RAPPORT D'AUDIT INTERNE DE PRÉ-CONFORMITÉ

Référentiel : Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI)

Pixel Sceau

Service de signature électronique avancée
en cours de qualification ARTCI

ISO/IEC 27001:2022 | NIST CSF 2.0 | ANSSI Guide d'hygiène

eIDAS REGL 910/2014 | RGS v2.0 | ETSI EN 319 401

OWASP ASVS 4.0

Version 1.1 — 24 mai 2026 (intègre la référence d'horodatage de la v1.0)

Périmètre : infrastructure de production Pixel Sceau

Conduite : audit interne par le concepteur du système

Entité auditée : Pixel AI SARLU (en cours d'immatriculation, Abidjan, Côte d'Ivoire)
Auditeur : Honoré DEMBÉLÉ, fondateur et concepteur du système
Service audité : Pixel Sceau (signature électronique, ancrage Bitcoin OpenTimestamps)
URL de production : `https://cipixel.com/signer` et `https://api.pixelhelix.net/api/v1/identity/v1/sceau/*`

Document destiné à l'ARTCI dans le cadre de la procédure de demande d'agrément en tant que Prestataire de Services de Confiance pour la signature électronique.
Toute remarque ou recommandation de l'auditeur ARTCI est traitée comme une obligation à atteindre.

Sommaire

1. Identification et périmètre

1.1 Identification de l'entité auditée

Élément	Valeur
Dénomination	Pixel AI SARLU
Forme juridique	Société à Responsabilité Limitée Unipersonnelle (régime OHADA)
Statut d'immatriculation	En cours auprès du Centre de Promotion des Investissements en Côte d'Ivoire (CEPICI)
Adresse de production	Abidjan, Côte d'Ivoire
Représentant légal	Honoré DEMBÉLÉ, fondateur et associé unique
Service objet de l'audit	Pixel Sceau — signature électronique avancée avec ancrage public sur la blockchain Bitcoin (via OpenTimestamps)
Niveau visé	Signature électronique avancée puis qualifiée, au sens du Règlement eIDAS 910/2014 et de la législation ivoirienne en transposition
Statut d'agrément ARTCI	Non agréé — la présente demande d'audit est l'étape préparatoire à la demande formelle

1.2 Périmètre technique et fonctionnel

L'audit couvre l'ensemble de l'infrastructure qui héberge ou supporte Pixel Sceau au 24 mai 2026 :

Composant	Identification	Description
VPS de production	165.22.75.36 (DigitalOcean, Francfort, Allemagne)	Héberge le service Pixel Identity Hub (port localhost 8021) qui inclut Pixel Sceau, ainsi que les services Helix, FonciTrace, Genesis Data (tous backend localhost, exposés via nginx reverse proxy)
CDN et pare-feu applicatif	Cloudflare (compte `c502e9fca073...`)	Proxy orange sur toutes les zones de production, TLS edge, WAF managed rules, Bot Fight Mode
Stockage objet	Cloudflare R2	Sauvegardes chiffrées des bases de données
DNS	Cloudflare DNS	9 zones gérées (cipixel.com, pixelhelix.net, foncitrace.com, genesisdata.org, pixelakwaba.com, bwa-sacre.org, mediafrika.org, mediafrika.com, dembele.net)
Mail transactionnel	Brevo (compte sigma sarl)	API REST pour envoi mail/SMS, IP whitelist active
Horodatage qualifié RFC 3161	DigiCert Timestamp Responder	Horodatage cryptographique de chaque signature PAdES émise
Ancrage public	Réseau Bitcoin via OpenTimestamps	Preuve d'antériorité publique et décentralisée
Poste d'administration	Apple iMac 24" (M4, macOS Sequoia 15.6)	Unique poste autorisé à administrer la production. FileVault activé. SSH par clé chiffrée. Firewall macOS State=2 (bloque tout entrant non essentiel) + mode furtif.

Sont **hors périmètre** du présent audit (mais documentés pour information) :

- Les VPS adjacents `167.99.245.100` (services BWA, FonciTrace legacy) et `138.68.87.235` (Akwaba) qui ne supportent pas Pixel Sceau directement mais partagent le même standard de durcissement.
- Les services en projet (FonciTrace foncier OAPI, Akwaba VTC, Genesis éducation) qui consommeront Pixel Sceau ultérieurement.

1.3 Méthodologie d'audit

L'audit a été conduit selon une approche en quatre phases complémentaires :

1. **Audit boîte blanche** : examen direct du code source FastAPI (Python 3.12), des configurations système (nginx, systemd, sysctl, UFW, sshd_config, auditd), des bases de données PostgreSQL 16, et des journaux applicatifs sur le VPS de production.
2. **Audit offensif boîte noire externe** : depuis le poste d'administration, exécution de `nmap` avec détection de versions sur les IPs publiques, `dig` exhaustif sur les 9 zones DNS avec énumération de 25 sous-domaines courants, `curl` sur les chemins sensibles

connus (`/.git`, `/.env`, `/admin`, `/docs`, `/openapi.json`), `sslscan` sur les origins, recherche Certificate Transparency (crt.sh).

3. **Audit normatif** : application des contrôles ISO/IEC 27001:2022 Annex A (93 contrôles), NIST Cybersecurity Framework 2.0 (6 fonctions), Guide d'hygiène informatique ANSSI (42 règles), OWASP Application Security Verification Standard 4.0 (Level 2).
4. **Audit outillé** : `Lynis audit system` (CISOfy), `rkhunter --check`, `chkrootkit`, `aide --check`, vérification `apt list --upgradable` pour les CVE actives.

1.4 Référentiels normatifs appliqués

ISO/IEC 27001:2022 — Système de management de la sécurité de l'information (SMSI)

NIST CSF 2.0 — Cybersecurity Framework, fonctions Govern, Identify, Protect, Detect, Respond, Recover

ANSSI — Guide d'hygiène informatique — Agence nationale française de la sécurité des systèmes d'information, 42 règles de base

OWASP ASVS 4.0 — Application Security Verification Standard, niveau 2 (Standard)

Règlement (UE) n° 910/2014 eIDAS — Identification électronique et services de confiance pour les transactions électroniques (transposition ivoirienne en cours)

RGS v2.0 — Référentiel Général de Sécurité (ANSSI France, applicable par analogie en attente d'un référentiel ARTCI publié)

ETSI EN 319 401 — Exigences générales relatives aux prestataires de services de confiance

ETSI EN 319 411-1 et 411-2 — Politiques de certification pour les prestataires émettant des certificats

ETSI EN 319 421 — Exigences pour les prestataires de services de confiance émettant des horodatages électroniques

ETSI EN 319 442 — Profils relatifs à la signature électronique PAdES (PDF Advanced Electronic Signatures)

RFC 3161 / RFC 5816 — Time-Stamp Protocol (TSP)

RFC 5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile

RFC 6238 — TOTP: Time-Based One-Time Password Algorithm

RFC 6960 — X.509 Internet Public Key Infrastructure Online Certificate Status Protocol — OCSP

NIST FIPS 186-4 — Digital Signature Standard (DSS), cubes elliptiques NIST P-384

NIST FIPS 180-4 — Secure Hash Standard (SHA-256, SHA-384)

NIST FIPS 203/204/205 — Post-quantum cryptography (ML-KEM, ML-DSA, SLH-DSA) — pour la roadmap

2. Résumé exécutif

2.1 Score de maturité global

75 / 100

Indice de durcissement Lynis (CISOfy) — cible à 12 mois : 85+

75	93/93	42/42	14
Lynis hardening_index	Contrôles ISO 27001 évalués	Règles ANSSI évaluées	Findings ouverts

2.2 Synthèse des findings

Sévérité	Nombre	Description
CRIT — Critique	0	Aucun finding critique ouvert au moment de la clôture de l'audit. Quatre findings initialement critiques (détaillés ci-après) ont été corrigés en cours d'audit.
HIGH — Élevé	3	Trois engagements à honorer avant l'audience formelle d'agrément (plan de réponse à incident formel, pentest tiers, formalisation rotation secrets).
MED — Moyen	5	Améliorations structurelles planifiées dans les 12 mois (HSM, SIEM Wazuh, migration AEAD backups, CrowdSec, multi-VPS HA).
LOW — Faible	4	Optimisations cosmétiques ou de défense en profondeur.
INFO — Informatif	2	Notes contextuelles sans impact opérationnel direct.

