



MINTID

MintID Issuer Manual

How to establish and operate as an identity issuer on the MintID network: compliance, software and infrastructure.

VERSION 0.1 · 2026-08-09 · PUBLIC EDITION

PROTOCOL ECONOMIC PARAMETERS: ILLUSTRATIVE BANDS, PENDING EXTERNAL
SIMULATION

THIS DOCUMENT IS NOT LEGAL ADVICE

Status and scope. Public edition (v0.1). The network is in the pre-genesis phase (internal testnet); the protocol's economic parameters (fees, bond, commissions) are **illustrative bands pending the external simulation** – no figure in this manual is a ratified price. This manual is not legal advice: the compliance chapter describes the tasks and their order, it does not replace the opinion of a specialised law firm.

1. The issuer role in five minutes

An **issuer** is the organisation that performs the real KYC on people and companies, issues the resulting anonymous credentials, and keeps their revocation status up to date. It is the only piece of the entire system that sees personal data – and for that reason it is the one that concentrates the compliance obligations.

What an issuer does:

- Verifies the holder's identity (KYC/AML) at the corresponding assurance grade (A1–A4).
- Signs anonymous credentials that the holder keeps in their wallet. The issuer keeps **no** copy of the credential: it keeps the **identity link** (who is behind which case file) in its vault.
- Publishes a status root (a 32-byte cryptographic digest) to the chain **every 30 seconds** – the “heartbeat” that powers revocation for all of its holders.
- Charges for each agent's onboarding (*mint*), a recurring fee (*lease*), and brokerage commissions on consented disclosure.
- Deposits a **slashable bond** that it loses, in whole or in part, if it misbehaves.

What it never does (hard protocol invariants):

- No personal data, credential or serial number ever touches the chain (R2/R8). The chain only sees the issuer's registry entry and its roots (R19).
- It never reveals a holder's identity on its own initiative or for money: unmasking exists only through the dispute path with due process (council + independent custodian).
- It does not decide the re-verification cadence: the protocol fixes it per grade (A1/A2: 12 months · A3: 6 months · A4: 3 months).

The business, in one line: revenue $\approx$ \$12 per agent-year at the base point (band \$7–27), with high fixed costs – the **break-even is a portfolio of 25,000–40,000 active agents**. It is a business of volume and trust, not of unit margin.

2. The path to establishment – overview

PHASE	CONTENT	INDICATIVE DURATION
1 • Legal & compliance	Entity, registration as an obliged subject, AML manual, GDPR/DPO, contracts with providers	3–6 months (in parallel with phase 2)
2 • Technical	Deployment of the issuer stack, key ceremony, KYC provider integration	2–4 months
3 • Testnet	Full operation against the testnet: root SLOs, emergency drills	1–2 months
4 • Admission	Application to the network, admission fee, bond deposit	weeks
5 • Production	Gradual go-live, continuous operation with SLOs	–

3. The compliance workload

3.1 Legal framework and registration as an obliged subject

The issuer performs identity verification for KYC/AML purposes: depending on the jurisdiction and the service model, this makes it an **obliged subject** under anti-money-laundering law. Taking Spain as the example (Law 10/2010 and its regulation):

- **Registration and representative before SEPBLAC**, if the activity falls within scope (prior opinion from the law firm: the exact perimeter depends on whether the issuer serves third-party obliged entities or acts on its own account).
- **AML prevention manual**: risk analysis, customer-acceptance policies, due diligence (standard, simplified and enhanced), thresholds and alert scenarios.
- **Internal control body (OCI)** and authorised representative; minutes and meeting calendar.
- **Mandatory annual training** for all staff with access to case files.
- **Annual external audit** of the prevention system (independent external expert).
- **10-year document retention** of due-diligence files – which deliberately clashes with GDPR minimisation and must be resolved through the vault design (§3.2).

