



MINTID · ROLE MANUAL

MintID Validator Manual

What it means to secure an identity-first chain: the role, what you need, the road to genesis, your obligations, the economics as ratified and the risks.

PUBLISHED BY

MintID Foundation

Netherlands Stichting, Amsterdam · related parties disclosed

VERSION

**0.2 · October
2026**

AUDIENCE

**Validator operators and
delegators**

NETWORK

**Single-node
production**

ECONOMICS

**Ratified bands and
priors**

Contents

01	The role in one page	3
02	What you secure	4
03	Consensus and the validator set	5
04	What you need	5
05	The road to genesis	6
06	Obligations, slashing and guarantees	8
07	Economics	9
08	Governance: where you have power	11
09	For delegators	11
10	Risks, stated plainly	12
A	Validator values at a glance	12

Status and scope. MintID runs in production on **the single-node production chain** (since 20 September 2026), operated by the CONECTIA group; the distributed mainnet has not launched, and there is no token genesis, no public validator set and no token price. **The public testnet**, with its KYC sandbox, is where third parties test the software at production parameters; it has one validator, run by the operator, takes no outside validators and is not the public adversarial testnet of \$5.3; whether it is live is stated in one place, the developer documentation's page *The public testnet and its KYC sandbox* ([docs/sdk/17-sandbox-and-testnet.md](#) in the main repository). Every validator value in this manual is a *ratified band* or a *ratified prior* — an argued working point that the independent pre-genesis economic simulation validates or argues against — unless it is marked as frozen. **Nothing is for sale and no price exists.** This manual is a non-normative role guide: it is **not** the crypto-asset white paper required by MiCA (Regulation (EU) 2023/1114) Title II, not an offer of any crypto-asset and not investment, legal or tax advice. The specification corpus governs and is available on request to prospective operators. The specification corpus is available on request at info@mintid.net.

01

The role in one page

A MintID validator replicates a small, deterministic state machine that anchors identity trust, and is never asked to judge who anyone is.

MintID is a sovereign, permissionless proof-of-stake Layer-1 built with the Cosmos SDK on CometBFT. Its product is **identity trust, not decentralised finance**: accepted KYC issuers vouch for people and the AI agents they deploy, holders prove claims with zero-knowledge presentations that never touch the chain, and the chain holds only what must be public for that trust to be checkable. The commercial word for the role is *miner*; technically it is a **validator** under delegated proof of stake.

60

validators in the genesis active set, growing toward 100 by governance

~5 s

finality objective, with blocks every two to three seconds

5 %

cap on any validator's effective voting power

21 days

unbonding period for validators and delegators

What you validate. Deterministic protocol state transitions: the issuer and verifier registries, the signed status roots every issuer publishes at least every 30 seconds, issuer bonds, compliance-council decisions, protocol parameters, fees, staking, governance and token transfers.

What you never touch. KYC documents, biometrics, names, addresses, credentials, presentations or any person record. None of it exists in the state you replicate — by construction, not by policy.

What you are paid for. Replicating the state machine correctly and staying live. No reward exists for subjective “identity validation work”, and no slashing rule punishes you for an identity decision you never make.

In short: you run professional, independently controlled infrastructure; you bond stake and sign blocks; you upgrade when token governance decides; and in return you share the scheduled emission and the fee market under rules that are published, capped and enforced by the chain itself.



02

What you secure

A consensus failure here would not just move balances — it would corrupt the trust fabric that issuers, verifiers and holders rely on.

2.1 A small, institutional state

AREA	WHAT THE CHAIN HOLDS
Registries	Accepted issuers and KYC-approved verifiers: keys, exact origins, permitted grades, authority state
Status	The latest signed root per issuer, its freshness bounds and any emergency update
Self-revocation	Recorded one-time nullifiers and the check of their proofs — in production on the single-node production chain since 24 September 2026, off at the distributed public network's genesis until governance switches it on there; its dedicated audit is a published milestone
Bonds and treasury	Issuer bonds, slashes, remediation cases and reserve-movement commitments
Governance	Council decisions with reason codes and evidence commitments; proposals; versioned parameters
Economics	Staking, delegation, distribution, fees and the supply ledger

No record identifies a holder, a credential or a verification. State grows with **issuers, verifier origins, validators, revocation-tree roots and governance records** — never with people, credentials or presentations: a billion credentials cost the chain what a thousand do, one root per issuer. A consensus takeover would let an attacker censor or reorder those roots and tamper with the registries — the trust fabric itself, not only balances.