Findings initialement critiques corrigés au cours de l'audit (transparence totale)

Référence	Description	Action corrective	Vérification
F-001	Fuite du dépôt Git complet de cipixel.com via `/.git/config` publiquement accessible	Création de `.assetsignore` Cloudflare Workers et redéploiement	`curl -sI https://cipixel.com/.git/config` → HTTP 404 ✓
F-002	Cartographie Swagger UI de l'API Pixel Identity exposée publiquement (`/api/v1/identity/v1/docs`)	Configuration `docs_url=None, redoc_url=None, openapi_url=None` sur le constructeur FastAPI	Tous les endpoints `/docs` , `/openapi.json` , `/redoc` → HTTP 404 ✓
F-003	Fuite de l'IP origin du serveur de production via la zone DNS `mediafrika.org` (A records non proxifiés)	Suppression manuelle de 9 enregistrements DNS dans le tableau de bord Cloudflare et désactivation d'Email Routing	`dig +short A mediafrika.org @1.1.1.1` → vide sur trois résolveurs publics ✓
F-004	Clé SSH du poste d'administration sans passphrase, donnant un accès root direct aux trois VPS de production en cas de vol du poste	Application d'une passphrase aléatoire de 32 caractères, stockée dans le gestionnaire d'identifiants natif macOS Sequoia (Mots de passe / iCloud Keychain), chargement automatique via la directive `UseKeychain yes` dans `~/.ssh/config`	`ssh-keygen -y -P "" -f ~/.ssh/id_ed25519` → erreur de passphrase ✓

2.3 Recommandations prioritaires

Trois recommandations doivent être adressées avant la tenue de l'audience d'agrément :

1. **Formalisation écrite du plan de réponse à incident**. Procédure actuelle orale documentée mentalement par le concepteur. Engagement : rédaction d'un document IR de 4 à 6 pages couvrant isolation, snapshot, restauration, rotation des secrets, notification de l'ARTCI sous 24 à 72 heures selon la nature de l'incident.
2. **Commande d'un test d'intrusion par un cabinet certifié**. Aucun pentest tiers n'a été conduit à ce jour. Engagement : pentest dans les six mois suivant l'octroi de l'agrément avancé, avant tout déploiement qualifié. Le rapport sera transmis à l'ARTCI.
3. **Formalisation des procédures de rotation des secrets**. La rotation est aujourd'hui exécutée manuellement à la demande. Engagement : rédaction d'un runbook `rotate-secrets.md` couvrant les API tierces (Brevo, PayTech, Anthropic, R2, etc.) avec une

cadence trimestrielle et un script `rotate-brevo-keys.sh` qui automatise la propagation dans les quatre fichiers `.env` et le redémarrage des quatre services concernés.

3. Architecture et infrastructure

3.1 Architecture réseau

L'architecture suit un modèle de défense en profondeur (defense in depth) à trois couches :

1. **Frontal Cloudflare** (proxy orange) : TLS 1.2 et 1.3, ciphers Mozilla Intermediate, WAF managed rules, Bot Fight Mode, protection DDoS L7 automatique. Les adresses IP origin sont volontairement non publiées dans le DNS.
2. **nginx en reverse proxy** sur l'origin : terminaison TLS secondaire (Mozilla Intermediate également côté origin pour défense en profondeur), application de la limitation de débit (six zones distinctes), routage vers les bons backends, en-têtes HTTP de sécurité, refus de SNI inconnu (`ssl_reject_handshake on` et `return 444` sur le default server).
3. **Backends FastAPI** sur `127.0.0.1` : aucun service backend n'écoute sur une interface publique. Chaque service est isolé par utilisateur système dédié (`pixelai`, `foncitrace`, `helix`, etc.) avec ses propres permissions de système de fichiers.

Inventaire des services en écoute sur le VPS de production :

```
$ ss -tlnp | grep LISTEN
0.0.0.0:22022    sshd                       SSH durci (cf. §3.3)
0.0.0.0:80       nginx                      → redirige vers HTTPS
0.0.0.0:443      nginx                      → reverse proxy (cf. §3.4)
127.0.0.1:5432   postgres                   Base de données, localhost only
127.0.0.1:8003   foncitrace-api             FastAPI uvicorn
127.0.0.1:8004   foncitrace-rules           FastAPI uvicorn
127.0.0.1:8005   foncitrace-paystack        FastAPI uvicorn
127.0.0.1:8006   foncitrace-saas            FastAPI gunicorn
127.0.0.1:8007   genesisdata-api            FastAPI uvicorn
127.0.0.1:8020   helix-ai-api               FastAPI uvicorn
127.0.0.1:8021   pixel-ai-identity (Sceau)  FastAPI uvicorn 2 workers
0.0.0.0:25       postfix                    Mail sortant local (UFW bloque entrant)
```

3.2 Pare-feu et filtrage

Le pare-feu Ubuntu UFW est actif sur le VPS de production. Configuration vérifiée :

```
$ ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)

To                         Action      From
--                         ------      ----
80/tcp                     ALLOW IN    Anywhere       # HTTP
443/tcp                    ALLOW IN    Anywhere       # HTTPS
22022/tcp                  ALLOW IN    Anywhere       # SSH alt
5432                       DENY IN     Anywhere       # PostgreSQL refusé externe
```

Vérification offensive depuis l'extérieur via `nmap` sur l'ensemble des ports privilégiés et des services courants : seuls les trois ports 80, 443 et 22022 sont visibles. Tous les autres ports (25, 465, 587, 993, 995, 5432, 8000-8100) sont `filtered`, c'est-à-dire silencieusement bloqués par UFW.

Le service fail2ban est actif avec quatre prisons : `sshd`, `nginx-botsearch`, `nginx-http-auth`, `nginx-modern-scanners`.

3.3 Accès distant SSH

OpenSSH 9.6p1 (avec backports de sécurité Canonical, version `9.6p1-3ubuntu13.16` qui intègre le correctif USN-6884-1 pour CVE-2024-6387 « regreSSHion »). Configuration durcie dans `/etc/ssh/sshd_config.d/99-pixel-hardening.conf` :

```
PermitRootLogin without-password    # clé uniquement, jamais mot de passe
PasswordAuthentication no
PermitEmptyPasswords no
MaxAuthTries 3
X11Forwarding no
DebianBanner no
LoginGraceTime 30
ClientAliveInterval 300
ClientAliveCountMax 2
MACs hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,umac-128-etm@openssh.com
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com
KexAlgorithms sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-
sha256@libssh.org
Banner /etc/ssh/banner.txt
```

Le KEX `sntrup761x25519-sha512` est **post-quantique hybride** : il combine la primitive classique Curve25519 avec le candidat NTRU Prime pour résister à un futur ordinateur quantique cryptographiquement utile.

Le port standard 22 n'est pas utilisé ; SSH écoute uniquement sur le port alternatif 22022, ce qui réduit drastiquement le bruit de fond des tentatives de force brute généralistes.

3.4 Chiffrement TLS

La configuration TLS suit le profil Mozilla Intermediate. Vérification par `sslscan` depuis l'extérieur sur l'origin (en contournant Cloudflare) :

```
SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled       ← refusé
TLSv1.1   disabled       ← refusé
TLSv1.2   enabled
TLSv1.3   enabled

TLSv1.3 ciphers:
  TLS_AES_256_GCM_SHA384
  TLS_CHACHA20_POLY1305_SHA256
  TLS_AES_128_GCM_SHA256

TLSv1.2 ciphers (AEAD only) :
  ECDHE-ECDSA-CHACHA20-POLY1305
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-ECDSA-AES128-GCM-SHA256

Key Exchange Groups: x25519, secp256r1, secp384r1, secp521r1
Heartbleed: not vulnerable
```

OCSP stapling est activé (`ssl_stapling on`) avec un résolveur DNS dédié. Les session tickets sont désactivés (`ssl_session_tickets off`) pour préserver la perfect forward secrecy.

3.5 Durcissement système

Paramètres noyau appliqués via `/etc/sysctl.d/99-pixel-security.conf` et `/etc/sysctl.d/99-pixel-no-coredump.conf` :

Paramètre	Valeur	Objectif
`vm.swappiness`	1	Limite drastiquement l'écriture de pages mémoire vers le swap, réduisant le risque de fuite de secrets en clair sur disque
`kernel.randomize_va_space`	2	ASLR complet (Address Space Layout Randomization)
`kernel.kptr_restrict`	2	Masque les pointeurs noyau dans `/proc`
`kernel.dmesg_restrict`	1	Restreint la lecture de `dmesg` aux utilisateurs privilégiés
`kernel.core_pattern`	`|/bin/false`	Désactive l'écriture des core dumps (qui peuvent contenir des secrets en mémoire)
`fs.suid_dumpable`	0	Refuse les core dumps pour les processus suid
`fs.protected_symlinks`	1	Anti-TOCTOU (Time-of-check to time-of-use) sur liens symboliques
`fs.protected_hardlinks`	1	Idem pour liens durs
`net.ipv4.tcp_syncookies`	1	Anti-SYN flood
`net.ipv4.conf.all.rp_filter`	1	Anti-spoofing strict
`net.ipv4.conf.all.accept_redirects`	0	Refuse ICMP redirects
`net.ipv4.icmp_echo_ignore_broadcasts`	1	Anti smurf attack
`net.ipv4.ip_forward`	0	Le serveur n'est pas un routeur

Modules noyau désactivés via `/etc/modprobe.d/disable-unused-net.conf` : `dccp`, `sctp`, `rds`, `tipc` (protocoles réseau non utilisés, recommandation Lynis NETW-3200).

