



MINTID · ROLE MANUAL

MintID Issuer Manual

How a regulated KYC organisation becomes an accepted MintID issuer, what it must operate, and what it commits to once it is live.

PUBLISHED BY

MintID Foundation

Netherlands Stichting, Amsterdam · related parties disclosed

VERSION

0.2 · October
2026

AUDIENCE

KYC providers and regulated
issuers

NETWORK

Single-node
production

STATUS

Not legal
advice

Contents

01	The issuer role in brief	3
02	What the protocol asks of you, and what it never asks	4
03	The path to admission	5
04	The compliance workload	6
05	The issuer services you operate	8
06	Infrastructure, costs and revenue	9
07	Continuous operation	10
08	Issuing for agents	11
09	Where things stand today	12
10	Risks and limits	13
–	References	14

Status and scope. Public role manual for issuers, version 0.2 (September 2026). MintID runs in production on a **single-node chain**, which is never a place to test; the distributed mainnet has not launched, there is no public issuer admission yet and no token price. **The public testnet**, with its KYC sandbox, is where third parties test: the same software and parameters, an issuer that verifies nobody (the caller chooses the outcome of every KYC session) and nothing issued that carries weight. It shows the whole issuance journey from the holder's and the verifier's side; it has no registration path for an issuer of your own, which the local stack of the main repository lets you run on your own machine. 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 economic value mentioned here is a ratified band or prior; the independent pre-genesis economic simulation fixes the final points, and values not yet fixed appear as cost categories. This manual is **not legal advice**, and it is **not a MiCA crypto-asset white paper**: nothing is for sale. If it differs from the specification corpus (available on request), the corpus governs.

01

The issuer role in brief

The issuer is the only party in MintID that sees personal data, so accountability and compliance concentrate there.

An **accepted issuer** is a regulated organisation, such as a KYC provider, bank or trust-service provider, that verifies people and organisations to a recognised standard. It has been admitted by the compliance council and has locked a slashable bond in the native token. It verifies a person once, issues an **anonymous credential** into that person's own holder software, and keeps the credential's status current for as long as the credential lives. Relying parties never learn who the holder is. They learn only that an accepted, bonded issuer stands behind the claim.

0

personal data, credentials or issuance events you ever write on-chain

30 s

maximum interval between your signed status roots

45 s

root age at which every verifier fails closed on your credentials

A1–A4

assurance grades you assign, with freshness bands alongside

What an issuer does.

- **Verifies identity** (KYC for people, KYB for organisations) and assigns a private assurance grade from A1 to A4, within the grades the council permits.
- **Issues anonymous credentials** that the holder controls. The evidence stays encrypted in the issuer's vault, and the issuer never holds the holder's secrets.
- **Publishes a signed status root at least every 30 seconds.** This heartbeat lets any verifier confirm a credential is still valid without learning anything about anyone.
- **Revokes** credentials through the next root, refused by every verifier in under a minute, or immediately with a separately scoped emergency key.
- **Mints agent credentials** for verified people who deploy AI agents, and keeps the private *accountability escrow* that links each agent to its human.
- **Backs its work with a bond**, which the council can slash on evidence.



How an issuer earns. The protocol gives issuers two revenue lines: a per-agent mint fee with a recurring lease and, from the financial-recourse stage, an optional fee for brokering consented disclosure (Chapter 6). Basic verification is free by design, because that drives adoption. Compliance, vaulting, hardware signing and round-the-clock operation carry high fixed costs, so issuing is a business of volume and trust, not unit margin.

02

What the protocol asks of you, and what it never asks

A few hard obligations, a longer list of things you are never asked to do, and what you get in return.

THE PROTOCOL ASKS YOU TO	THE PROTOCOL NEVER ASKS YOU TO
Verify people and organisations to the grade you assign, from enumerated, authenticated checks	Put KYC evidence, personal data, a credential, a serial number or an issuance event on-chain
Keep the evidence encrypted in a private vault that you control	Share evidence with validators, verifiers, the council or other issuers
Publish a signed status root at least every 30 seconds while active	Report who was verified, who presented a credential, or where
Hold a separately scoped emergency key and use it only for its purpose	Reveal a holder's identity because a relying party asks or pays
Keep a live bond at or above the governed minimum, and keep the agent-to-human link private except under due process	Alter another issuer's credentials, inspect presentations, or hold holders' keys or agents' funds

What the protocol guarantees you.

