

MINTID · EXECUTIVE EDITION

Executive Edition

PUBLISHED BY

MintID

Developed and operated by the CONECTIA group · related parties disclosed in §6

KYC-backed identity and accountability for the agentic era. *Zero-knowledge identity layer for agents.* Verified once, proven anywhere, revealed nowhere — for people and for the AI agents they deploy. · v1.0 · 2026-10-03

Contents

01	MintID in one page	3
02	The problem and the thesis	4
03	How it works	5
04	Design choices that define the system	6
05	Token economics — bands, priors, and what is fixed	7
06	Governance, the Foundation and related parties	8
07	Launch plan	10
08	Where it stands, what remains, and the risks	11

01

MintID in one page

The whole argument in one page: what MintID is, why it matters, what is different and where it stands.

The idea. Do KYC once, with a regulated issuer; then prove what a counterparty needs — “*assurance $\geq$ A3*”, “*over 18*”, “*credential active*”, “*backed by an accepted issuer*” — as often as needed, in ten-second zero-knowledge presentations, **without ever revealing who you are and without anything identifying ever touching a public ledger.**

What it is. MintID is a sovereign, permissionless proof-of-stake Layer-1 (Cosmos SDK and CometBFT) whose only job is to be the *public trust layer* for identity: who the accepted issuers are, whether they are in good standing and bonded, which verifiers are KYC-approved and bound to which domains, and — every 30 seconds — a compact **status root** per issuer that lets a verifier check, failing closed, that a credential is still valid. Everything else — the KYC evidence, the credential, the proof — stays off-chain, under the holder’s control.

Why it matters. Identity systems fail in two opposite directions: the ones that work do so by *surveillance* (every check leaks a durable identifier to someone who keeps it); the ones that protect privacy usually *abandon accountability* (keys with no liable human behind them). MintID separates the two cryptographically — the claim is provable, the identity is not — while keeping a governed, bonded, on-chain-checkable chain of accountability from every proof back to a regulated issuer. Autonomous AI agents make this urgent: they act in fleets at machine speed, and the “know-your-agent” rails shipping today restore accountability by revealing the human’s identity to every seller.

0

identities, credentials or presentations written on-chain

10 s

lifetime of a fully-bound zero-knowledge presentation

30 s

status-root heartbeat per issuer, fail-closed when stale

108M

native tokens, a hard cap that is exact and immutable

What is different.

- **Nothing identifying on-chain, ever** — no KYC, personal data, credential, serial, presentation or per-holder record; state grows with issuers, verifiers and validators, never with people. A billion credentials cost the chain what a thousand do.
- **Accountable, bonded issuers**, admitted by a compliance council, with slashable native-token collateral that gates their right to operate and a separately scoped emergency key.
- **Ten-second, fully bound presentations** verified online against finalised state, with a verification path that is free by design.
- **Human-backed agent identity**: an agent proves it is operated by a KYC-verified, liable principal at grade $\geq$ G, within scope S, with $\geq$ F of self-custodied recourse (USDC, EURC or BTC) behind it — without revealing who, and without two agents of one person being linkable.
- **Identity leaves only by consent or due process**: a priced commercial disclosure rail that defaults to refusal, and a dispute rail that settles with money before it touches identity.
- **A hard-capped, transparent token** (108,000,000, exact) with no anonymity-enhanced transfers, no dividends and no backing.



Where it stands. The chain, the verifier service, the issuer status plane and a first issuer service, a client SDK, the public testnet with its KYC sandbox, and the single-node production chain on which ZadQ, the first product built on MintID, runs its pilot exist, and the proof core is built and in production. Launch is **staged and condition-triggered**: identity-only mainnet first (target H2 2027, ahead of the eIDAS 2.0 wallet-acceptance date of 24 December 2027), the financial-recourse rail on organic demand, financed by a MiCA Title II public offer executed in full — and *nothing* is for sale until that white paper is notified.

Legal posture. This is a condensed, non-normative companion to the MintID Protocol Whitepaper v1.0. It is not the MiCA Title II crypto-asset white paper; no price exists; every economic figure is a ratified band or an argued prior, subject to the independent pre-genesis simulation; items marked (*counsel*) await legal review. The frozen specification corpus governs and is available on request.