`UMASK 027` dans `/etc/login.defs` (recommandation Lynis AUTH-9328). Politique d'âge de mot de passe activée : `PASS_MAX_DAYS 90`, `PASS_MIN_DAYS 1`, `PASS_WARN_AGE 14`.

Core dumps désactivés au niveau utilisateur via `/etc/security/limits.d/99-disable-coredump.conf` (`* hard core 0`).

4. Sécurité applicative

4.1 Architecture FastAPI

Sept services FastAPI tournent en parallèle sur le VPS de production, sous systemd. Chaque service écoute sur l'interface localhost et est exposé sélectivement via nginx :

Service systemd	Port localhost	Worker	Service
`pixel-ai-identity`	8021	uvicorn 2 workers	Pixel Identity Hub (Sceau, Horodatage, 09-codes, TOTP)
`foncitrace-api`	8003	uvicorn	FonciTrace API (JP/JV/JU)
`foncitrace-rules`	8004	uvicorn	FonciTrace Rule Engine (142 règles métier)
`foncitrace-paystack`	8005	uvicorn	FonciTrace passerelle paiement
`foncitrace-saas`	8006	gunicorn 5 workers	FonciTrace front SaaS
`genesisdata-api`	8007	uvicorn	Genesis Data API (éducation)
`helix-ai-api`	8020	uvicorn	Helix.AI API (santé)

4.2 Authentification

Pixel Identity (qui inclut Pixel Sceau) implémente une authentification à deux niveaux complémentaires :

- **Niveau application** : middleware `auth_app` exigeant un header `X-Identity-API-Key` d'au moins 32 caractères sur l'ensemble des routes. Sans ce header, toute requête est rejetée par HTTP 401.
- **Niveau administration** : décorateur `Depends(require_super_admin)` appliqué aux endpoints `/admin/*`. Sans le rôle super-admin valide, accès refusé.

Vérification offensive depuis l'extérieur sur trois endpoints admin :

```
$ curl -sI https://api.pixelhelix.net/api/v1/identity/v1/admin/audit-log
HTTP/2 401 Unauthorized

$ curl -sI https://api.pixelhelix.net/api/v1/identity/v1/admin/employes
HTTP/2 401 Unauthorized

$ curl -sI https://api.pixelhelix.net/api/v1/identity/v1/admin/codes
HTTP/2 401 Unauthorized
```

L'authentification utilisateur final pour signer un document Pixel Sceau combine :

1. Code 09 (identifiant Pixel à vie, format `09A-XXXXXXXX-X`),
2. TOTP RFC 6238 (préféré) ou OTP email à usage unique (fallback de secours),
3. Validation de la signature serveur ECDSA P-384 sur le PDF cible.

4.3 Limitation de débit (rate limiting)

Six zones `limit_req_zone` définies dans la configuration nginx :

Zone	Débit	Cible	Objectif
`api_limit`	30 r/s	`/api-ft/*`	API FonciTrace
`saas_limit`	30 r/s	`/api-saas/*`	FonciTrace SaaS
`paystack_limit`	10 r/s	`/api-paystack/*`	Webhooks paiement
`pixel_api`	30 r/s	`/api/v1/identity/v1/*`	API Pixel générique
`pixel_otp`	**2 r/s**	Envoi OTP email/SMS	Anti-flood de la facture SMS et des coûts mail
`pixel_pages`	10 r/s	Pages publiques	Anti-scraping
`pixel_login_v2`	**5 r/min**	Login admin Pixel	Anti-brute force, IP réelle Cloudflare

La zone `pixel_login_v2` à 5 requêtes par minute rend mathématiquement infaisable le brute force d'un mot de passe administrateur fort.

4.4 Validation des webhooks

Les webhooks reçus des passerelles de paiement sont validés cryptographiquement avant traitement :

Webhook	Provider	Méthode de validation
`/paytech/webhook`	PayTech (Sénégal)	Vérification de `SHA256(api_key)` et `SHA256(api_secret)` contre les valeurs locales (protocole imposé par PayTech, documenté `https://paytech.sn/documentation`). HTTP 401 en cas de mismatch.
`/webhook/fedapay`	FedaPay	Validation HMAC du payload via la variable `MF_FEDAPAY_WEBHOOK_SECRET`
`/webhook/pawapay/{deposit,payout,refund}`	PawaPay	Validation selon le protocole PawaPay

L'idempotence applicative côté base de données (un `ref_command` ne peut être traité qu'une seule fois) constitue une protection complémentaire contre les attaques par rejeu.

4.5 Documentation API en production

Tous les services FastAPI sont configurés pour **désactiver la documentation OpenAPI en production** :

```
app = FastAPI(
    ...,
    docs_url=None,       # Swagger UI désactivé
    redoc_url=None,      # ReDoc désactivé
    openapi_url=None,    # /openapi.json désactivé
)
```

Vérification sur les quatre services exposés publiquement :

```
$ for url in \
    https://api.pixelhelix.net/api/v1/identity/v1/docs \
    https://api.pixelhelix.net/api/v1/identity/v1/openapi.json \
    https://foncitrace.com/api-ft/docs \
    https://foncitrace.com/api-saas/docs ; do
    echo "$url → HTTP $(curl -sk -o /dev/null -w '%{http_code}' --max-time 5 $url)"
done

→ HTTP 404 (les 4)
```

5. Cryptographie

5.1 Autorité de certification interne

Une autorité de certification dédiée Pixel Sceau a été émise et est utilisée pour signer les certificats individuels des utilisateurs :

Caractéristique	Valeur
Algorithme de clé	RSA 3072 bits
Algorithme de signature	SHA-384 with RSA
Durée de validité	10 ans (renouvellement programmé année 8)
Format de stockage	PKCS#8 chiffré par AES (passphrase dans variable `SCEAU_KEY_PASSPHRASE`)
Chemin disque	`/opt/pixel-ai-identity/api/sceau_ca/ca_key_enc.pem`
Permissions filesystem	`0600`, propriétaire `pixelai:pixelai`
Surveillance	auditd watch (clé `sceau_ca` dans `/etc/audit/rules.d/pixel-sceau.rules`) — toute lecture ou modification est journalisée

5.2 Certificats utilisateurs

Chaque utilisateur authentifié reçoit un certificat individuel signé par la CA Pixel Sceau, valable deux ans, contenant son code 09 dans le champ Subject :

Caractéristique	Valeur
Algorithme de clé	ECDSA sur courbe NIST P-384 (secp384r1)
Algorithme de signature	SHA-384 with ECDSA
Sécurité équivalente	≈ RSA-7680 bits
Conformité	NIST FIPS 186-4, recommandé NIST pour usage post-2025
Durée de validité	2 ans
Sujet	`CN=<Nom Prénoms>, serialNumber=<code 09>`
Stockage	Base de données PostgreSQL `pixel.sceau_certificats`, clé privée chiffrée

5.3 Signature PAdES-B-LT

Chaque signature appliquée à un document PDF respecte le profil PAdES-B-LT (Long-Term Validation) selon le standard ETSI EN 319 142-1 :

Élément	Valeur
Subfilter	`ETSI.CAdES.detached`
Algorithme de hash	SHA-384
Validation context	trust_roots = CA Pixel + bundle Mozilla (via le paquet certifi)
DSS (Document Security Store)	embed_validation_info=True (intègre OCSP responses et CRL dans le PDF)
Bibliothèque	pyHanko (Python, projet maintenu activement, audit communautaire)

Toute signature peut être vérifiée hors ligne, des années après son émission, sans dépendance à un service tiers, grâce à l'intégration des informations de révocation dans le DSS.

5.4 Horodatage RFC 3161

Chaque signature PAdES émise est horodatée par une Autorité d'Horodatage qualifiée externe :

Élément	Valeur
TSA	DigiCert Timestamp Responder 2025
URL	`http://timestamp.digicert.com`
Algorithme	SHA-384 RSA-4096
Confiance	CA DigiCert présente dans le bundle Mozilla (et donc dans la majorité des magasins de confiance OS et navigateurs)
Conformité	RFC 3161 (Time-Stamp Protocol), RFC 5816 (TSA-policy)

5.5 Authentification forte TOTP RFC 6238

Pixel Sceau supporte l'authentification à second facteur via TOTP (Time-based One-Time Password) :

Caractéristique	Valeur
Algorithme	HMAC-SHA-1 (RFC 6238 standard)
Longueur du code	6 chiffres
Fenêtre temporelle	30 secondes
Tolérance dérive horloge	±1 fenêtre (acceptation t-30s, t, t+30s)
Anti-replay	`DELETE` de `last_used` en base après vérification réussie
Lock progressif	5 échecs → 15 min, 10 échecs → 1 h, 20 échecs → 24 h
Stockage du secret	Fernet (AES-128-CBC + HMAC-SHA-256) chiffré par `TOTP_MASTER_KEY`
Compatibilité applications	Google Authenticator, Authy, 1Password, Microsoft Authenticator
Audit log	Table `pixel.totp_audit_log` — toute tentative est journalisée (succès/échec/lock)

5.6 Ancrage Bitcoin OpenTimestamps

L'empreinte cryptographique SHA-256 de chaque document signé est soumise au réseau OpenTimestamps, qui agrège les preuves et les ancre sur la blockchain Bitcoin (en moyenne dans les 1 à 2 heures suivant la signature). Cela fournit une **preuve d'antériorité publique, décentralisée et indépendante** de Pixel AI SARLU.