2.2 Liveness is a user-facing property

The chain rejects status roots that are expired, stale, future-dated or valid for longer than policy allows, and every verifier treats a root older than **45 seconds** (the reference value) as stale and **fails closed**. The consequence is direct: **if the chain stalls, no fresh roots finalise, and within about 45 seconds verification fails closed everywhere**. An issuer's emergency revocation takes effect at finality, so the network's finality latency *is* its revocation latency. On most chains downtime costs rewards; here it also takes identity verification offline.

The ten-second figure seen throughout MintID is the lifetime of a holder-to-verifier presentation, not a chain requirement: presentations never go on-chain, and the chain does not finalise individual verifications.

2.3 The determinism boundary

Block execution is **self-contained**: no network call, no wall-clock time outside block time, no randomness, no hardware signer, no remote service, no external database and no foreign-function bridge runs while a block is executed. Every validator reaches the same result from the transaction bytes and the current state alone, and any new cryptography in a consensus path receives its own independent audit, published with its findings. For an operator this is good news: your node needs no oracle, no KYC connection and no outside service, and hardware-backed signing protects your votes from outside the state machine.



03

Consensus and the validator set

Anyone can run a node and bond; the top validators by capped voting power form the active set.

Admission is **permissionless**: an operator runs a node, bonds native tokens and registers a validator. The validators with the most **capped** bonded voting power form the active set; every other candidate is a standby validator or a delegator. There is no admission committee for validators — the compliance council has no say over who validates, and validators have no say over who is an accepted issuer.

PARAMETER	VALUE	STATUS
Consensus	Delegated proof of stake on CometBFT, through the Cosmos SDK	Decided
Active set	60 at genesis, growing toward 100 only by token governance, once fee-funded security supports it	Ratified point
Block time · finality	Two to three seconds · about five seconds under normal conditions	Candidate · objective
Voting-power cap	5 % of effective voting power per validator	Prior
Unbonding period	21 days	Prior
Minimum self-bond, jailing thresholds, slash fractions	Fixed before genesis, from the simulation	Open

Why start at 60. A young chain is cheapest to attack at genesis, and a smaller set concentrates the security budget while the fee market matures. Until bonded stake is self-sufficient, governance is expected to keep the set conservative, front-weight early emission toward validators and delay any feature whose compromise would be irreversible.

Why the cap matters to you. Rewards are shared by **capped** voting power (\$7.2), so piling stake onto the largest validators earns nothing extra. Stake is pushed toward a wider set of operators, which raises the Nakamoto coefficient the launch gate measures and gives smaller professional operators a structural place in the set.

04

What you need

A professional operator, independently controlled infrastructure, a self-bond — and a counterparty able to sign a service agreement.

4.1 Organisation

- **An accountable operating entity.** A genesis validator must be able to sign a fiat or stablecoin service agreement (\$5.5), disclose its self-bond and agreement status publicly, and meet its own tax and regulatory obligations.
- **Genuine independence.** Your keys and your votes are under your control and nobody else's; only then does your stake count as independent for the launch gate.



- **On-call capability and experience.** A round-the-clock incident process, because downtime here is visible to every verifier. Operators already running Cosmos-ecosystem infrastructure are the recruitment target for genesis.

4.2 Infrastructure

Validators are expected to run a **professional topology**:

- **Sentry nodes**, so the signing validator is never exposed directly to the public network.
- **Separated keys**: the consensus key that signs blocks apart from the operational key that controls stake.
- **Hardware-backed or remote signing** where possible, protected against ever signing twice at the same height.
- **Monitoring and alerting**, plus **snapshots and a restore plan** for fast replacement of a failed node.
- **Verified releases** only — published, reproducible builds that anyone can check against the source.
- **Diversity**: genesis recruitment sets geographic and hosting-provider targets.

4.3 Sizing and stake

The recurring load comes mainly from **issuer heartbeats** — each active issuer's root at least every 30 seconds, batched by relayers — not from the number of people using MintID. Ordinary validators keep current state plus a short history; **archival nodes**, an optional role, keep full history and evidence commitments.

No hardware classes or cost figures are published yet. Mainnet launches with **conservative resource limits** that grow only on measured evidence; bootstrap times will be **measured on the public adversarial testnet and published per hardware class**; and the reference operator's costs and the **minimum self-bond** are set by the pre-genesis simulation (\$7.5). Bonded stake is exposed to slashing (\$6) and stays locked for **21 days** when withdrawn.

05

The road to genesis

From today's single-validator networks to a genesis that is triggered by conditions, not by a calendar.

5.1 Where the project stands

MintID launches in stages behind published gates, under one overriding rule: **if a minimum is not reached, re-stage — never launch under-funded or under-secured**. Audits are milestones published with their findings, never gates. Windows are targets, not commitments.