02

The problem and the thesis

The proof of a claim and the identity of the claimant travel together; MintID separates them.

Two failure modes, one root cause. Mainstream identity — federated login, per-service KYC, document-upload age checks — assumes that *knowing who someone is* is the price of *trusting what they claim*; the result is structural over-collection that data-protection law now treats as a liability. The privacy-preserving alternatives solved the leakage but gave up the liable, verified party that regulators and counterparties need. Both share one root cause: **the proof of a claim and the identity of the claimant travel together**. Agents make it urgent — around 50 non-human identities per human already (Omdia/IBM), more than a billion active agents projected by 2029 (IDC), no verifiable link to a liable party, no scoping, no recourse — and the “know-your-agent” primitives every major payment network shipped by April 2026 restore accountability by **revealing the principal’s identity to the seller**.

The thesis. Accountability can be *provable and funded* while identity stays private by default:

LAYER	WHAT IS PROVEN	WHAT IS NEVER REVEALED
Person	Backed by an accepted issuer at grade $\geq G$; over 18; active; unexpired	Name, date of birth, document, exact grade, expiry, credential identifier
Agent	Operated by a KYC-verified, liable human at grade $\geq G$, within scope S, with $\geq F$ of recourse	Which human; which sibling agents belong to the same human
Dispute	Harm proven in zero knowledge against the disputed session; paid from escrow (L0); minimal fraud signal (L1)	Identity — until a due-process determination (L2), never by payment alone

What the market validates. MintID does not compete for the low-assurance mass segment the payment networks own. Its validated, unserved niche is *privacy-preserving, funded, regulated-grade backing* — sellers and agents with meaningful economic volume, regulated business counterparties, and the EU sectors obliged to accept wallet-based identity from December 2027. Verification is free by design; the protocol earns only where adoption scales — agent mint and lease, and consented disclosure.



03

How it works

Two planes: everything that identifies a person stays off-chain; the chain holds registries, commitments and economics.