Equal terms. Every issuer, including the one run by the project's own implementing group, passes the same admission, posts the same bond and publishes the same roots, and anyone can check this on-chain.

Sanctions need evidence. Suspension, slashing and forced key rotation need a council decision backed by evidence; the only automatic sanction is suspension when a slash exhausts your bond.

Your registry is yours alone. No one else can change your credentials' status; your emergency key acts alone.

Disclosure cannot be bought. Payment never justifies disclosing personal data, commercial release of full KYC needs live consent, a mandated identification delivers only the fields a governed obligation class names to a counterparty the principal nominated, and a dispute reveals identity only on a neutral arbiter's finding.

Bounded state. The chain sees only your registry entry and your roots, so a billion credentials cost it no more than a thousand: one root per issuer.



03

The path to admission

Five steps take an organisation from applicant to active issuer, and the bond is what lets you go live.

STEP 1 Compliance AML/KYC, grading and data policies before applying	STEP 2 Council review Application and permitted grades council vote	STEP 3 Keys Signing and emergency keys, in hardware registered	STEP 4 Bond Native tokens at or above the minimum activation gate	STEP 5 Heartbeat First root, then every 30 seconds active
---	--	---	--	--

1. Compliance programme. Put the programme described in Chapter 4 in place before you apply. Admission depends on it.

2. Council review. You apply to the compliance council, a threshold body with a recommended configuration of 5-of-9. The council votes on-chain and records a reason code and an evidence commitment for every decision; sensitive evidence stays off-chain. It decides whether to admit you and which grades you may issue, and you can never assign a grade outside that set. Until the council is seated, admissions run through token governance — on the single-node production chain, a proposal voted by the chain's single validator — and an explicit hand-over stops that interim arrangement becoming permanent.

3. Keys. You generate your keys in hardware-backed signers, and the protocol registers them against your record. You need signing keys for credentials and roots, plus a **separately scoped emergency status key** that can publish an immediate root on its own. The set must always contain an active signing key and an active emergency key. Routine rotation is self-service, signed by the account that operates your record. Only that account can lock your bond, so no one else can take your bond position or activate you. Keep sealed recovery copies: if you lose that account, recovery takes a key rotation ordered by the council.

4. Bond. From your operating account, you lock native tokens at or above the governed minimum. The chain lets you become *active* only while a live bond meets that minimum, and it rejects smaller locks. The simulation sizes the minimum against a published fiat deterrence target, so the bond exceeds the modelled gain from the cheapest slashable violation, and the minimum is reviewed yearly. The bond is locked capital, not a fee: it is released after the governed lock period if no case is open.

5. Heartbeat and go-live. Your first signed root starts the 30-second cadence, which must never stop: once your latest root is 45 seconds old, verifiers refuse your credentials. Open gradually, with a limited portfolio first.

Authority states. Your record moves only between the states *pending*, *active*, *enhanced monitoring* (operating under closer council scrutiny), *suspended* and *revoked*, which is final. The chain rejects any other transition. Every return to active passes the bond check again, and a suspended issuer also needs a council reinstatement.



The compliance workload

Most of the work is regulatory: the protocol fixes the vocabulary, but your legal obligations remain yours. This chapter lists the tasks a compliance lead needs to plan. The perimeter, registrations and retention periods depend on your jurisdiction and service model, so take specialist legal advice.