STAGE	TARGET	WHAT IT MEANS FOR VALIDATORS
0 — Single-node production	now–2027	The single-node production chain and the public testnet with its KYC sandbox, one validator each; no public validator set; the simulation fixes genesis values
1 — Public offer	2027	MiCA Title II offer; proceeds fund, among other things, the bootstrap
2 — Mainnet	H2 2027–2028	Identity-only genesis with 60 validators, once the economic gate is met; audit reports published
3 — Recourse	2028–2029	Escrow and disputes, off the consensus path — no new consensus module
4 — Maturity	2030–2031	The set grows toward 100 by governance



The target is anchored to **24 December 2027**, when eIDAS 2.0 wallet-acceptance obligations take effect. Genesis is **condition-triggered** — a published traction criterion, an acceptable raise window and the delivered simulation and counsel outputs — and otherwise the single-node production mode simply continues.

5.2 The operator journey

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6
Prepare	Public adversarial testnet	Bootstrap agreement	Genesis registry	Operate	Operator floor
Study the protocol, request the specification corpus, build a professional topology	Run an independent validator through load, failure and attack drills	A fiat or stablecoin service agreement; keys and votes stay yours	Self-bond and agreement status disclosed in the public registry	Sign blocks, upgrade on schedule, vote, report	Renewable agreements for verifiable service while fees mature
now	before genesis	12-24 months	pre-genesis	from genesis	after bootstrap

5.3 The public adversarial testnet

No mainnet happens before a **public adversarial testnet** with independent validators, issuers and verifiers: load tests, node-failure drills, malicious transaction campaigns and governance drills. For operators it is the qualifying ground, where topology, failover, upgrades and monitoring are proven in public.

Testnet tokens are **worthless by construction** — a distinct denomination, an open faucet, no conversion to mainnet, no points program, and state that may be reset at any time. **No reward for testnet work is promised**; any recognition of testers is a discretionary decision made after the contribution.

5.4 The economic-security launch gate

Economic security is a launch criterion in its own right: genesis does not proceed until published, price-independent thresholds are met.

THRESHOLD	RATIFIED PRIOR
Bonded stake held by external parties, as a share of maximum supply	$\geq 20\%$
Independent validator operators	≥ 25
Nakamoto coefficient — the fewest validators that together hold a blocking share of voting power	≥ 7
Estimated attack cost in fiat, by a published methodology	From the simulation

The method is published before any offer opens. **Development and foundation accounts, and delegations traceable to them, are excluded**; stake bought in the public offer counts; contracted stake counts as independent only where the operator controls its own keys. The simulation must also evaluate *rented* security (shared-security or Bitcoin-staking checkpointing) for the first 12–24 months — adopting it is optional, evaluating it is not.

5.5 Bootstrap agreements and the genesis-validator registry

Before a market exists emission has no price, and token rewards outside the schedule may not be promised. Genesis validators are therefore recruited under **fiat or stablecoin service agreements for the first 12–24 months** — an instrument a professional operator can underwrite.

- **Keys and votes stay yours:** no agreement may give the operating group, or anyone else, control over them.
- **Disclosed, not hidden:** a public registry lists each self-bond and agreement status, related parties included.
- **Then the operator floor program** (§7.3). If the offer misses its invariant raise floor, the project re-stages — possibly resizing the bootstrap.

06

Obligations, slashing and guarantees

What you commit to, what can cost you stake, and what the protocol commits to in return.

6.1 Your obligations

Never double-sign. One consensus key, one active signer, always; failover must be designed so that it cannot sign twice at the same height.

Stay live. Sustained downtime is slashed and jailed — and on MintID it also takes verification offline (§2.2).

Keep your keys independent. Consensus and operational keys separated, hardware-backed where possible, under nobody else's control.

Validate only what the protocol defines. Signatures, freshness bounds and deterministic rules. You never judge whether a real-world identity is genuine, and you never inspect, store or index presentation data.

- **Upgrade on schedule.** Token governance decides upgrades and when they apply; a validator that is not ready stops signing and is treated as down.
- **Handle key incidents openly:** a suspected consensus-key compromise triggers emergency rotation and the incident process.
- **Govern and disclose.** Vote, explain your positions to delegators, declare your commission and keep your registry entry current.
- **Keep the firewall.** Paid off-chain services you run — mirrors, archives, verification — earn direct fees, never mixed with consensus rewards.

6.2 Slashing and jailing

Only objective, on-chain evidence can cost you stake.