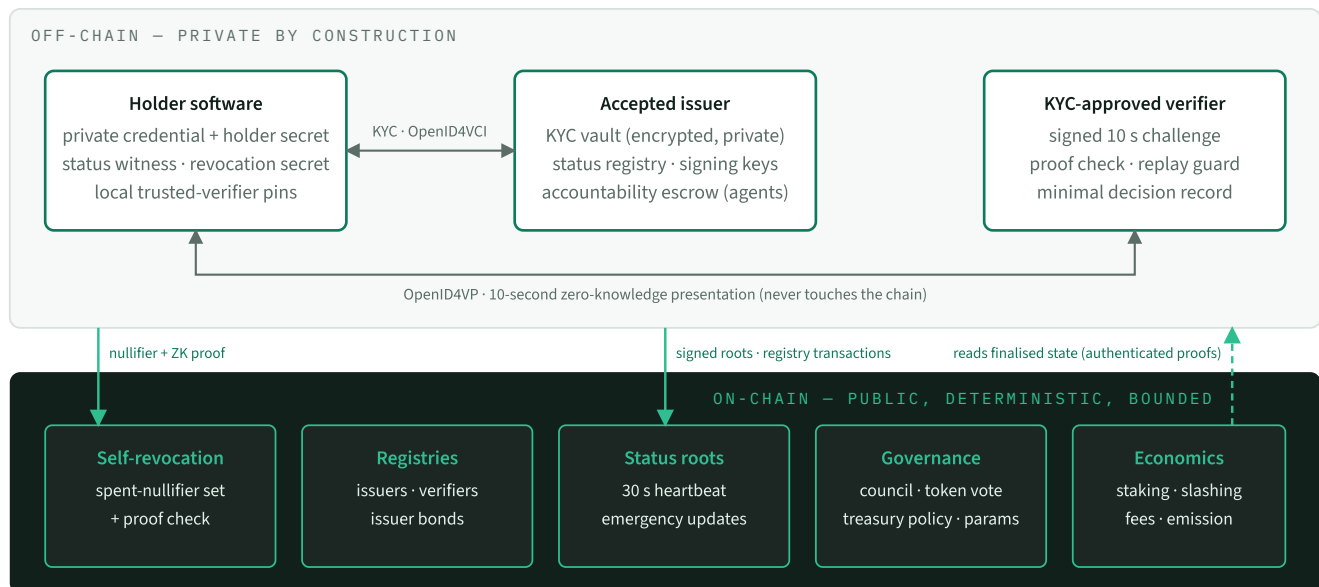


Figure 1 — Two planes. Everything that identifies a person stays in the off-chain plane; the chain holds registries, commitments and economics. Solid arrows write to chain (issuer roots, holder nullifiers); the dashed arrow is the verifier's read of finalised state.

The life of a credential, in six steps.

- 1. Admission.** A KYC organisation is reviewed by the compliance council (until the council is seated, by token governance, voted today by the chain's single validator), registers its signing keys and a separately scoped *emergency status key*, is granted permitted assurance grades (A1–A4), and locks a native-token bond of at least the governed minimum. Only then can it become active — the bond is a condition of operation, and a slash that exhausts it suspends the issuer in the same transition.
- 2. Issuance.** The person completes KYC; the issuer keeps the evidence encrypted in its private vault and delivers, over OpenID4VCI, an **anonymous credential** — signed blind, bound to a secret only the holder knows, carrying a private grade, a validity window and a private status reference — plus a status witness. At the next 30-second heartbeat a new signed **status root** is finalised on-chain and the credential becomes usable. No transaction records that it was issued.
- 3. Presentation.** A KYC-approved verifier, registered on-chain with exact HTTPS origins and request keys, issues a signed, single-use challenge that states the claims it needs and expires within ten seconds. The holder's software checks the verifier against its local trust pins, produces **one zero-knowledge proof for all requested predicates**, and returns it encrypted. The verifier re-checks finalised state, applies a fixed set of acceptance conditions, consumes the challenge so it can never be replayed, and keeps a minimal decision record. **Nothing is written to the chain.**
- 4. Status.** Roots every 30 seconds; the chain enforces the time bounds as consensus rules; a verifier fails closed at 45 seconds of staleness. Issuer revocation enters the next root (≤ 30 s) and is refused everywhere in under a minute, or at once through the emergency key. **Holder self-revocation** is a chain transaction carrying a one-time nullifier



and a zero-knowledge authorisation proof through a privacy relay: it reveals neither the holder nor a credential identifier, and the issuer removes the credential within a consensus-enforced grace or has its roots refused: under two minutes, everywhere, at the reference values.

5. **Renewal and recovery.** Renewal is a new, publicly unlinkable credential from any accepted issuer. Losing the holder's keys has exactly one recovery path: fresh KYC and a brand-new credential. No social recovery, no custodial back door.
6. **Agents.** A verified human proves in zero knowledge that they hold an unrevoked credential; the issuer *mints* a fresh, unlinkable agent credential carrying a backing assertion and a delegated scope, and records the only link between agent and human in its private accountability escrow. The chain sees nothing new.

04

Design choices that define the system

Six invariants, and the standards decisions that follow from them.

1 — The chain never learns who anyone is. · **2 — State scales with institutions, not people.** · **3 — Consensus is deterministic and self-contained** (no network, clock, randomness, hardware signer, remote service or foreign-function bridge in block execution). · **4 — Backing is provable, identity is not.** · **5 — Disclosure is rail-segregated and, on the commercial rail, consensual** — no payment is ever a lawful basis for disclosing personal data. · **6 — The value layer is transparent and hard-capped**, with no anonymity-enhanced transfer modes.