4.1 Anti-money-laundering perimeter and programme

Performing customer due diligence usually brings an issuer inside anti-money-laundering law. In the EU, that means the national transpositions today and the AML Regulation (EU) 2024/1624 from July 2027. Plan for:

- **A perimeter opinion.** Establish whether you are an obliged entity in your own right, a service provider to obliged entities, or both, and what registration with your supervisor that requires.
- **An AML/KYC programme.** This covers a business-wide risk assessment, customer acceptance, standard, simplified and enhanced due diligence, and screening for sanctions, politically exposed persons (PEP) and adverse media. It also covers ongoing monitoring and suspicious-activity reporting.
- **Governance.** A compliance officer, internal control, staff training and periodic independent audits.
- **Proofing evidence.** Your identity-proofing process, whether your own or your provider's, must map to the standards below. In Europe, conformity with ETSI TS 119 461 is the natural evidence.

4.2 Grading: strength and freshness

You decide each grade yourself, from enumerated, authenticated checks and within the grades the council has permitted you. Grades measure the *strength* of a verification. They are anchored on eIDAS and aligned with ISO/IEC 29115. The external columns below map the grades to those frameworks; they do not redefine them.

GRADE	MEANING	EIDAS	ISO/IEC 29115	NIST SP 800-63	AML POSTURE
A1	Basic identity binding and issuer verification	low	LoA2	IAL1	customer due diligence
A2	Stronger document and liveness verification	substantial	LoA3	IAL2	due diligence with biometric liveness (ETSI TS 119 461 baseline proofing)
A3	Enhanced due diligence and periodic evidence review	substantial + enhanced due diligence	LoA3+	IAL2 + EDD	sanctions, PEP and adverse-media screening; evidence reviewed at least yearly
A4	Highest assurance, stricter issuer controls and audit requirements	high	LoA4	IAL3	qualified identity proofing (ETSI extended proofing, notified eID at <i>high</i> , EUDI Wallet)

ISO's LoA1 (self-asserted identity) is below MintID's floor. The step from A2 to A3 adds enhanced due diligence (EDD) under AML rules; it is not an extra eIDAS level. If you serve organisations, your grading policy must also cover the legal entity, the person acting for it and, at enhanced levels, its beneficial owners.

Freshness is a separate dimension. Next to each grade you hold a **freshness band** for the last successful proofing: under 30 days (F4), under 90 (F3), under 180 (F2) or under 365 (F1). It is published as a band, never as a date, so it cannot become a correlator. A verifier may require both a minimum grade and a minimum freshness band. For ZadQ, the anchor product, “human-backed” means grade A2 or higher and freshness F1 or better.

Validity and re-verification. Each grade has a default validity: 12 months for A1 and A2, 6 for A3 and 3 for A4. This is the *longest* a verification may back credentials, not a timetable. Within it, re-verify on risk and events as AML rules require, and plan for renewing a whole portfolio. A renewal is a new credential with fresh secrets, publicly unlinkable to the old one, and the holder may renew with any accepted issuer. A credential expires exactly when the verification behind it does — however late in that period it was issued — with no grace period and no extension; past that instant every issuance step is refused, and the way back is a new verification. Expiry is not revocation: MintID’s first issuer treats withdrawn consent as revoking everything it backed; that policy awaits counsel’s sign-off.

4.3 Data protection

You are the controller of the KYC data, and the only party in the system that holds any. Plan for:

- **Accountability and assessment.** Appoint a data protection officer where required and keep a record of processing. Complete an impact assessment before go-live, because large-scale verification with biometric liveness is high-risk processing.
- **Consent and retention.** Get explicit consent for biometrics, kept separate from consent to the credential service. Keep records for the statutory AML period (five years after the relationship ends under EU rules, longer in some Member States). Do this through the vault: encrypted storage, sealed and audited access, and deletion when the period ends.
- **Rights, breaches and processors.** Handle data-subject rights through your own case files, since the chain holds nothing to erase or correct. Have rehearsed breach-notification procedures. Sign processor agreements with your verification, hosting and hardware-signing providers.

The design helps you: no personal data flows from your vault to the chain or to verifiers, so you protect one audited store rather than a spread of copies.