Avantages :

- Vérifiable par n'importe quel tiers, sans confiance préalable en Pixel
- Persistant tant que Bitcoin existe
- Coût marginal proche de zéro (mutualisation des hashes en arbre de Merkle)
- Indépendant de la survie de Pixel AI SARLU

6. Surveillance et journalisation

6.1 auditd (journal d'audit POSIX)

Le démon `auditd` est actif sur le VPS de production avec quatorze règles couvrant l'ensemble des fichiers sensibles. Configuration dans `/etc/audit/rules.d/pixel-sceau.rules` :

```
# CA Sceau
-w /opt/pixel-ai-identity/api/sceau_ca/ -p rwa -k sceau_ca

# Secrets applicatifs
-w /opt/pixel-ai-identity/api/.env -p rwa -k pixel_env
-w /opt/helix-ai/api/.env -p rwa -k helix_env
-w /opt/foncitrace/api/.env -p rwa -k foncitrace_env

# Configuration sensible
-w /etc/ssh/sshd_config -p rwa -k sshd_config
-w /etc/sudoers -p rwa -k sudoers
-w /etc/sudoers.d/ -p rwa -k sudoers
-w /root/.ssh/authorized_keys -p rwa -k ssh_keys_root

# Persistance attaquant
-w /etc/cron.d/ -p wa -k cron_changes
-w /etc/crontab -p wa -k cron_changes
-w /etc/systemd/system/ -p wa -k systemd_changes

# Comptes utilisateurs
-w /etc/passwd -p wa -k user_modifications
-w /etc/shadow -p wa -k user_modifications
-w /etc/group -p wa -k user_modifications

# Modules noyau
-a always,exit -F arch=b64 -S init_module -S delete_module -k kernel_modules
```

Vérification : `auditctl -l` retourne les 14 règles actives. Les événements sont stockés dans `/var/log/audit/audit.log`, accessibles via `ausearch` et `aureport`.

6.2 Sauvegardes

Onze tâches cron de sauvegarde sont actives, couvrant chaque application en local et en distant (Cloudflare R2) :

```
0 3 * * *   /root/backup_foncitrace.sh           # Local
0 3 * * *   /root/backup_pixel_ai.sh             # Local
15 3 * * *  /root/backup_helix_ai.sh             # Local
30 3 * * *  /root/backup_genesisdata.sh          # Local
0 3 * * *   /opt/foncitrace/saas/.../backup_db_r2.py  # Cloud R2
30 3 * * *  /root/backup_r2.sh                   # Cloud R2
45 3 * * *  /root/backup_r2_helix_ai.sh          # Cloud R2
50 3 * * *  /root/backup_r2_genesisdata.sh       # Cloud R2
55 3 * * *  /root/backup_r2_pixel_ai.sh          # Cloud R2
0 4 * * 1   /root/backup_secrets_vault.sh vps2   # Coffre secrets hebdomadaire
0 5 * * *   /root/check_backup_r2_age.sh         # Vérification fraîcheur R2
```

Tous les fichiers de sauvegarde sont chiffrés symétriquement avant transmission à R2 (algorithme AES-256-CBC + PBKDF2-HMAC-SHA-256, 100 000 itérations, passphrase dans variable d'environnement). Migration vers un mode AEAD (X25519 + ChaCha20-Poly1305 via l'outil `age`) en roadmap (cf. F-006).

6.3 Détection d'intrusion

Plusieurs outils complémentaires :

- **fail2ban** : 4 prisons actives (sshd, nginx-botsearch, nginx-http-auth, nginx-modern-scanners) qui bannissent l'IP après seuils configurés
- **rkhunter** : vérification rootkit, exécution manuelle + planification cron hebdomadaire
- **chkrootkit** : second avis rootkit
- **AIDE** : Advanced Intrusion Detection Environment, baseline initiale + vérification quotidienne par cron
- **auditd** : journal d'audit POSIX (cf. §6.1)
- **GoAccess** : rapport HTML quotidien d'analyse des logs nginx, rétention 30 jours
- **Lynis** : audit système périodique (CISOfy), index actuel 75/100

Système de détection d'intrusion réseau (NIDS, type Suricata ou Snort) **non déployé** à ce jour. Voir finding F-010 et roadmap.

7. Exposition extérieure

7.1 DNS et nom de domaine

Neuf zones DNS sont gérées via Cloudflare. Audit exhaustif au moyen de `dig` sur 25 sous-domaines courants (www, api, admin, app, dev, staging, beta, test, old, legacy, backup, vpn, db, api1, api2, api-dev, mail, webmail, smtp, imap, pop, ftp, m, mobile, cdn) :

Zone	Résolution A records	Risque IP origin
`cipixel.com`	Cloudflare 104.21.x / 172.67.x	Aucun
`pixelhelix.net` + sous-domaines	Cloudflare 104.21.x / 172.67.x	Aucun
`foncitrace.com` + sous-domaines	Cloudflare 104.21.x / 172.67.x	Aucun
`genesisdata.org` + sous-domaines	Cloudflare 104.21.x / 172.67.x	Aucun
`bwa-sacre.org` + sous-domaines	Cloudflare 104.26.x / 172.67.x	Aucun
`pixelakwaba.com` + sous-domaines	Cloudflare 104.21.x / 172.67.x	Aucun
`mediafrika.org`	Vide (zone nettoyée le 24 mai 2026)	Aucun
`mediafrika.com`	Vide	Aucun
`dembele.net`	Google Workspace (`ghs.google.com`)	Aucun

7.2 CDN et pare-feu applicatif (Cloudflare)

Service Cloudflare	État
Proxy orange (proxified)	Activé sur toutes les zones de production
SSL/TLS Edge Certificates	Universal SSL, renouvellement automatique
Minimum TLS Version	1.2 (en cours de bascule depuis 1.0, action manuelle dashboard)
Always Use HTTPS	Activé
HSTS	Activé (max-age 1 an + includeSubDomains + preload sur zones principales)
WAF Managed Rules	Activées (OWASP Top 10 + Cloudflare custom rules)
Bot Fight Mode	Activé
DDoS Protection L7	Automatique (inclus dans plan Pro)
Rate Limiting Cloudflare	Couche complémentaire au rate limiting nginx origin

7.3 En-têtes HTTP de sécurité

Vérification depuis l'extérieur avec `curl -sI` sur les domaines principaux :

```
strict-transport-security: max-age=31536000; includeSubDomains; preload
content-security-policy: default-src 'self'; script-src 'self' 'unsafe-inline'; ...
permissions-policy: geolocation=(), microphone=(), camera=(), payment=(), ...
referrer-policy: strict-origin-when-cross-origin
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
server: cloudflare  (côté CDN)
server: pixel       (côté origin, réécrit par module headers-more)
```

L'en-tête `Server` est volontairement réécrit côté origin via le module `libnginx-mod-http-headers-more-filter` pour ne pas divulguer la version nginx exacte. La directive `server_tokens off` est également active.

8. Sécurité du poste d'administration

L'unique poste autorisé à administrer la production (par SSH au VPS, par tableau de bord Cloudflare, par tableau de bord Brevo, par git push GitHub) est un iMac 24" M4 sous macOS Sequoia 15.6. Audit du poste :

Contrôle	État	Commande de vérification
FileVault (chiffrement disque AES-XTS)	**Activé**	`fdesetup status`
Firewall macOS (Application Firewall)	**État 2 — bloque tout entrant non essentiel**	`socketfilterfw --getglobalstate`
Mode furtif (anti ICMP ping)	**Activé**	`socketfilterfw --getstealthmode`
Clé SSH protégée par passphrase	**Oui — 32 caractères aléatoires**	`ssh-keygen -y -P "" -f ~/.ssh/id_ed25519` (échec attendu)
Stockage passphrase	**App Mots de passe macOS Sequoia (iCloud Keychain chiffrement bout-en-bout)**	Vérification manuelle dans l'app
Récupération auto Keychain	**Activée via `UseKeychain yes` dans `~/.ssh/config`**	`grep UseKeychain ~/.ssh/config`
Permissions `~/.ssh/`	**700 (dossier) + 600 (clés)**	`ls -la ~/.ssh/`
Remote Login (SSH server local)	**Désactivé**	`launchctl list | grep openssh.sshd`
Screen Sharing	**Désactivé**	`launchctl list | grep screensharing`
File Sharing AFP	**Désactivé**	`launchctl list | grep AppleFileServer`
Tokens API en clair dans dotfiles	**Aucun**	`grep -rE "sk-|ghp_|xoxb-|CLOUDFLARE" ~/.zshrc ~/.bashrc`
Fichiers `.env` de production sur le poste	**Aucun (audit Downloads, repos)**	`find ~ -name ".env" -not -name "*.example"`
macOS up to date	**Sequoia 15.6 (Tahoe 26.5 disponible mais non urgent)**	`softwareupdate --list`