EVENT	TREATMENT
Double-signing (equivocation)	Slash and permanent exclusion from the set
Sustained downtime	Slash and temporary jail, on missed-signature evidence
Invalid transaction or state transition	Rejected before finality; no reward
Consensus-key compromise	Emergency rotation and incident process; possible jail pending evidence
Alleged censorship	No slashing rule at launch — attribution is too subjective
Issuer fraud or verifier abuse	Not a validator matter: issuer-bond adjudication by the council, or verifier suspension



A slash hits everything bonded to the validator, **delegations included**. Fractions, downtime window and jail duration are fixed before genesis — not taken from internal networks.

6.3 What the protocol guarantees you

GUARANTEE	WHAT IT MEANS FOR AN OPERATOR
No personal data in state	No KYC, personal data, credential, presentation or per-person record — by construction
Self-contained execution	No oracle, KYC connection or remote service is needed to validate
Objective slashing only	No identity-specific slashing; issuer fraud is settled against issuer bonds, never your stake
Bounded state	Growth follows institutions, not people; resource limits rise only on measured evidence
A reward pool with one use	Validator emission only; no post-cap mint; no tax on stake
Neutral consensus	Off-chain service revenue never influences consensus rewards; basic verification stays free
No insider voting weight	Development and foundation accounts neither delegate nor vote while vesting or locked

07

Economics

A scheduled, declining emission shared by performance, a fee market with a validator-directed share — and no price anywhere in this manual.

Status of every figure in this chapter. The maximum supply is frozen; every other figure is a ratified band (points move only inside it, by governance) or a ratified prior (validated or argued against by the independent simulation). No token price, yield or return is stated or implied; before a market exists, emission has no price at all.

7.1 The security budget

The maximum supply is **108,000,000 tokens**, exact. The **reward pool** — 60 % of the cap, 64.8 M tokens — is the dominant genesis allocation (development 15 %, public-sale tranche 25 % within a 20–25 % band) and has **one use: validator emission**. The prior curve starts at **3 % of the cap in year one** (3.24 M tokens) and decays by **×0.95 per year**, strictly declining, with cumulative emission equal to the reward pool exactly: roughly 40 % of the pool is emitted in the first ten years and about 79 % within thirty. Emission is paid per block and rounds down, so it can only undershoot the schedule.

7.2 How rewards are shared

Each epoch's emission is shared among active validators **in proportion to their capped voting power, weighted by their signing performance**. Delegators share through the standard distribution path; you charge your **declared commission**; missed signatures cost you the performance share and, when sustained, lead to jailing.



Validators also earn **transaction fees** and the **validator-directed share of the protocol cuts** on the two flows that scale with adoption — the agent mint and lease (flow A) and consensual disclosure (flow C):

PARAMETER	RATIFIED BAND	PRIOR
Flow-A protocol cut	A governed parameter under review	—
Allocation of each A/C cut	Governed parameters	Final form under review

The allocation of each cut among its destinations is a set of governed parameters whose final form is under review. The foundation share is earmarked — first for the operator floor program, then for foundation operations, under a public annual report — and is never distributed to token holders. Dispute fees and premium verification services carry **no** protocol cut and never influence consensus rewards; there is no usage tax, and basic verification is free.

7.3 Contracted income in the early years

- **Bootstrap service agreements** (\$5.5), in fiat or stablecoin, for the first 12–24 months.
- **The operator floor program** afterwards: renewable fiat or stablecoin agreements for a set number of independent operators, funded by the foundation share (the operating budget is only a bridge), paying for **verifiable service** — uptime, sentry topology, monitoring — and **never for stake**, never for subjective work, and never through an on-chain subsidy indexed to a price, since no price oracle may enter block execution. Its size and terms come from the simulation.

7.4 After emission

When the pool is exhausted, the validator budget is the fee market: transaction fees plus the validator-directed share of the cuts. If the simulation shows that this does not sustain the target set, a **succession ladder is committed, in order**, with no step skipped: (1) governed adjustment of the cut points; (2) a protocol-state rent, redirected pro rata to validators; (3) supplementary shared security. **A post-cap mint is prohibited by construction and permanently excluded from the ladder.**

7.5 What the simulation will publish for operators

The independent simulation — external by requirement and re-runnable by the economic review — fixes the minimum self-bond, the gate thresholds, the emission and cut points and the post-emission budget. It also publishes a **reference-operator break-even analysis**: cost, self-bond and commission scenarios for a marginal professional validator under adverse, base and growth adoption, stating when it breaks even without the floor program and what program budget closes the gap. Until then, **this manual quotes no earnings, costs or hardware prices.**

08

Governance: where you have power

Token governance owns the software; the compliance council owns operational gates; validators never judge identities.