4.4 Operating policies and counsel items

The network expects written policies on the following:

- **Grading,** for each grade and each type of subject.
- **Revocation** for fraud, death, compromise or holder request. The emergency key is reserved for serious cases, and every use of it is attributable and reviewed by the council.
- **Agent controls** (Chapter 8).
- **Dispute response.** You release an agent’s human identity only on a neutral arbiter’s certified finding, never because a relying party asks or pays.
- **Mandates.** Before mandated identification is switched on, counsel settles per jurisdiction what makes a principal’s mandate valid, which obligation classes are recognised and with which fields, the longest horizon and cap, the revocation guarantee, and how the counterparty keeps what it receives.
- **Continuity and exit:** notice to holders, renewal elsewhere and an orderly wind-down.
- **Insurance** for professional liability and cyber risk.

Counsel items. The first issuer's KYC policy (provider terms, proofing per grade, consent, evidence reuse) awaits counsel, and you will need the same review for your jurisdiction. Supported jurisdictions and data retention are set before genesis. The governance of identity release on the dispute path gates the financial-recourse stage, not the identity-only launch.

05

The issuer services you operate

What any compliant issuer implementation must do, described by function rather than design.

CAPABILITY	WHAT IT DOES, AND WHY IT MATTERS
KYC integration	Acquires evidence from one or more identity-verification providers behind a provider-neutral interface, so you can switch or combine providers. The grade is always your decision
Identity vault	Holds the evidence and the link between case files and credentials, encrypted, with sealed and audited access. It is the only place personal data exists
Credential issuance	Delivers anonymous credentials to holders' software over OpenID4VCI, each bound to a secret only the holder knows. The proof core behind it is in production
Private status registry	Keeps each credential's status, encrypted, and gives holder software the private status proofs (witnesses) they need to keep proving, so it needs high availability
Root publication	Builds and signs the heartbeat root at least every 30 seconds for relaying. An optional push channel announces new roots early; it carries no security weight
Emergency updates	Publishes an immediate root under the emergency key, linked to the previous root, so a revocation need not wait for the next heartbeat
Hardware-backed signing	Keeps credential, root and emergency keys in hardware signers; nothing is signed outside them
Chain access and monitoring	Reads finalised state through authenticated proofs, so you see what verifiers see. Watches root age, bond margin, throughput and vault access; the root-age alert is the one that must wake someone up
Agent services	Minting (including bounded agents from your bundle catalogue), the accountability escrow, sybil controls and the disclosure rail — built, switched off and fail-closed until activated (Chapter 8)

Relaying. Anyone can relay status updates. Relayers batch many issuers' roots into one transaction and pay the fees, but they gain no authority: only your signature authorises your root. **Zoning.** Keep issuance and witness delivery in a public zone, and KYC integration, the registry, root building and relaying in an internal zone. Keep the vault and the signers in a sealed zone with no outbound internet access. Every signature goes through hardware. **Software.** MintID's first issuer runs on services built by the project's implementing group. Other issuers build or procure a conforming implementation against the specifications, which are available on request at info@mintid.net. Whatever you run, cryptographic checks must come from the single, audited, version-pinned proof core, never from a reimplementation.



06

Infrastructure, costs and revenue

Costs as categories, network economics as ratified bands: the final figures are not yet fixed.

Your costs fall into six categories. The pre-genesis simulation publishes an issuer break-even analysis and shows who ultimately bears the cost of status publication. Indicative figures are available on request; none of them is a protocol parameter.

COST CATEGORY	WHAT DRIVES IT
Compliance programme	Counsel, compliance officer and internal control, data protection, independent audits, training, insurance
Identity verification	Per-check provider pricing and minimums; screening at onboarding and ongoing monitoring; scales with onboardings
Infrastructure	Highly available issuer services, vault, hardware signers, chain access and monitoring, in sandbox and production environments
People	Compliance, operations and round-the-clock on-call engineering, because the heartbeat never stops
Network fees	Admission, renewal and active-registry lease; status-publication fees
Bond	Locked capital, not an expense, but exposed to slashing and to changes in the governed minimum

What the network charges. Admission, renewal and registry-lease fees and status-publication fees are governed parameters set by the simulation before genesis. How each fee is allocated is a governed parameter whose final form is under review. When the council slashes a bond, part becomes a **remediation share** held for the parties harmed in that case, and the allocation of the rest is a governed parameter under review. After a governed period, unclaimed remediation stays earmarked, and a late claim on the original case can still draw on it, so the body that decides slashes never profits from it.

