Virtual Earth Nation - Section 8: Identity, Citizenship & Reputation (v1.0-textfix)

8.1 Overview

Section 8 defines how people and organizations are known, trusted, and accountable in the Virtual Earth Nation (VEN). We balance privacy with safety: citizens control what they share, while marketplaces and governance obtain the proofs they need. Identity is the foundation for paid work (WT -> VEX -> VC), consumer protection, and fair elections (Section 3).

8.2 Principles

• Human-first: jobs are performed by verified humans; AI tools assist but do not replace proof-of-human-work.
• Minimal disclosure: prove compliance (age, residence, KYC) without revealing extra data.
• Portability: credentials work across all VEN services and compatible partners.
• Revocability & recovery: you can rotate keys, recover accounts, and revoke leaked credentials.
• Due process: moderation and sanctions include notice, evidence, appeal (per Section 3).

8.3 Identity Architecture

• Decentralized Identifiers (DIDs): each person/org has one primary DID and optional sub-DIDs per context.
• Verifiable Credentials (VCreds): signed attestations for age, name, skills, licenses, permits.
• Zero-Knowledge Proofs (ZK): ZK-KYC and age assurance let users prove eligibility without exposing raw documents.
• Device & session binding: strong authentication; optional privacy-preserving liveness checks for anti-bot.
• Custody options: self-custody wallets, social recovery, or regulated custodial agents for new users.
• Data minimization: services request proofs, not raw PII; storage is encrypted and time-limited.

8.4 Citizenship & Residency Model

• Visitor (V): read/attend; limited purchases; no work or voting.
• Resident (R): may work (WT), hold VC, and access most services; no national vote.
• Citizen (C): full civic rights; voting, proposal rights, and access to certain public benefits.
• Organization (O): businesses, co-ops, NGOs with KYB; hire workers, hold concessions (Sections 4-7).
• Status upgrades: via background checks, contribution thresholds, and community endorsements; all processes auditable.

8.5 Onboarding & Compliance

• KYC/KYB pathways: document checks, address verification, sanctions screening; ZK-compatible wherever possible.
• Age & region policies: publish allowed/blocked categories; ZK proofs avoid storing birth dates.
• Work eligibility: basic training + code-of-conduct acceptance; higher SLA tiers require micro-certs (Appendix B).
• Risk tiers: higher-risk sectors (finance, safety-critical) require stronger proofs and continuous monitoring.
• Visa & permits: time-bound, scope-bound credentials for pilots, events, and foreign orgs.

8.6 Reputation & Credentials

• Work graph: every completed task writes to a tamper-evident ledger (who, what, when, SLA, QA result).
• Reputation score: weighted by role, difficulty, dispute rate, on-time %, and verified client feedback.
• Skills & licenses: VCreds issued by accredited bodies after exams or micro-certs; expire unless renewed.
• Badges & tiers: Bronze/Silver/Gold/Platinum worker tiers unlock higher WT rates and complex jobs.
• Client reputation: buyers earn reliability scores to deter abuse; repeat abusers lose privileges.

8.7 Privacy & Data Governance

• Consent ledger: what you shared, with whom, and for how long is visible to you.
• Retention limits: default 12-24 months for operational data, longer for financial records where required.
• Redaction & erasure: submit requests; system propagates deletes where lawfully feasible.
• Differential privacy (DP): aggregates for dashboards use DP to prevent re-identification.
• Cross-border transfers: routing obeys data-residency rules; export justified by contractual and technical safeguards.

8.8 Safety, Security & Compliance

• Anti-sybil: liveness + device binding + stake; repeat fraud slashes stake and revokes credentials.
• AML/CFT: on/off-ramp monitoring; risk scoring; suspicious-activity workflows; ZK-KYC proofs accepted where partners agree.
• Moderation: layered approach (AI triage + human review) with evidence chain and appeal in Section 3.
• Incident response: key rotation, session kills, and credential revocation; publish post-incident reports.
• Sanctions & penalties: transparent schedules; progressive restoration tied to training and restitution.

8.9 Interoperability (Sections 2-7)

• Section 2: WT/WT-E -> VEX -> VC payouts require verified identity; escrow and dispute flows link to DIDs.
• Section 3: voting/representation bound to Citizen status; ZK ballots preserve secrecy with public tallies.
• Section 4: access control for sites/depots; contractor badges and safety permits.
• Section 5: service-provider licenses and consumer protections rely on credentials and reputation.
• Section 6: eco-worker WT-E roles require environmental training credentials.
• Section 7: operator permits for eVTOL/maglev/Hyperloop; AI-ATC controllers hold elevated clearances.

8.10 KPIs & Public Dashboards

• Onboarded users by status (V/R/C/O) and completion time.
• % of transactions covered by ZK proofs vs. raw KYC.
• Credential renewal rate; expired-credential work attempts prevented.
• Dispute rate by worker tier; appeal outcomes and time to resolution.
• Account recovery success rate; fraud recidivism after sanctions.
• Privacy metrics: average data retention; # of erasure requests honored.

8.11 Risks & Safeguards

• Deanonymization risk: mitigate with ZK, DP, and compartmentalized DIDs.
• Exclusion risk: provide assisted onboarding and low-tech credentials; multilingual support.
• Credential forgery: cryptographic verification; issuer accreditation; revocation registries.
• Capture or bias: independent oversight on accreditation and sanctions; appeals process.
• Data breach: end-to-end encryption, key rotation, anomaly detection, tabletop exercises.

8.12 Roadmap

• Q1: Ship DID/VCred wallet with social recovery; launch ZK-KYC pilot.
• Q2: Roll out worker tiers and skills micro-certs; enable org KYB and contractor badges.
• Q3: Integrate ZK ballots with Section 3; publish privacy dashboards.
• Q4: Cross-border portability with partner ecosystems; annual security & fairness audit.