3.2 Data protection (GDPR)

The issuer is the **data controller** for the KYC data – the only piece of the system that holds any. Tasks:

- **Data protection officer (DPO)** appointed and notified to the authority (AEPD in Spain).
- **Impact assessment (DPIA)** mandatory: the processing includes biometrics (selfie/liveness) and large-scale identity verification – high-risk by definition.
- **Record of processing activities**, retention policy (10-year AML vs minimisation: encrypted retention with sealed access), and data-subject-rights procedures – with the particularity that the exercise of rights goes through the **vault's identity link**, never through clear-text data scattered around.
- **The design works in your favour**: since no data ever leaves the vault towards the chain or towards verifiers, the exposure surface is a single audited safe – not a continuous flow of copies.

3.3 Contracts and coverage

- **KYC provider** (document verification + biometrics): data-processing agreement (DPA), latency and approval-rate SLAs, per-check pricing (2026 market: \$0.80-1.85 per automated check, annual minimums \$20k-100k depending on provider).
- **AML screening** (sanctions/PEP) on every onboarding and **continuous monitoring** of the portfolio (~\$0.25 per mint; ~\$0.09/profile/month at market rates).
- **Insurance**: professional liability and a cyber policy (the issuer custodies the identity link – the most sensitive asset in the system).
- **HSM and key custody**: service contract or purchase (see §5).

3.4 Operating policies the network requires

- **Assurance grades A1-A4** with protocol-fixed validity (12/12/6/3 months) and re-KYC on expiry: you need the operational process for mass portfolio renewal.
- **Active-agent limit per holder** (anti-sybil) enforced privately by the issuer.
- **Revocation procedure** (fraud, death, holder request) effective within ≤ 45 seconds via the next root, and an **emergency root** for serious incidents.
- **L2 dispute response**: the issuer only opens the identity link upon a council order with an independent custodian, recorded on-chain – never upon a direct demand from a verifier or a third party.
- **Incident and exit plan**: what happens to the portfolio if the issuer ceases (orderly transfer or wind-down with fail-closed).

3.5 Cost of the compliance workload (indicative bands)

ITEM	SET-UP	ANNUAL RECURRING
Specialised law firm (AML + GDPR + perimeter opinion)	\$20-60k	\$10-20k
Annual external AML audit	–	\$10-30k
DPO (external or part-time internal)	–	\$15-40k
Training, manuals, internal control body	\$5-10k	\$3-8k
Insurance (liability + cyber)	–	\$10-30k
Compliance subtotal	\$25-70k	\$48-128k

4. The software to install

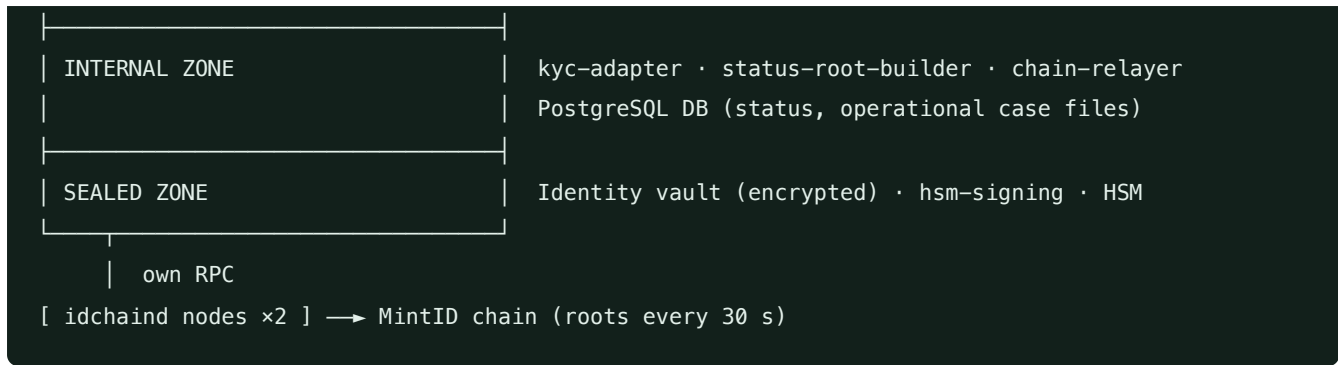
4.1 The reference stack (issuer-agent/)

Status: the network is pre-genesis; the issuer stack is under construction on the frozen architecture. The components below are those of the reference design – final binaries will be published together with the corresponding audits.