DECISION	INSTEAD OF	WHY
Sovereign Cosmos SDK application chain on CometBFT	Contracts on a general-purpose L1; a rollup	The privacy invariants are chain-wide properties a shared VM cannot promise; registries, council, bonds and root policy are native capabilities with native economics; nothing of consensus, P2P, staking or light clients is rewritten
Go / Rust / Python as a security boundary	One language everywhere	Go owns consensus-visible state; Rust owns cryptography (never in a block-execution path without its own published independent audit); Python owns simulation, testing and automation — never keys or consensus
Standard, deterministic primitives and authenticated state reads	Novel primitives; trusted RPC	Widely audited signatures and hash trees in the consensus path; verifiers read finalised state through light-client-verified proofs, adding no new cryptography to consensus
Anonymous credentials (AnonCreds lineage) as the primary profile	SD-JWT VC / ISO mdoc; DIDs	Unlinkability across verifiers, predicate proofs and non-revocation without a correlatable identifier — properties salted-hash disclosure formats do not give. HAIP is used for security guidance only; SD-JWT and mdoc interoperability is not claimed until a separate profile is certified
A1–A4 anchored on eIDAS, squared with ISO/IEC 29115; freshness as a separate band	A bespoke vocabulary, or one foreign framework adopted wholesale	Europe's regulators and the EUDI Wallet speak eIDAS first; ISO gives the four-level backbone; no framework attaches a validity period to a level, so recency lives in a freshness band published by the issuer — never a date, and not a presentation predicate



DECISION	INSTEAD OF	WHY
OpenID4VCI / OpenID4VP transports	Bespoke transports	The same protocols as the European Digital Identity Wallet — eIDAS 2.0-compatible by construction — plus chain-native verifier registration and exact-origin binding
One verification pipeline, thin clients	Per-language reimplementation	Acceptance logic lives in one place, with one conformance suite; the ten-second lifetime is a constant nobody can weaken
x402 + Web Bot Auth transport profile for agent payments	A parallel payments rail	The facilitator is the registered verifier; a ladder from anonymous → identified software → identified software with an accountable human
MiCA Title II as the only offer path; AEC invariant; no anonymity-enhanced reserve	Private pre-sale, SAFTs, shielded transfers	An identity network courting regulated issuers cannot afford a contestable token characterisation; privacy lives in the credential layer, not the money layer

Security posture. Every party is assumed potentially malicious. Objective-evidence-only slashing; a launch gate on economic security (priors: $\geq 20\%$ externally bonded, ≥ 25 independent operators, Nakamoto coefficient ≥ 7); a council threshold of 5-of-9, with an independent custodian co-signing reserve movements; and a committed slate of quality milestones — two chain audits, a cryptography audit, a penetration test, an economic review, a public adversarial testnet and a bug bounty — each scheduled and published with its findings, none a precondition of a release.

05

Token economics — bands, priors, and what is fixed

A security asset with a hard cap and a declining emission — and no price in this document.

No price appears in this document; the offer price, if an offer is made, exists only in the MiCA Title II white paper. The maximum supply is frozen; everything else is a ratified **band** (binding) or **prior** (an argued working point that the independent simulation validates or argues against). This is disclosure, not an offer.

What the token is for. The economic-security asset: validator bonding and delegation, issuer bonds, fees, registry leases, governance-weighted operations. It is not a stablecoin, not backed, not price-supported, not dividend-bearing, and not a claim on anyone’s revenue. It confers no distribution of any kind, and the token is a *launch vehicle for network security*, not a scarcity instrument.

VALUE	STATUS	FIGURE
Hard cap	Frozen	108,000,000, exact, counted against everything ever minted; no post-cap mint, ever
Genesis allocation — development / public sale / reward pool	Bands 15 / 20–25 / $\geq 60\%$	Prior 15 / 25 / 60 % (16.2 M / 27 M / 64.8 M)

VALUE	STATUS	FIGURE
Emission	Rule: cumulative emission equals the reward pool; strictly declining	Prior 3 % of the cap in year one (3.24 M) , ×0.95 per year — about 40 % of the pool in ten years, 79 % in thirty
Protocol cut on agent mint and lease fees (flow A)	Governed parameter	Under review
Allocation of each A/C cut	Governed parameters	Final form under review
Agent mint and lease-fee prices	Set before genesis	From the simulation; the lease prior is a competitive ceiling, with a cross-issuer anti-sybil floor
Genesis validator set · voting-power cap · unbonding	Priors	60 (→ 100 by governance) · 5 % · 21 days
Vesting and lock-up for insiders	Policy	Four-year continuous vesting, one-year cliff; 12-month lock-up; no delegation, no vote while it applies; excluded from the launch gate
Raise floor	Ratified invariant	\$4.0 M net of statutory withdrawals — below it the project <i>re-stages</i> , never launches under-funded
Price mechanism	Ratified	A single fixed price, no tiers, no discounts; every other offer term is set only in the MiCA white paper