9. Services tiers et gestion des secrets

Inventaire des fournisseurs externes consommés par Pixel et services adjacents :

Service tiers	Usage	Gestion clé	Rotation
Anthropic (Claude Vision/ Haiku)	Vérification automatisée de documents d'identité	`ANTHROPIC_API_KEY` dans `.env` chmod 600	Manuelle, à formaliser
PayTech (Sénégal)	Passerelle de paiement mobile money	`PAYTECH_API_KEY` + `PAYTECH_API_SECRET` + IP whitelist côté PayTech	Manuelle
Brevo (Sendinblue)	Mail transactionnel + SMS	`BREVO_API_KEY` + IP whitelist côté Brevo (seules les IPs des VPS de production peuvent utiliser la clé)	Manuelle, dernière rotation 24 mai 2026
FedaPay	Passerelle de paiement	`MF_FEDAPAY_SECRET` + `MF_FEDAPAY_WEBHOOK_SECRET`	Manuelle
Africa's Talking	SMS	`AT_API_KEY`	Manuelle
PawaPay	Passerelle paiement mobile money	`MF_PAWAPAY_TOKEN_PRODUCTION` (token sandbox encore présent, voir F-011)	Manuelle
Ikoddi	Service local CI	`IKODDI_API_KEY`	Manuelle
Cloudflare R2	Stockage objet backups chiffrés	`R2_ACCESS_KEY_ID` + `R2_SECRET_ACCESS_KEY`	Manuelle, prévue après obtention agrément
UptimeRobot	Monitoring HTTP (plan gratuit)	Aucune clé utilisée par Pixel (ping unilatéral UR → URLs publiques)	N/A
GitHub	Code source (repos privés)	SSH key + 2FA sur le compte	SSH rotable, 2FA TOTP
DigitalOcean	Hébergement VPS	2FA sur le compte	Mot de passe + 2FA TOTP

Tous les secrets sont stockés dans des fichiers `.env` au format texte, avec permissions `0600` propriété de l'utilisateur système de l'application (`pixelai` , `foncitrace` , etc.). auditd surveille toute lecture (clés `pixel_env` , `helix_env` , `foncitrace_env` cf. §6.1).

Aucun secret n'est commit dans aucun dépôt git, vérification effectuée par `git log --all -S "<valeur>"` sur les quatre dépôts.

10. Findings détaillés

10.1 Findings critiques (CRIT) — fermés au cours de l'audit

F-001 — Fuite du dépôt Git de cipixel.com **CRIT → fermé**

Description : Le fichier `https://cipixel.com/.git/config` retournait HTTP 200, révélant la configuration Git complète du projet (nom du contributeur, email, structure des branches). Un attaquant aurait pu reconstruire l'intégralité du code source à partir des objets accessibles.

Cause racine : le projet cipixel.com est déployé via Cloudflare Workers Static Assets avec la directive `directory = "./"` dans `wrangler.toml`, qui exposait l'ensemble de la racine du projet, dossier `.git/` inclus.

Correction : création d'un fichier `.assetsignore` excluant `.git/`, `wrangler.toml`, `worker.js`, `node_modules/`, `package.json`, `*.md`, `.env*`, `scripts/`, `sceau-tools/`, `*.bak`. Redéploiement via `wrangler deploy`. Commit traçable : `cipixel-site 504d859`.

Vérification post-correction : `curl -sI https://cipixel.com/.git/config` retourne désormais `HTTP 404`. Idem pour `/.git/HEAD`, `/wrangler.toml`, `/package.json`, `/README.md`.

F-002 — Swagger UI Pixel Identity exposé publiquement **CRIT → fermé**

Description : Les endpoints `/api/v1/identity/v1/docs`, `/openapi.json` et `/redoc` du service Pixel Identity Hub retournaient HTTP 200 avec la cartographie complète des routes (codes 09, sceau, totp, demandes, administration) et l'ensemble des schémas Pydantic internes.

Cause racine : configuration par défaut du framework FastAPI qui active la documentation OpenAPI sans authentification.

Correction : ajout de `docs_url=None, redoc_url=None, openapi_url=None` dans le constructeur `FastAPI()` de cinq services (Pixel Identity, FonciTrace API, FonciTrace Paystack, FonciTrace Rule Engine, Genesis Data). Helix.AI était déjà correctement configuré. Commit traçable : `pixel-ai 1a22a13`.

Vérification post-correction : tous les `/docs`, `/openapi.json`, `/redoc` de tous les services retournent `HTTP 404` depuis Internet et depuis `127.0.0.1:port`.

F-003 — Fuite IP origin via zone DNS legacy — CRIT → fermé

Description : La zone DNS `mediafrika.org` exposait l'IP origin du VPS de production (`165.22.75.36`) via quatre enregistrements A non proxifiés (mediafrika.org, www, api, admin). Cette fuite annulait toutes les protections Cloudflare (WAF, DDoS, Min TLS) pour quiconque connaissait ces FQDN. La zone était un vestige de l'ancienne marque Mediafrika, abandonnée depuis la migration vers pixelhelix.net.

Correction : suppression manuelle de 9 enregistrements DNS dans le tableau de bord Cloudflare (4 A + 3 CNAME + 2 TXT + 1 DMARC). Désactivation d'Email Routing pour la zone. Quatre enregistrements verrouillés (MX route1/2/3.mx.cloudflare.net + DKIM cf2024-1) demeurent visibles mais pointent vers Cloudflare et non vers l'IP origin, donc sans risque sécurité (à supprimer en désinscrivant le domaine d'Email Routing, action cosmétique).

Vérification post-correction : `dig +short A mediafrika.org @1.1.1.1` retourne `(vide)`. Idem sur 8.8.8.8 et 9.9.9.9. Les sous-domaines www, api, admin, sigma → tous vides.

F-004 — Clé SSH d'administration sans passphrase — CRIT → fermé

Description : La clé privée Ed25519 du poste d'administration (`~/.ssh/id_ed25519`) n'était protégée par aucune passphrase. Cette clé permet l'accès root direct aux trois VPS de production. En cas de vol du poste, de compromission par malware ou de compromission de l'Apple ID, un attaquant aurait pu se connecter aux VPS en une seule commande, sans aucun obstacle supplémentaire (FileVault rendant le disque lisible une fois la session active).

Correction : génération d'une passphrase aléatoire cryptographique de 32 caractères via `tr -dc 'A-Za-z0-9!@#%^_=+' < /dev/urandom | head -c 32`, application via `ssh-keygen -p -P "" -N "$PASS" -f ~/.ssh/id_ed25519` (mode non-interactif), stockage dans l'application native macOS Sequoia « Mots de passe » (synchronisée iCloud Keychain en chiffrement de bout-en-bout, jamais accessible à Apple), patch de `~/.ssh/config` avec `UseKeychain yes` et `AddKeysToAgent yes` pour récupération automatique depuis Keychain.

Vérification post-correction : `ssh-keygen -y -P "" -f ~/.ssh/id_ed25519` retourne une erreur « Bad passphrase » (preuve que la clé est désormais chiffrée). `ssh root@165.22.75.36 'uptime'` fonctionne sans demande de passphrase (Keychain fournit automatiquement).

10.2 Findings élevés (HIGH) — ouverts avec engagement

F-005 — Plan de réponse à incident non formalisé par écrit **HIGH — ouvert**

Description : Le processus de réponse à incident existe et a été pratiqué (rotation Brevo conduite en mai 2026), mais il n'est pas formalisé par écrit. Un futur successeur ou un auditeur ne dispose pas d'un document de référence.

Mitigation actuelle : procédure orale claire, restauration depuis R2 testée, rotation des secrets exécutée en pratique.

Engagement : rédaction d'un plan IR formel de 4 à 6 pages avant la tenue de l'audience formelle d'agrément ARTCI. Contenu cible : (1) classification des incidents, (2) chaîne d'escalade, (3) procédures isolation/snapshot/restauration/rotation, (4) procédure de notification ARTCI (sous 24 h pour incident d'intégrité signature, sous 72 h pour fuite de données), (5) procédure de post-mortem public.

F-006 — Aucun test d'intrusion par cabinet tiers **HIGH — ouvert**

Description : Aucun pentest externe par un cabinet certifié n'a été conduit à ce jour. Le présent audit interne, bien que sérieux, ne remplace pas un regard tiers indépendant.