COMPONENT	FUNCTION	DEPLOYMENT NOTES
<code>openid4vci</code>	Issuance service: the standard protocol through which the holder's wallet receives the credential	Public HTTPS; the holder's only entry point
<code>kyc-adapter</code>	Abstraction layer over the KYC provider (documents + biometrics + AML)	One adapter per provider; lets you switch providers without touching the rest
Identity vault	Safe holding the case-file $\rightleftharpoons$ credential link – the only copy of personal data	Encrypted at rest with keys in the HSM; sealed, audited access; encrypted offline backups
<code>status-registry</code>	Live registry of each credential's status (valid/revoked) and witness service for wallets	High availability: wallets depend on it to sync witnesses
<code>status-root-builder</code>	Builds the cryptographic status root every 30 seconds	The operational heart: if it stops >45 s, the whole portfolio goes fail-closed
<code>hsm-signing</code>	Signs credentials and roots with keys inside hardware	Never software keys in production
<code>chain-relayer</code>	Publishes the roots to the chain (2,880 transactions/day) and manages nonces, retries and gas	Operating account separate from the bond account
<code>idchaind node (x2)</code>	Own chain nodes to publish and read without depending on third parties	One publishing + one standby
Monitoring	Metrics, logs and alerts (root age, bond balance, KYC latency)	The root-age alert at 35 s is the critical alert

4.2 Three-zone architecture





Separation rules: the public zone has no access to the vault; the sealed zone has no internet egress; every signature goes through the HSM; the relayer is the only thing that talks to the chain.

4.3 Base software

Containers (Docker/Podman) orchestrated with systemd or lightweight Kubernetes; managed PostgreSQL with replicas; Prometheus + Grafana + Alertmanager; TLS with automatic renewal; secrets management (Vault/KMS); SoftHSM **only** on testnet – in production, a real HSM (see §5).

5. Infrastructure and server costs

5.1 Environments

ENVIRONMENT	SIZING	MONTHLY COST
Sandbox / testnet	1 application server (4 vCPU/16 GB) + 1 chain node + SoftHSM + small DB	\$200-400
Production (HA)	Next table	\$1,300-4,000

5.2 Production, line by line

ITEM	SIZING	MONTHLY COST (CLOUD, 2026)
Issuer services (×2, HA)	4-8 vCPU, 16 GB each	\$250-500
<code>idchaind</code> nodes (×2)	4-8 vCPU, 16 GB, 500 GB NVMe	\$300-500
Managed database	PostgreSQL with replica + PITR backups	\$200-400
Identity vault	Hardened dedicated instance + encrypted storage	\$150-300
HSM	Option A: managed cloud HSM (HA pair) – ~\$2,100/month · Option B: 2× USB/network HSM on-prem (~\$1,500-3,000 one-off) + hosting	\$150-2,100
Monitoring and logs	Own or managed stack	\$100-250
Network, WAF, TLS, DNS	–	\$100-250
Infrastructure total		≈\$1,300-4,000/month → \$16-48k/year

5.3 Variable and network costs

ITEM	MAGNITUDE	ANNUAL COST
KYC checks (per holder onboarding)	\$0.80-1.85 × onboardings	depends on portfolio (e.g. 1,200 holders: ~\$2.2k)
AML screening per mint	~\$0.25 × mints	e.g. 25,000 mints: ~\$6k
Root gas	2,880 tx/day = 1.05 M tx/year , forever	open parameter – budget \$1-10k/year
Network registry fee	admission + annual fee	~\$15k/year (band \$5-30k)
Bond (locked capital, not a cost)	placeholder 1,000 tokens; will be sized against a fiat deterrence target	–