Five flows, one firewall. Only two flows carry protocol cuts: **A** — agent mint and lease — and **C** — consented disclosure (a percentage plus a fixed per-disclosure floor). Issuer registry fees (**B**) are protocol fees; the protocol cut on agent flows and its allocation are governed parameters; their final form is under review. Arbiter fees (**D**) and premium verification services (**E**) are off-chain revenue that **must never influence consensus rewards**, and **basic verification is free by design** — no usage tax exists or is planned. The **foundation share** is earmarked (the operator floor program, then foundation operations, with a public annual report) and is **never distributed to holders**. After the reward pool is exhausted, the security budget is the fee market; if the simulation finds it insufficient, a succession ladder is committed in order — cut points inside the bands → protocol-state rent → shared security — and a post-cap mint is excluded by construction.

06

Governance, the Foundation and related parties

Software is governed by token holders, compliance by a threshold council, and the whole by a Dutch foundation.

Two organs, never conflated. Token-weighted governance owns the software: upgrades, consensus parameters and every versioned protocol parameter. The **compliance council** — a threshold-vote body, recommended 5-of-9 — owns the operational gates: it admits, suspends and revokes issuers and verifiers, adjudicates bonds with public reason codes and evidence commitments, and co-signs protected treasury actions. It never changes software or parameters, and on the dispute-path identity reveal its role is supervisory and *after the fact* only: **the arbiter decides and certifies, the issuer releases, the council supervises.**



The MintID Foundation. The steward is a dedicated **Netherlands *Stichting*** seated in Amsterdam. **The Foundation is being incorporated by the founder and stays dormant until the public-offer route is chosen:** it holds no treasury, enters no contracts, seats no sponsors and receives no services (ADR-0016 §5). The single-node production chain is operated by the CONECTIA group as a disclosed related party, and the code is published under an Apache-2.0 licence (ADR-0014, ADR-0016). On the public-offer route it performs the genesis, holds the treasury and lock-up commitments, publishes the Genesis Allocation Statement (its hash committed in the genesis file, reconcilable from block 1) and, as offeror, fixes the notification authority under MiCA Art. 3(1)(33): the Dutch **AFM**. Governance is staged, and the staging is itself ratified: the founder is sole director **only** for the pre-offer phase; before any white paper is signed, independent members join the board, statutory locks take effect (a cap on unrelated activity, the founder below a board majority, a devolution clause) and the council is constituted as an organ of the Stichting. The Foundation has no protocol revenue role — sponsorship seats, if opened, buy voice and visibility and never a vote (ADR-0017) — and no debt relationship with the implementing group in either direction.

Related parties, disclosed. MintID is conceived and built by the **CONECTIA group** (Conectia OÜ, Estonia, and Conectia PRO, its wholly-owned Spanish operating company). This document does not claim an independence it does not have:

ROLE	HELD BY	DISCLOSED FLOWS
Founder	Marc Molas	Founder of MintID; beneficial owner of the CONECTIA group; founder-director of the Stichting at incorporation. Recused from every Foundation decision that concerns the group; the founder-separation commitments of ADR-0017 apply before any white paper is signed
Development company	Conectia PRO (Spanish SL, 100 % Conectia OÜ)	Development allocation; operating budget from proceeds. Pre-genesis work is CONECTIA's own R&D at its own cost: no advance, no reimbursement, no debt in either direction
First accepted issuer · first registered verifier	CONECTIA group	Issuer fees and disclosure brokerage — the same admission path as any issuer (a governance proposal, voted by the chain's single validator until the compliance council is seated), same slashable bond, same 30-second roots, verifiable on-chain from block 1
Reference SDK / premium-services operator	CONECTIA group	Direct service revenue, firewalled from consensus rewards
Anchor-product operator (ZadQ)	CONECTIA group	x402 seller-verification service revenue (fiat); base verification stays free
Operator of the single-node production chain	CONECTIA group	Operates the chain's infrastructure; no on-chain money flow beyond nominal fees and the bond; activity reported as a related-party pilot, excluded from the traction criterion
Pre-genesis R&D funder	CONECTIA group	An internal pre-genesis budget of €400,000 spent by CONECTIA on MintID as its own R&D; disclosed in amount; no services on credit to the Foundation, no reimbursement, no claim on proceeds
Steward	MintID Foundation	Being incorporated by the founder; dormant until the public-offer route is chosen; on that route, treasury custody, grants, sponsorship dues and the foundation share; no protocol revenue role; no debt with the group