What the network pays you. Your main income is the *agent mint fee and lease fee* on a governed schedule, net of the protocol cut. The simulation sets the prices before genesis: the lease prior is a competitive ceiling, and admission policy sets an anti-sybil floor for every issuer. From the financial-recourse stage you may take an optional *brokering fee* on a consented disclosure: the relying party's bid goes to the principal, minus that fee and a protocol cut (a percentage plus a per-disclosure floor, band ratified before genesis).

PARAMETER	RATIFIED BAND	PRIOR
Protocol cut on agent mint and lease fees	A governed parameter under review	—
Allocation of each protocol cut	Governed parameters	Final form under review

These are the only protocol cuts; no usage tax exists or is planned.



07

Continuous operation

Once active, the heartbeat, the bond and the vault are permanent duties with automatic consequences.

OBLIGATION	TARGET	IF IT FAILS
Status roots	At least every 30 seconds, never older than 45; roots that are expired, future-dated or valid for too long are rejected	Every verifier refuses your credentials until a fresh root is final
Emergency updates	Available at all times, within governed rate limits	The council audits patterns of use and can suspend or slash
Bond	Live, above the minimum, with margin	A slash that exhausts it suspends you at once, and all your roots are then rejected
Keys	Routine rotation; any compromise disclosed at once	Undisclosed compromise is slashable; a lost operating account needs a council-ordered rotation
Reviews	Quarterly issuer-quality and false-issuance review; annual review of grades, validity periods, bond values and remediation	Findings can lead to enhanced monitoring, suspension or slashing

Your state, council actions, slashes and root-liveness statistics appear in the public transparency report, which never contains holder data. **The council may slash** for proven fraudulent issuance, issuance outside your permitted grades, deliberate failure to keep status live, an undisclosed signing-key compromise, or other violations published in advance. Each decision carries a public reason code and an evidence commitment.

The golden rules.

- 1. The heartbeat is sacred.** Build redundancy, on-call cover and alerting around the 45-second limit.
- 2. The bond is the brake.** Keep a margin: while you are suspended, your holders can prove nothing.
- 3. Never lose or expose the vault.** Everything else can be redeployed; the identity link cannot.

Incidents. Rehearse these before go-live:

- **Key compromise.** Publish an emergency root, rotate the key and tell the council.
- **Heartbeat outage.** Holders fail closed until a fresh root supersedes the stale one. Nothing needs backfilling.
- **Vault breach.** Make the data-protection notifications, inform the council and revoke any credentials at risk.
- **False issuance.** Revoke the affected credentials through the next root, report the case and support remediation.

Leaving. Give holders notice to renew elsewhere, then wind down. Your bond is released after the governed lock period if no case is open.



08

Issuing for agents

As verified people deploy AI agents, issuers give those agents their backing and hold the only link back to the human behind them.

Minting. A principal, the human behind the agent, proves in zero knowledge that they hold an unrevoked credential at a sufficient grade, and optionally that they are within their agent cap. You then mint a fresh agent credential that cannot be linked to the principal or to their other agents. It has its own secrets, a backing assertion and a delegated scope. You record the agent-to-human link in your accountability escrow, and your next root makes the agent usable. Nothing new goes on-chain: to the chain, an agent credential is just another entry under your status root.

YOUR RESPONSIBILITY	WHAT IT INVOLVES
Backing and scope	Mint only from a valid principal credential, never above its grade. Sign a scope into the credential (what the agent may do, with whom, where, when, up to what value), bounded by your policy; the agent cannot raise it
Custody and operator	Attest how the agent's keys are held and who operates the agent. Use classes that cannot link sibling agents to each other. A managed runtime is a signal, never a trust root
Sybil controls	Enforce a KYC gate, a per-principal cap on active agents, a KYC freshness requirement, and the mint fee and lease. Do this privately, with no per-agent data on-chain
Escrow and revocation	Keep the agent-to-human link in the vault. Revoke agents through your next root or the emergency key; a principal-wide cascade must reveal neither the principal nor the fleet size