5.4 Staff and total

BLOCK	ANNUAL
Team (2-4 FTE: compliance, operations, on-call engineering)	\$250-400k
Recurring compliance (\$3.5)	\$48-128k
Infrastructure (\$5.2)	\$16-48k
Variables and network (\$5.3)	\$10-35k
Total annual operating cost	≈\$325-610k

At the base revenue of ~\$12 per agent-year, the **break-even again lands around 25,000-40,000 active agents** – the figure that must preside over any issuer's business plan.

6. Joining the network, step by step

1. **Entity and base compliance** in place (§3): without the AML manual and the DPO there is no point in continuing.
2. **Key ceremony**: generation inside the HSM of (a) the credential-issuance key, (b) the root-signing key, and (c) the operating account (`operator_account`). Careful: **only the `operator_account` can deposit the bond** (the protocol's anti-impersonation rule) – the deposit cannot be delegated to any other account. Sealed recovery copies, distributed.
3. **Testnet deployment**: full stack (§4) against the testnet; validate 30 days of root cadence with no gaps >35 s, an emergency-root drill and a key-rotation drill.
4. **Admission application** to the network registry and payment of the fee; publication of the issuer's keys and metadata.
5. **Bond deposit** from the `operator_account` : the ACTIVE state is, by definition, *live bond* $\geq$ *minimum* – a deposit below the minimum is rejected outright.
6. **Heartbeat start**: first root published and the 30 s cadence running. From here on, **it cannot stop**: if the root ages past 45 s, all of your holders go fail-closed.
7. **Gradual go-live**: first real onboardings with a limited portfolio; staged opening with the SLOs green.

7. Continuous operation: SLOs and golden rules

SLO / RULE	VALUE	CONSEQUENCE OF BREACH
Root cadence	30 s	–
Maximum accepted root age	45 s	Entire portfolio fail-closed (verifications rejected)
Internal critical alert	age >35 s	10 s margin to intervene
Emergency roots	always available (network limit: 16/block)	–
Bond balance	> minimum + operating margin	Depletion = automatic suspension, no grace: the network rejects your roots – emergency ones included
Key rotation	procedure rehearsed on testnet	–
Own-fraud incidents	–	Bond slash (≈50% burned, remainder to the remediation fund for those harmed)

Three golden rules to close:

1. **The heartbeat is sacred.** The whole operational design (HA, on-call, alerts) exists so the 45-second window is never missed.
2. **The bond is not a formality, it is the brake.** Keep margin and a balance monitor: suspension is deterministic and the reputational damage immediate – your holders can prove nothing until you come back.
3. **The vault is the one thing you can neither lose nor expose.** Everything else in the stack can be redeployed; the identity link cannot.

Annex A – Model first-year budget (base band)

BLOCK	AMOUNT
Compliance set-up	\$25-70k
Technical deployment and ceremonies (own engineering + HSM)	\$30-60k
Annual operation (team + compliance + infra + variables)	\$325-610k
Network fee	~\$15k
Total year 1 (excluding bond)	≈\$395-755k
Bond (locked, recoverable capital)	per final parameter

Annex B – References

- [master/SPEC-1-...](#) §6.2 (bond and slashing), §9 (status roots and cadences), R2/R8 (no PII on-chain, ever), R9 (30 s heartbeat), R16 (bond), R19 (bounded state).
- [docs/integration/kyc-provider-abstraction.md](#) (KYC provider abstraction layer).
- Monetization report 2026-08-09 ([docs/economics/](#)) – economic bands and break-even.
- KYC market pricing: external research August 2026 (Veriff, Sumsb, Vendr; see the report).

Manual v0.1 (public edition) – 2026-08-09. The protocol's economic figures are illustrative bands pending the external simulation; market figures come from the August 2026 research. This document does not constitute legal advice.