The independence that *is* claimed is methodological — every figure sourced, every model re-runnable — and the independent pre-mainnet economic review remains the only genuinely arm's-length opinion. Transparency

reporting covers issuer and verifier states, council actions, slashes, root liveness, reserve activity, labelled-address movements, vesting releases and related-party flows — never holder data.

07

Launch plan

Each stage opens only when its published gate is met; if a minimum is not reached, the plan re-stages.

The master rule. Launch in stages behind published gates; if a minimum is not reached, re-stage — never launch under-funded or under-secured. Audits are milestones published with their findings, never gates. Identity first; the recourse rail on organic demand; genesis triggered by conditions with a target date.

STAGE 0 Single-node production Production chain, frozen specifications, Foundation, first issuer and verifier, simulation and counsel now → 2027	STAGE 1 Public offer MiCA Title II white paper, AFM notification, offer, admission to trading 2027	STAGE 2 Identity-only mainnet Credentials, presentations, status roots, free verification, 60 validators H2 2027 → 2028	STAGE 3 Financial recourse Escrow, disputes, arbiter market, consented disclosure 2028 → 2029	STAGE 4 Maturity Many issuers, a growing agent population, active set toward 100 2030 → 2031
--	--	---	---	--

STAGE	TARGET	GATE
0 — Single-node production	now → Gate 1	The single-node production chain, in production since 20 September 2026 and operated by the CONECTIA group (ADR-0014, ADR-0016) · proof core in production · code Apache-2.0 · Foundation being incorporated, dormant · financing route decided at the Gate-1 go/no-go · on the public route: simulation, counsel, trademark, Foundation board and statutory locks
1 — Public offer	2027	White paper cleared by counsel and notified; board and locks before signature; bank and custodian; \$4.0 M net floor , else re-stage
2 — Identity-only mainnet	H2 2027 → 2028	Economic-security thresholds met in measurable units · Genesis Allocation Statement published · audit reports published; no escrow or disputes yet
3 — Financial recourse	2028–2029	Organic-demand activation criterion · unmasking governance (<i>counsel</i>) · circuit and escrow-contract audit reports published
4 — Maturity	2030–2031	Continuous reporting and annual audits

Windows are targets, not commitments: each stage opens only when its gate is met.

The eIDAS clock. On **24 December 2027** the eIDAS 2.0 relying-party acceptance obligations for the European Digital Identity Wallet take effect; sectors across the EU will be choosing verification stacks, and MintID’s wallet speaks the same protocols. That date is why the simulation and counsel work is sequenced to make a 2027 offer window achievable.

Cold start: first implementer and anchor product. The CONECTIA group operates the first accepted issuer and the first verifier on **undifferentiated terms** — same admission, same bond, same roots, verifiable on-chain — and builds the issuer and verifier services and the holder library under a permissive licence. The **anchor product, ZadQ**

(zadq.app), is an **x402 seller-verification service** and the first product built on MintID, run by the group as its own product line: a pay-per-request seller proves that an accountable, KYC-verified person or organisation stands behind its payment address, without revealing who; explorers and buying agents consume the signal through the free path and publish their own signed verdicts. It needs no protocol change, targets sellers with meaningful economic volume and regulated business counterparties, and sells **privacy, funded recourse and compliance by design — not cost savings**. Its first version runs with conventional issuer-signed attestations on the seller side, **makes no zero-knowledge claim for that rail**, and migrates to the zero-knowledge path next, now that the proof core is in production. **ZadQ runs on the single-node production chain**, stewarded by the Foundation and operated by the CONECTIA group — not yet the distributed network, and excluded from the traction criterion — changing one thing at a time: first the proof form, then the topology.

