'un acte n'est qu'une étape parmi d'autres : il faut au préalable établir l'identité du signataire, gérer un certificat dans la durée, garantir l'horodatage par un tiers, conserver un journal d'audit, offrir aux tiers vérificateurs une voie de contrôle accessible, et engager la responsabilité de quelqu'un en cas de contestation. Les logiciels libres ne traitent qu'un seul de ces aspects, le calcul cryptographique. Pixel Sceau prend les autres en charge.

A.2 — Qui garantit que le signataire est bien celui qu'il prétend être ?

Chaque signataire Pixel Sceau dispose d'un identifiant à neuf caractères, dit code 09. Cet identifiant n'est délivré qu'après vérification de pièce d'identité et contrôle de cohérence avec les données de l'ONECI, autorité ivoirienne de l'état civil. Le certificat X.509 émis pour le signataire inscrit ce code 09 dans son SerialNumber, lien irrévocable entre la clé cryptographique et l'identité juridique vérifiée du titulaire.

Aucun logiciel libre, par construction, ne procède à cette vérification d'identité. Avec un outil libre, le signataire indique lui-même son nom dans le certificat qu'il génère ; rien n'empêche techniquement de signer sous un nom d'emprunt.

A.3 — Comment un tiers, par exemple un acheteur ou un magistrat, peut-il vérifier une signature sans installer de logiciel particulier ?

Le service expose une voie de vérification publique à l'adresse `cipixel.com/verifier-signature`. Tout tiers y dépose le document signé ; le service retourne, sans conserver

le document, le statut d'authenticité ainsi que le détail des éléments cryptographiques. Aucune installation, aucune compétence technique requise.

Le notaire qui le souhaite peut, en outre, vérifier la signature au moyen d'Adobe Acrobat Reader, d'openssl, de pyhanko ou de l'opentimestamps-client, selon les procédures rappelées au chapitre 5 du présent mémoire.

A.4 — Les actes signés sont-ils conservés sur les serveurs du prestataire ?

Non. Le document signé transite par les serveurs du prestataire le temps strictement nécessaire à l'apposition de la signature, puis n'y est plus conservé. Seule l'empreinte cryptographique SHA-256 du document signé est gardée, à des fins de traçabilité et de vérification ultérieure. L'acte lui-même demeure chez le notaire, conforme aux exigences du secret professionnel.

A.5 — Que se passe-t-il si le prestataire cesse son activité ?

Les documents antérieurement signés conservent leur pleine valeur probante :

1. Le document signé est auto-portant : il embarque la signature, le certificat de signataire, l'horodatage RFC 3161 et les éléments de validation. Sa vérification ne dépend d'aucun serveur Pixel.
2. L'empreinte du document est inscrite sur la chaîne Bitcoin. Cette preuve indépendante survit à la disparition de tout intermédiaire commercial.
3. L'autorité de certification Pixel sera, à l'horizon de l'agrément qualifié, déposée auprès d'un tiers séquestre de confiance, garantissant la pérennité au-delà de la durée de vie du prestataire.

A.6 — En cas de contestation portée devant les tribunaux, qui est l'interlocuteur du juge ?

Pixel AI SARLU est l'interlocuteur unique en cas de litige. La société, de droit ivoirien et soumise au régime OHADA de la SARL unipersonnelle, porte la responsabilité civile et juridique du service dans la limite de son capital social. Aucune personne physique, fondateur ou collaborateur, n'engage à titre personnel sa responsabilité à raison du fonctionnement normal du service.

La société est conçue dès l'origine pour **survivre à son fondateur** : ses statuts prévoient le remplacement du gérant, la continuité de la fourniture du service, la conservation des éléments cryptographiques par tiers séquestre, et la transmission de la fonction d'opérateur sans rupture pour les notaires utilisateurs. Le chapitre 6.4 du présent mémoire détaille ces dispositions.

A.7 — L'étude conserve-t-elle la trace de ses propres opérations de signature ?

Oui. Le service tient un journal d'audit horodaté de chaque opération : émission ou révocation de certificat, demande et validation d'OTP, vérification du second facteur d'authentification, apposition de signature, vérification ultérieure. Ce journal est consultable à la demande motivée du signataire, de son étude, de l'Ordre des Notaires ou de l'autorité judiciaire. Sa durée de conservation est alignée sur la durée légale de conservation des actes notariés.

A.8 — Plusieurs personnes peuvent-elles signer un même acte ?

Oui. Le service permet l'apposition de plusieurs signatures successives sur le même document, chacune avec sa propre cartouche visible portant le nom du signataire, son identifiant Pixel et la date d'apposition. L'ordre des signatures est préservé et figure dans la structure cryptographique du document. Cette fonctionnalité couvre les actes nécessitant la signature du notaire, des parties, et le cas échéant de témoins ou de mandataires.

A.9 — Le notaire est-il facturé à chaque signature ?

Non. Le service est, à ce jour, offert gratuitement aux notaires inscrits durant les douze premiers mois suivant leur première signature, à titre de geste de bonne foi et de période de prise en main, conformément à l'engagement exposé au chapitre 8 du présent mémoire. Le modèle économique à long terme, qui demeure à définir, ne sera arrêté qu'à l'issue d'une concertation avec l'Ordre des Notaires de Côte d'Ivoire.

A.10 — Ce service prétend-il se substituer à l'écrit authentique notarié ?

Aucunement. Pixel Sceau apporte un complément technique de traçabilité au document numérique. Il n'authentifie aucun droit, n'établit aucun fait juridique, ne saurait remplacer la qualité d'officier ministériel du notaire ni la valeur particulière conférée par la loi à l'acte qu'il reçoit. L'usage de Pixel Sceau s'inscrit en accompagnement de la pratique notariale traditionnelle, en aucun cas en concurrence avec elle.