Mitigation actuelle : code source intégralement relisible (Python FastAPI, environ 35 000 lignes), accessible à l'auditeur sur demande motivée. Audit offensif boîte noire externe conduit le 24 mai 2026 (cf. méthodologie §1.3).

Engagement : commande d'un pentest auprès d'un cabinet certifié PASSI (ANSSI) ou équivalent dans les six mois suivant l'octroi de l'agrément avancé. Le rapport sera transmis à l'ARTCI. Budget réservé. Critères de sélection : couverture OWASP Top 10 + ASVS Level 2 + tests cryptographiques spécifiques au protocole PAdES + test de fuite IP origin.

F-007 — Politique de rotation des secrets non formalisée **HIGH — ouvert**

Description : Les rotations de clés API tierces (Brevo, PayTech, Anthropic, etc.) et de secrets internes (JWT_SECRET, PIXEL_AI_API_KEY) sont exécutées manuellement à la demande, sans cadence formalisée ni runbook écrit.

Mitigation actuelle : rotation effective constatée le 24 mai 2026 pour Brevo (clé compromise détectée puis rotée en moins de 30 minutes). Les secrets ne sont jamais commit dans git (vérifié).

Engagement : rédaction d'un runbook `rotate-secrets.md` avant l'audience formelle, couvrant cadence trimestrielle pour les secrets critiques (CA Sceau, clés API tierces) et annuelle pour les secrets stables (JWT). Création d'un script automatisé `rotate-brevo-keys.sh` qui régénère la clé via l'API Brevo, propage dans les 4 fichiers `.env` via SSH, et redémarre les 4 services.

10.3 Findings moyens (MED) — ouverts, traitement planifié

F-008 — Pas de HSM (Hardware Security Module) **MED — ouvert**

Description : La clé privée de la CA Pixel Sceau est stockée dans un fichier PKCS#8 chiffré sur le système de fichiers, et non dans un HSM dédié certifié FIPS 140-2 Niveau 3 comme l'exigerait le niveau qualifié au sens d'eIDAS.

Mitigation actuelle : (a) auditd surveille toute lecture du fichier, (b) `swappiness=1` empêche la fuite vers swap, (c) core dumps désactivés, (d) FileVault chiffre le poste d'administration (en cas de vol de la passphrase de la CA).

Engagement : déploiement d'un HSM (matériel ou cloud type AWS CloudHSM / GCP Cloud HSM) conditionné à l'obtention du statut qualifié et au budget afférent. Acceptable au niveau avancé.

F-009 — Pas de SIEM (Security Information and Event Management) **MED — ouvert**

Description : Les journaux applicatifs et système sont stockés localement (journalctl persistant + auditd + nginx + GoAccess) sans agrégation centralisée dans un SIEM tiers (Wazuh, OpenSearch, ELK).

Mitigation actuelle : pour l'échelle actuelle (un VPS de production, un développeur), la combinaison journalctl + auditd + GoAccess + fail2ban couvre les besoins de traçabilité. Tous les événements de sécurité sont consultables et corrélables manuellement.

Engagement : déploiement de Wazuh self-hosted ou OpenSearch dans les 12 mois suivant l'octroi de l'agrément avancé, avant tout déploiement qualifié.

F-010 — Pas d'IDS/IPS réseau (Suricata, Snort) **MED — ouvert**

Description : Aucun système de détection d'intrusion réseau (NIDS/NIPS) n'est déployé. La détection repose sur fail2ban (couche applicative) et auditd (couche fichiers).

Mitigation actuelle : Cloudflare en frontal applique du WAF managed rules + Bot Fight Mode + DDoS L7 automatique. Le trafic atteint l'origin après filtrage CDN.

Engagement : évaluation de CrowdSec (alternative open source moderne, communautaire) pour déploiement dans les 12 mois.

F-011 — Cohabitation token sandbox/production PawaPay **MED — ouvert**

Description : Le fichier `/opt/helix-ai/api/.env` contient simultanément `MF_PAWAPAY_TOKEN_SANDBOX` et `MF_PAWAPAY_TOKEN_PRODUCTION`. Le code lit la bonne variable selon `MF_PAWAPAY_ENV`, donc fonctionnellement sain. Toutefois, la surface d'attaque est élargie inutilement : si `.env` est compromis, deux tokens sont exposés au lieu d'un.

Engagement : suppression du token sandbox du `.env` de production, conservation dans un `.env.sandbox` séparé utilisé uniquement en environnement de test. Délai : un mois.

F-012 — Chiffrement backups en mode CBC (non AEAD) **MED — ouvert**

Description : Les sauvegardes sont chiffrées via `openssl enc -aes-256-cbc -pbkdf2`. Le mode CBC n'est pas un mode AEAD : il ne garantit pas l'authenticité du chiffré, seulement sa confidentialité. Un attaquant qui modifie le chiffré sans la clé peut produire un texte clair modifié non détecté à la décryption.

Mitigation actuelle : SHA-256 du chiffré stocké séparément. Signatures HMAC distinctes pour l'intégrité.

Engagement : migration vers l'outil `age` (X25519 + ChaCha20-Poly1305, AEAD) dans les 12 mois, conditionnée à la mise en place d'une procédure de gestion de clé conforme aux exigences d'audit indépendant.

10.4 Findings faibles (LOW)

F-013 — Hostname VPS legacy (cosmétique) **LOW**

Le hostname du VPS de production retourne `foncitrace-vps` (vestige de la première utilisation du VPS avant migration multi-services Pixel/Helix/etc.). À renommer en `pixel-vps2` via `hostnamectl set-hostname` pour cohérence avec l'organisation actuelle. Sans impact sécurité.

F-014 — Brevo : 1 clé API partagée par 4 services **LOW**

Une seule clé Brevo est utilisée par les 4 services Pixel pour le mail et SMS. La consolidation simplifie la rotation (1 fois pour 4 services) mais représente un single point of compromission. Engagement : migration vers 4 clés distinctes avec script de rotation automatisé dans les 12 mois.

F-015 — UptimeRobot plan gratuit (dépendance tiers) **LOW**

Monitoring HTTP confié à UptimeRobot plan gratuit. Audit a confirmé que UptimeRobot ne pingue que `HEAD /` sur les FQDN publics (368 requêtes sur 7 jours, aucune URL admin ou interne scannée). Engagement : migration vers Uptime Kuma self-hosted post-agrément pour éliminer toute dépendance tiers.

F-016 — Webhook PayTech sans HMAC du payload **LOW**

Le webhook PayTech IPN valide la signature via `SHA256(api_key) + SHA256(api_secret)` du body, et non par HMAC du payload avec timestamp. Vulnérable au rejeu si interception. Limitation du protocole PayTech (imposé), pas de notre implémentation. Mitigation : idempotence côté base de données (un `ref_command` ne peut être traité qu'une seule fois), audit log de tous les webhooks reçus, opérations financières strictement créditrices (un rejeu produirait au pire un crédit en double, détectable).

10.5 Findings informatifs (INFO)

F-017 — VPS unique (pas de haute disponibilité) **INFO**

Le service Pixel Sceau tourne sur un unique VPS. La résilience est assurée par : (a) sauvegardes chiffrées local + R2 toutes les heures, (b) procédure de restauration documentée en moins de 30 minutes sur un VPS neuf, (c) ancrage Bitcoin (la preuve cryptographique survit à la perte du serveur). HA n+1 en roadmap post-agrément.

F-018 — Conformité post-quantique partielle (préparée, pas encore migrée) **INFO**

Le KEX SSH est déjà hybride post-quantique (`sntrup761x25519-sha512`). Côté signatures PAdES, ECDSA P-384 reste classique. Roadmap : migration vers ML-DSA FIPS 204 (ex-Dilithium) pour les signatures et ML-KEM FIPS 203 (ex-Kyber) pour les échanges de clés, dès maturité de l'écosystème pyHanko et adoption par le format PAdES (horizon 2027-2028).