Bounded agents (ADR-0023). Instead of a scope assembled per mint, you can offer named **bundles**: a versioned, content-hashed catalogue in which each bundle fixes the actions and bounds the categories, regions, sellers, value per transaction, lease, custody and backing grade — written only in values of the current scope vocabulary, and always in the private-only disclosure class (the credential carries no class commitment, which SPEC-3 R-A19 reads as private-only). MintID specifies the catalogue's format and rules; the content is yours (or your operator's), fitted to the industries you serve. Your issuer service loads the catalogue file you supply, checks it against those rules and refuses to start on an invalid one; if you supply none, it runs the reference catalogue MintID ships as an example. Either way it reports the catalogue's identifier, content digest and whether it is the reference or your own, and every offer names the identifier and digest. The operator picks a bundle and its choices inside it; you refuse anything outside it, and you can refuse every mint that names no bundle. The operator's price for each bundle rides in the offer as a price line: the fee is the operator's, never a chain fee. Relying parties accept these agents with policy presets built from your catalogue: give them the catalogue file and its digest, and their SDK checks one against the other.

Mandated identification (ADR-0023, SPEC-3 v3.1). Some counterparties must by law record who their client is — accommodation, vehicle rental, passenger transport. A principal can give its agent a bounded **mandate** under which you deliver, without a live human on each exercise, exactly the fields that a governed **obligation class** names to a counterparty the principal nominated. The obligation classes are governed content: each names the rule, the act and the field schedule, and neither the counterparty nor the agent chooses a field. The mandate has a cap per period and an expiry no later than the credential; the first exercise towards each counterparty is confirmed live, and the principal can revoke it at any time. You read the fields from your identity provider at the moment of release and keep none of them; you deliver them signed, directly to the counterparty, never through the agent; and you receipt every exercise. The agent relays and executes; it never consents. The software for this rail is built and ships **switched off and fail-**



closed: nothing is released until counsel settles the mandate standard (section 4.4) and the rail is switched on, and the proof by which an agent shows the issuer which agent a request concerns is still to be added to the proof core.

From the financial-recourse stage, three further duties apply:

- **Escrow coverage.** An agent may prove that a minimum of USDC or EURC, locked by smart contract in the principal’s own wallet, backs it. You check the funds’ origin and attest the band; you never hold the funds.
- **Commercial rail.** As consent broker, you apply the principal’s policy to a relying party’s priced bid. The policy refuses by default or escalates to the human. You release only the item consented to, never full KYC on delegated consent, and safeguards contain the conflict that your fee creates. Mandated identification runs on this rail under the same activation gate.
- **Dispute rail.** Money comes before identity, in three levels:
 - **L0:** the escrow pays the claimant, and no identity is involved.
 - **L1:** you attest a minimal, banded fraud signal: a real verified human, a grade, a jurisdiction and a count of prior disputes. The signal contains no personal data.
 - **L2:** you release identity into the judicial process only on the arbiter’s certified finding, and the council audits the release afterwards.

Every level runs off the consensus path. The chain holds only commitments to disclosure receipts.

09

Where things stand today

MintID runs in production on a single-node chain: the issuer side is implemented, credential issuance runs on the proof core, and the first issuer runs the ZadQ pilot on that chain.

STAGE 0 Single-node production First issuer and ZadQ pilot on the production chain now → 2027	STAGE 1 Public offer MiCA Title II process; bond minimum and fee points fixed 2027	STAGE 2 Identity mainnet Admission, bonds, issuance, free verification H2 2027 → 2028	STAGE 3 Financial recourse Escrow coverage, disputes, consent brokering 2028 → 2029	STAGE 4 Maturity Many issuers, a growing agent population 2030 → 2031
---	--	---	---	---

AREA	STATUS IN SEPTEMBER 2026
On-chain issuer capabilities	Implemented (registry, bonds, status roots, council, fees) and running on the single-node production chain; the council is built, not seated: admissions run as governance proposals voted by the chain’s single validator
Issuer services	A first issuer service is implemented: encrypted status registry, 30-second root publication and relaying, hardware-signing interface, provider-neutral KYC interface with a real identity-verification provider behind it, whose evidence never enters MintID