Condition-triggered genesis. Genesis fires only when all three hold: (1) the published **traction criterion** — at least N attested x402 sellers with at least R % retained after 90 days, and at least M active, independent registered verifiers (the promoter group excluded), both sustained for two consecutive quarters, with N , M and R calibrated by the simulation, measured only in registry-based or aggregate units, and with nothing measured on the single-node production chain counted; (2) an acceptable raise window; (3) the simulation and counsel outputs delivered. Otherwise the single-node operating mode continues, funded by the first implementer as its own R&D with no operating loss — product marketing unrestricted, token marketing prohibited until a white paper is published.

08

Where it stands, what remains, and the risks

What exists today, what must still be fixed, and what could go wrong.

Built (October 2026). The application chain with its issuer, bond, verifier, status, council, treasury, parameter and fee capabilities, pinned by cross-language test vectors and determinism tests; the verifier service with the full acceptance pipeline, authenticated chain reads and a versioned service contract; the issuer status plane and a first issuer service behind a provider-neutral KYC interface, with a real identity-verification provider behind it, including the conventional seller attestations of the ZadQ pilot; the proof core — credential profile, issuance, selective-disclosure presentations and the non-revocation path — built and **in production**, with its construction, proof system and library revision frozen; holder **self-revocation**, in production on the single-node production chain since 24 September 2026; the client SDKs (Python, TypeScript, MCP) and the holder library; simulators and adversarial tests; the public testnet, with its KYC sandbox, where third parties test (its status is stated in the developer documentation); and the single-node production chain on which ZadQ runs.

Not yet done. The independent audit of self-revocation is a scheduled milestone. An independent audit of the proof core's implementation is scheduled and its findings will be published. The distributed mainnet of Stage 2 has not launched: there is no token, no token price and no public validator set.

Must be fixed before genesis. Allocation and emission points inside the bands; the protocol cut and the allocation of the cuts, governed parameters under review; economic-security thresholds; the issuer bond minimum, slashing and remediation; council selection and quorum; the validator cap, self-bond and unbonding; freshness limits after benchmarks; jurisdictions, the counsel sign-off on the KYC policy, and retention; agent-economy parameters and — an activation-blocking governance item for the agent layer only — the accountability-escrow disclosure policy.

Risks, stated plainly.



- **Competitive timing** — transparent know-your-agent rails already ship at every major payment network; MintID's niche is validated but narrow, and the answer is sequencing, not repositioning.
- **Cold start** — two-sided; addressed by the first implementer and ZadQ, the anchor product, with success criteria defined in advance and measured.
- **Cryptographic delivery** — the proof core is built and in production; self-revocation, the highest-risk consensus item, has been in production on the single-node production chain since 24 September 2026, and is switched off at the distributed public network's genesis, where switching it on is a governance decision, with its audit published as a milestone.
- **Regulatory** — MiCA execution, the Foundation's statutes, GDPR and consent texts, AI Act conformity and unmasking governance are subject to counsel; the design chose the strictest reading at each point.
- **Economic** — the token case rests on bands whose points are not yet fixed; adverse scenarios show a thin protocol P&L and must be presented, not averaged away; the raise floor is invariant, and re-staging is the answer to a weak offer.
- **Related-party concentration** — development, the first issuer, the reference SDK, ZadQ, the operation of the single-node production chain and pre-genesis funding sit in one group; the answer is disclosure, equal on-chain terms, and excluding the pilot from the traction criterion.

Where to read more. The full *MintID Protocol Whitepaper v1.0* (architecture, chain, credential protocol, agent layer, standards rationale, security, economics, governance, launch plan, glossary, requirement index); the MintID Issuer, Verifier & SDK, Holder and Validator manuals; and the frozen specification corpus, available on request.

MintID Executive Edition v1.0, 3 October 2026 · prepared by MintID, developed and operated by the CONECTIA group; the MintID Foundation, a Netherlands Stichting, is being incorporated and stays dormant until the public-offer route (related parties: §6) · non-normative; the specification corpus governs · not a MiCA crypto-asset white paper and not an offer, solicitation or marketing of a crypto-asset · not legal, tax or investment advice.