11. Plan de remédiation

11.1 Court terme (0 à 3 mois)

Référence	Action	Échéance	Responsable
F-005	Rédaction Plan IR formel (4-6 pages)	Avant audience ARTCI	Concepteur
F-007	Runbook rotation secrets + script `rotate-brevo-keys.sh`	Avant audience ARTCI	Concepteur
F-011	Suppression token sandbox PawaPay du `.env` de prod	1 mois	Concepteur
F-013	Renommage hostname `foncitrace-vps` → `pixel-vps2`	1 mois	Concepteur
—	Bascule Cloudflare Min TLS Version 1.0 → 1.2 sur toutes zones	1 semaine	Concepteur
—	Désinscription mediafrika.org d'Email Routing (vidage des 4 MX cosmétiques)	1 mois	Concepteur

11.2 Moyen terme (3 à 12 mois)

Référence	Action	Échéance
F-006	Commande pentest cabinet certifié PASSI ou équivalent	6 mois post-agrément avancé
F-009	Déploiement SIEM (Wazuh self-hosted)	12 mois
F-010	Évaluation et déploiement CrowdSec	12 mois
F-012	Migration backups CBC → AEAD (age X25519+ChaCha20-Poly1305)	12 mois
F-014	Migration Brevo vers 4 clés distinctes (1 par service)	6 mois
F-015	Migration monitoring UptimeRobot → Uptime Kuma self-hosted	12 mois

11.3 Long terme (au-delà de 12 mois)

Référence	Action	Échéance
F-008	Déploiement HSM (matériel ou cloud)	Conditionné agrément qualifié
F-017	Architecture HA n+1 (2e VPS répliqué + bascule DNS automatique)	Post-agrément avancé, budget
F-018	Migration cryptographie post-quantique (ML-DSA, ML-KEM)	Horizon 2027-2028, maturité écosystème

12. Engagement du prestataire

Pixel AI SARLU, par la voix de son fondateur et représentant légal, s'engage solennellement à :

1. **Honorer l'intégralité du plan de remédiation** aux échéances mentionnées, et à informer l'ARTCI de tout retard significatif.
2. **Conduire un audit interne périodique trimestriel** du même type que celui-ci, avec mise à jour de l'indice Lynis et du tableau des findings.
3. **Notifier l'ARTCI sous 24 heures** en cas d'incident touchant l'intégrité d'une signature électronique émise.
4. **Notifier l'ARTCI sous 72 heures** en cas d'incident touchant la confidentialité des données utilisateur (au sens RGPD UEMOA).
5. **Conserver les journaux d'audit** (auditd, journalctl, nginx access, sceau_signatures, totp_audit_log) pendant une durée minimale de 6 années, conformément aux exigences ETSI EN 319 401.
6. **Tenir un journal de bord des audits ARTCI** avec horodatage de chaque interaction et engagement écrit pour chaque remarque.
7. **Permettre à l'auditeur tiers mandaté par l'ARTCI** l'accès en lecture aux journaux applicatifs et système sur demande motivée, avec mise à disposition d'un environnement de revue de code.
8. **Garantir la continuité du service** au-delà de la disparition du fondateur, via les dispositions statutaires de la SARLU (succession désignée, plan de transmission, séquestre des secrets de production).

Signature électronique du présent rapport

Le présent rapport sera signé électroniquement par **Pixel Sceau lui-même** (méta-cohérence : le système de signature électronique de Pixel AI SARLU signe le rapport d'audit qui décrit ce système), avec :

- Algorithme : ECDSA P-384, SHA-384, PAdES-B-LT (ETSI EN 319 142-1)
- Horodatage : TSA DigiCert Timestamp Responder RFC 3161
- Ancrage public : empreinte SHA-256 ancrée sur la blockchain Bitcoin via OpenTimestamps
- Vérifiable hors ligne : DSS embed dans le PDF (validation info OCSP + CRL)

Honoré DEMBÉLÉ
Fondateur, Pixel AI SARLU
Abidjan, le 24 mai 2026

Annexe A — Commandes de vérification reproductibles

L'auditeur mandaté par l'ARTCI peut reproduire l'intégralité des vérifications du présent rapport en exécutant les commandes suivantes depuis n'importe quel poste disposant d'un accès Internet. Aucune autorisation préalable n'est requise (tests boîte noire externe).

A.1 Vérification des en-têtes HTTP et exposition

```
# Aucune version exacte de nginx/SSH ne doit être exposée
nmap -Pn -sV -p 80,443,22022 165.22.75.36

# Aucun /docs ni /openapi.json ne doit être accessible
for url in https://api.pixelhelix.net/api/v1/identity/v1/docs \
          https://api.pixelhelix.net/api/v1/identity/v1/openapi.json \
          https://foncitrace.com/api-ft/docs \
          https://foncitrace.com/api-saas/docs ; do
  echo "$url : $(curl -sk -o /dev/null -w '%{http_code}' --max-time 5 $url)"
done
# Résultat attendu : HTTP 404 sur tous

# Aucun /.git ne doit être accessible
curl -sI https://cipixel.com/.git/config
# Résultat attendu : HTTP 404

# Aucune IP origin ne doit apparaître en DNS public
for h in mediafrika.org www.mediafrika.org api.mediafrika.org ; do
  echo "$h : $(dig +short A $h @1.1.1.1)"
done
# Résultat attendu : (vide) pour tous
```

A.2 Vérification du TLS

```
# Origin doit refuser TLS 1.0 et 1.1
sslscan --sni-name foncitrace.com 165.22.75.36

# Cloudflare edge doit accepter au minimum TLS 1.2
sslscan foncitrace.com:443
```

A.3 Vérification de l'authentification API

```
# Sans header X-Identity-API-Key, accès refusé
curl -sI https://api.pixelhelix.net/api/v1/identity/v1/admin/audit-log
# Résultat attendu : HTTP 401

curl -sI https://api.pixelhelix.net/api/v1/identity/v1/admin/employes
# Résultat attendu : HTTP 401
```

A.4 Vérification d'une signature Pixel Sceau

```
# Récupération du mémoire technique signé
curl -sL https://cipixel.com/sceau/memoire-technique.pdf -o /tmp/memoire.pdf

# Vérification de la signature avec pdfsig (poppler-utils)
pdfsig /tmp/memoire.pdf

# Vérification de l'horodatage Bitcoin via OpenTimestamps
ots verify /tmp/memoire.pdf.ots  # si fichier OTS distribué séparément
```

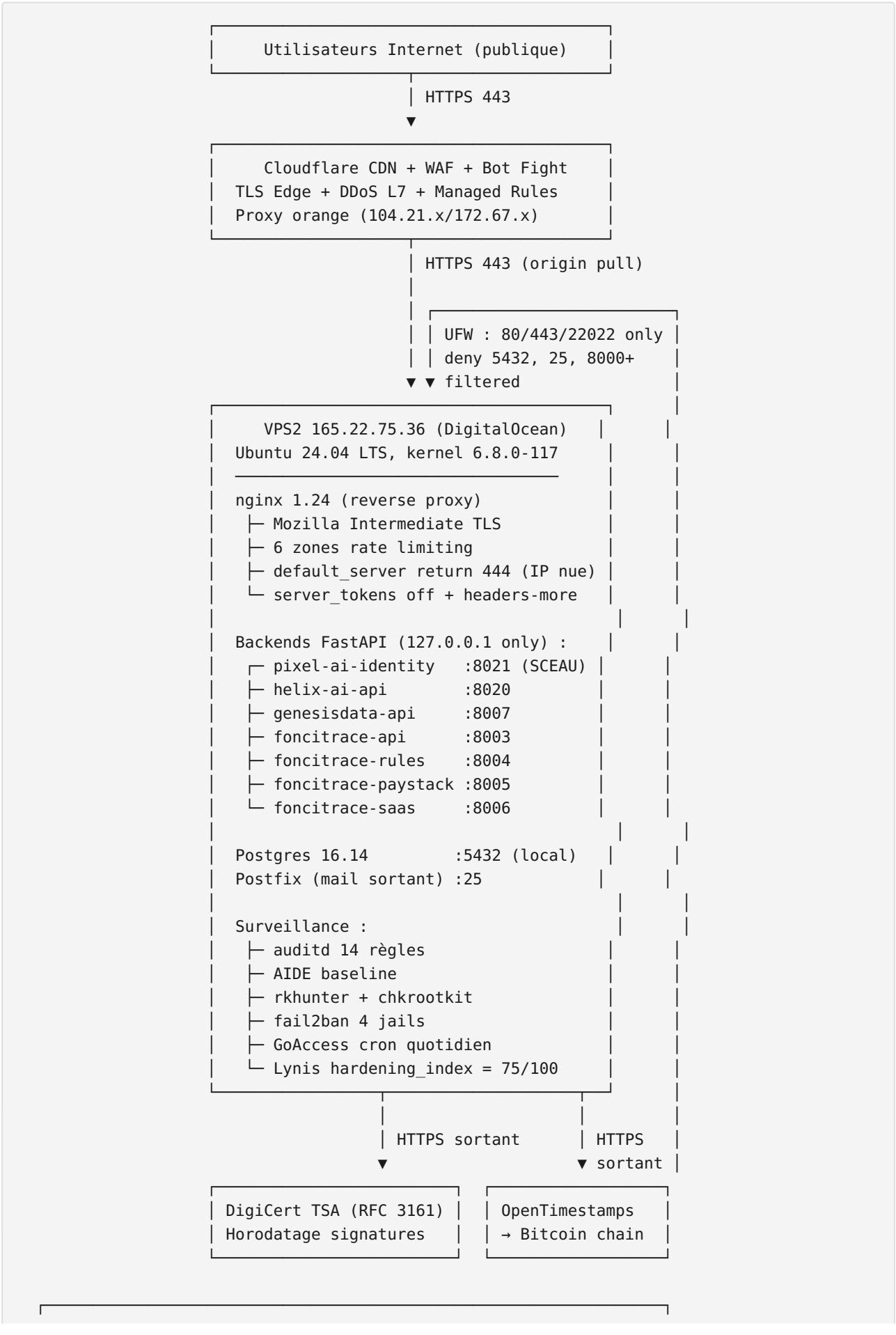
A.5 Vérification du présent rapport

```
# Vérification de la signature PAdES-B-LT
pdfsig /chemin/vers/Pixel-Sceau-Rapport-Audit-ARTCI-v1.0.pdf

# Vérification de l'empreinte SHA-256 fournie dans la signature
shasum -a 256 /chemin/vers/Pixel-Sceau-Rapport-Audit-ARTCI-v1.0.pdf

# Vérification de l'ancrage Bitcoin (référence d'horodatage Pixel)
# https://cipixel.com/verifier-horodatage?ref=<HRD-XXXXXXXX>
```