AREA	STATUS IN SEPTEMBER 2026
Credential issuance	Implemented and in production on the proof core. Holder self-revocation has been in production on the single-node production chain since 24 September 2026: when a holder revokes one of your credentials through the relay, only you learn which one, and you remove it within the grace the chain enforces — the chain refuses your updates if you do not. It runs on the public testnet as it does in production, and is switched off at the distributed public network's genesis, where switching it on is a governance decision. Its independent audit is a scheduled milestone, as is the audit of the proof core's implementation, whose findings will be published
Agent products	Bounded agents are minted today from a bundle catalogue. The consented commercial disclosure rail, mandated identification included, is built and ships switched off and fail-closed; activation waits for counsel
First accepted issuer	Operated by the CONECTIA group, which is the project's implementing group and a disclosed related party, on undifferentiated terms
ZadQ pilot	ZadQ, an x402 seller-verification service, is the first product built on MintID. The first issuer attests its sellers with conventional signed attestations (no zero-knowledge claim) on the single-node production chain, operated by the CONECTIA group: not yet the distributed network, and excluded from the traction criterion
Governance	The MintID Foundation, a Netherlands Stichting seated in Amsterdam (competent authority: the Dutch AFM), is being incorporated by the founder and stays dormant until the public-offer route is chosen (ADR-0016); the single-node production chain is operated by the CONECTIA group as a disclosed related party. The council, not yet seated, becomes a Foundation organ before any MiCA white paper is signed

Stage windows are targets, not commitments: each stage, genesis included, opens only when its published conditions are met. The plan is anchored on 24 December 2027, when the eIDAS 2.0 wallet-acceptance obligations for relying parties take effect. Before mainnet, a public adversarial testnet must run with independent validators, issuers and verifiers, and prospective issuers can rehearse there. **Organisations considering the issuer role can engage now** through mintid.net to request the specifications and discuss grading and the regulatory perimeter.

10

Risks and limits

Being an issuer carries real exposures, and this manual states them plainly.

- **Fail-closed exposure.** If you go silent, your credentials stop working within 45 seconds. This is the cost of the freshness guarantee, and you bear it.
- **Slashing and bond value.** Slashing needs evidence, and a slash that exhausts the bond suspends you. The bond is held in the native token, whose value varies, and its minimum is reviewed yearly in fiat terms.
- **Key and vault compromise.** The vault is the system's most attractive target. Defend it with hardware signing, zoning and rehearsed incident plans.
- **Open questions.** Counsel has yet to settle the AML perimeter, consent wording, AI Act conformity of disclosure receipts and the governance of identity release. Fees, lease and bond remain bands until the simulation fixes them, and adverse scenarios show thin margins.
- **Related-party competition.** The first issuer belongs to the implementing group and competes on disclosed, equal terms that anyone can verify. The pending independent economic review is the only arm's-length opinion.
- **Cross-issuer sybil evasion.** Agent caps apply per issuer, so a person verified by several issuers could run more agents. The shared anti-sybil price floor limits this; stronger mitigations are still research items.



REFERENCES

References

MintID documents. MintID Protocol Whitepaper v1.0 and its Executive Edition (September 2026); the Verifier & SDK, Holder and Validator manuals. The frozen specification corpus is available on request.

Standards and regulation. OpenID for Verifiable Credential Issuance; Hyperledger AnonCreds; Regulation (EU) 910/2014 as amended by Regulation (EU) 2024/1183 (eIDAS 2.0); Implementing Regulation (EU) 2015/1502 (levels of assurance); ISO/IEC 29115; ETSI TS 119 461; NIST SP 800-63; Regulation (EU) 2024/1624 (AML Regulation); Regulation (EU) 2016/679 (GDPR); Regulation (EU) 2024/1689 (AI Act); Regulation (EU) 2023/1114 (MiCA), Title II; x402 (Linux Foundation).

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