BODY	DECIDES	YOUR ROLE
Token governance (stake-weighted)	Upgrades, consensus and protocol parameters — including the set size, the council's size and threshold, and the cut points	Full — your stake votes
Compliance council (5-of-9 recommended)	Issuer and verifier admission, suspension and revocation; bond adjudication; co-signing protected treasury actions	None — it never changes software
Reserve controls (council + custodian)	Movements of the off-chain remediation and security reserve, under timelock	None — rewards are a prohibited use
MintID Foundation (Dutch <i>Stichting</i>)	Performs the genesis, holds the treasury and lock-ups, funds the operator floor program	None

Token governance is live from genesis; the council takes over the operational gates once seated. The separation is deliberate: validators secure a neutral state machine, and a different, accountable body decides whether an issuer may operate. **Accountability is observable:** the Genesis Allocation Statement, whose hash is committed in the genesis file, lists every genesis address with its label, vesting, custody and voting restriction; the transparency report covers council actions, slashes, root liveness, genesis-address movements, service-agreement counterparties and related-party flows — never holder data.

09

For delegators

Delegating puts your tokens behind a validator's work — and behind its mistakes.

A token holder who does not run infrastructure can **delegate** stake to a validator. Delegated stake adds to its voting power, earns a share of its rewards after commission, and is **exposed to its slashing**; withdrawing takes **21 days**. Under the framework's standard governance a delegator may vote directly; otherwise its validator's vote counts for its stake. **Choosing a validator** means reading the public record, not promises:

- **Signing performance** — rewards are weighted by it, and sustained downtime is slashed.
- **Commission, self-bond and independence** — on-chain and in the registry, including any service agreement or related-party position.
- **Voting power and diversity** — stake piled onto validators near the 5 % cap earns nothing extra; spreading it across operators, regions and hosting providers strengthens the network you hold.

Nothing in this manual is a recommendation to acquire, hold or delegate tokens, and no return is stated or implied.



10

Risks, stated plainly

Operational, economic, regulatory and delivery risks — named, not softened.

- **No price, no market, no promised return.** There is no market or price before a MiCA Title II offer and admission to trading, and nothing guarantees one, or its level; early on, the underwritable income is the service agreement.
- **Pre-genesis uncertainty.** Priors can move inside their bands; self-bond, slash fractions and jailing thresholds are not yet fixed; genesis may slip or re-stage, and the bootstrap may be resized.
- **Operational slashing and visibility.** Double-signing means permanent exclusion and downtime a slash and a jail, for you and your delegators; a chain halt is visible to every MintID user within about 45 seconds.
- **Post-emission budget.** The fee market may not sustain the target set without the committed ladder; the adverse adoption case will be published, not averaged away.
- **Cryptographic delivery.** The proof core is built and in production on the single-node production chain; an independent audit of its implementation is scheduled and its findings will be published. Holder self-revocation, the only proof verified in block execution, has been in production on the single-node production chain since 24 September 2026; on the distributed public network, switching it on is a governance decision every validator then enforces, with its own audit published as a milestone.
- **Regulatory.** The token is designed as a MiCA Title II “other crypto-asset”; the offer, service-agreement treatment and tax are subject to qualified legal review. Operators remain responsible for their own obligations.
- **Related-party concentration.** Development, the first issuer and verifier, the reference SDK, the anchor product and pre-genesis funding sit in one group (CONECTIA): the answer is disclosure and equal on-chain terms, and the independent economic review is the only arm’s-length opinion.

APPENDIX A

Validator values at a glance

VALUE	STATUS	FIGURE
Maximum supply	Frozen	108,000,000 exact · no post-cap mint
Emission	Sums to the pool	Prior 3 % of cap in year one, $\times 0.95/\text{yr}$
Active set · power cap · unbonding	Point · priors	60 → 100 by governance · 5 % · 21 days
Block time · finality	Candidate · objective	2–3 s · about 5 s
Self-bond, slashing, jailing	Open	Fixed before genesis
Launch gate	Priors	≥ 20 % external · ≥ 25 operators · Nakamoto ≥ 7
Compensation	Ratified policy	12–24-month agreements, then floor program
Allocation of each A/C cut	Governed parameters	Final form under review



VALUE	STATUS	FIGURE
Status freshness	Governed	30 s heartbeat · 45 s max age · fail closed

MintID Validator Manual v0.2, September 2026 · prepared by the MintID Foundation, a Netherlands Stichting · non-normative; the specification corpus governs · not investment advice · not a MiCA crypto-asset white paper and not an offer of any crypto-asset.