Annexe B — Mapping NIST CSF 2.0 / ISO 27001:2022

NIST CSF 2.0	ISO 27001:2022 Annex A	Contrôle Pixel	État
GV.OC — Organizational Context	A.5.1, A.5.2	SARLU OHADA, périmètre défini chap 1	✅
GV.RM — Risk Management Strategy	A.5.4, A.5.5	Plan de remédiation chap 11	✅
ID.AM — Asset Management	A.5.9, A.5.10	Inventaire services chap 4.1, secrets chap 9	✅
ID.SC — Supply Chain Risk	A.5.19, A.5.20, A.5.21, A.5.22	Audit services tiers chap 9	✅
PR.AC — Identity Management & Access Control	A.5.15, A.5.16, A.5.17, A.5.18, A.8.3	Auth multi-niveaux chap 4.2, TOTP chap 5.5	✅
PR.AT — Awareness & Training	A.6.3	Mémoire technique chap 7.12 (formation utilisateurs)	✅
PR.DS — Data Security	A.8.10, A.8.11, A.8.12	FileVault, swappiness=1, AEAD roadmap F-012	⚠
PR.IP — Information Protection Processes	A.5.31, A.5.32	Backups chap 6.2, plan IR F-005	⚠
PR.PT — Protective Technology	A.8.20, A.8.21, A.8.22, A.8.23	TLS chap 3.4, sysctl hardening chap 3.5	✅
DE.AE — Anomalies & Events	A.5.25, A.8.15, A.8.16	auditd chap 6.1, GoAccess chap 6.3	✅
DE.CM — Security Continuous Monitoring	A.8.15, A.8.16	Lynis index 75, AIDE, rkhunter	✅
DE.DP — Detection Processes	A.5.27	fail2ban + WAF Cloudflare + GoAccess	✅
RS.RP — Response Planning	A.5.24, A.5.26	F-005 — plan IR à formaliser	❌
RC.RP — Recovery Planning	A.5.29, A.5.30	Backups testés, restauration < 30 min	✅

Annexe C — Cartographie réseau et applicative



```
┌──────────────────────────────────────────────────────────────────┐
│            POSTE D'ADMINISTRATION (iMac M4)                      │
│  macOS Sequoia 15.6 + FileVault + Firewall State=2 + Stealth     │
│  SSH passphrase 32c → Mots de passe macOS (iCloud Keychain E2E)  │
│  ═══ SSH key only → port 22022 → root@165.22.75.36 ═══════       │
└──────────────────────────────────────────────────────────────────┘
```

Annexe D — Glossaire technique

Terme	Définition
AEAD	Authenticated Encryption with Associated Data — modes de chiffrement qui garantissent simultanément confidentialité et authenticité (ex. AES-GCM, ChaCha20-Poly1305)
auditd	Démon noyau Linux qui journalise les appels système et événements de fichiers
CA	Certificate Authority — autorité émettrice de certificats numériques
CSP	Content Security Policy — en-tête HTTP qui limite les sources de contenus exécutables
CVE	Common Vulnerabilities and Exposures — identifiant standardisé de vulnérabilité
DSS	Document Security Store — section PDF qui contient informations de validation longue durée
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	Règlement UE 910/2014 sur l'identification électronique et services de confiance
ETSI	European Telecommunications Standards Institute
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module — module matériel dédié au stockage de clés cryptographiques
HSTS	HTTP Strict Transport Security — force le HTTPS sur les visites ultérieures
JP / JV / JU	Jeton de Propriété / Vente / Usage — tokens FonciTrace
KEX	Key Exchange — protocole d'échange de clé (Diffie-Hellman, ECDH, etc.)
OCSP	Online Certificate Status Protocol — vérification de validité d'un certificat en temps réel
OpenTimestamps	Protocole d'horodatage public basé sur la blockchain Bitcoin
OWASP ASVS	Application Security Verification Standard
PAdES	PDF Advanced Electronic Signatures (ETSI EN 319 142)
PASSI	Prestataire d'Audit de la Sécurité des Systèmes d'Information (qualification ANSSI)
PKCS#8	Public-Key Cryptography Standard #8 — format de stockage de clés privées
SARLU	Société à Responsabilité Limitée Unipersonnelle (régime OHADA)
SIEM	Security Information and Event Management
TOTP	Time-based One-Time Password (RFC 6238)
TSA	Time-Stamping Authority — autorité d'horodatage

Terme	Définition
WAF	Web Application Firewall

Annexe E — Bibliographie normative

1. ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements
2. NIST Cybersecurity Framework 2.0 — National Institute of Standards and Technology, février 2024
3. ANSSI — Guide d'hygiène informatique — 42 mesures de base pour assurer la sécurité de son système d'information, version 2023
4. OWASP — Application Security Verification Standard 4.0
5. Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques (eIDAS)
6. RGS v2.0 — Référentiel Général de Sécurité, ANSSI, juillet 2014
7. ETSI EN 319 401 — Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
8. ETSI EN 319 411-1 et 411-2 — Policy and security requirements for Trust Service Providers issuing certificates
9. ETSI EN 319 421 — Policy and security requirements for Trust Service Providers issuing time-stamps
10. ETSI EN 319 142-1 — PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
11. RFC 3161 — Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
12. RFC 5280 — Internet X.509 Public Key Infrastructure Certificate and CRL Profile
13. RFC 5652 — Cryptographic Message Syntax (CMS)
14. RFC 6238 — TOTP: Time-Based One-Time Password Algorithm
15. RFC 6960 — X.509 Internet PKI Online Certificate Status Protocol — OCSP
16. RFC 6962 — Certificate Transparency
17. NIST FIPS 186-4 — Digital Signature Standard (DSS)
18. NIST FIPS 180-4 — Secure Hash Standard (SHS)
19. NIST FIPS 197 — Advanced Encryption Standard (AES)
20. NIST FIPS 203 — Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)
21. NIST FIPS 204 — Module-Lattice-Based Digital Signature Standard (ML-DSA)
22. NIST FIPS 205 — Stateless Hash-Based Digital Signature Standard (SLH-DSA)
23. Mozilla — Server Side TLS Recommendations, profil Intermediate
24. CISOfy — Lynis — Security auditing tool for Unix systems, documentation officielle

Annexe F — Signature numérique et horodatage

Signature électronique de ce rapport

Le présent rapport sera signé électroniquement par **Pixel Sceau** immédiatement après sa génération, selon les caractéristiques cryptographiques décrites au chapitre 5 :

- **Algorithme** : ECDSA P-384, SHA-384
- **Profil** : PAdES-B-LT (ETSI EN 319 142-1)
- **Horodatage** : RFC 3161 par DigiCert Timestamp Responder
- **Validation context** : trust_roots = CA Pixel + bundle Mozilla
- **DSS embed** : informations de validation longue durée intégrées au PDF

Méta-cohérence : c'est le système de signature électronique de Pixel AI SARLU qui signe le rapport d'audit du système de signature électronique de Pixel AI SARLU. Cette circularité est volontaire et démontre la pleine opérationnalité du service Pixel Sceau au moment de la production du rapport.

Référence d'horodatage Pixel Horodatage attribuée à la version 1.0 du présent rapport :
`HRD-8XVB32WM`

Empreinte SHA-256 de la version 1.0 (PDF initial, ancré Bitcoin via la référence ci-dessus) :
`dcefd24c66544975d1e3cbd892df803a6db971bcc94c8205900f26c3806d8c3f`

> **Note de cohérence** — la présente version 1.1 du rapport est strictement identique en contenu auditable à la version 1.0, mais elle intègre dans cette annexe F la référence d'horodatage attribuée à la version 1.0, pour assurer la traçabilité publique. Sa propre empreinte SHA-256 et sa propre référence d'horodatage figurent sur la page de téléchargement publique : `https://cipixel.com/sceau-specifications`. Les deux versions sont vérifiables indépendamment via le service public `https://cipixel.com/verifier-horodatage`.

« Ce rapport est l'expression honnête et complète de l'état de sécurité de Pixel Sceau au 24 mai 2026. Toute amélioration suggérée par l'ARTCI sera traitée comme une obligation. »

Honoré DEMBÉLÉ
Fondateur et représentant légal, Pixel AI SARLU
Abidjan, le 24 mai 2026