BLUE BOOK · OPERATING MANUAL

The Blue Book of GNX Identity-to-Execution Logic Engine

설명서 · 매뉴얼 · 참고서

입력·신원·표시상태·세션증거·실행권한을 하나의 검증 가능한 증거 체인으로 묶어, 조건 없는 실행을 fail-closed 방식으로 차단하는 실행통제 엔진

문서명	The Blue Book of GNX Identity-to-Execution Logic Engine
문서상태	Enterprise Review Draft · License Table Edition
버전	v1.0 · GNX Identity-to-Execution Edition
기준일	2026-05-02
작성주체	주식회사 지엔엑스_GNX Co., Ltd. · CEO Kim Chul
적용표면	logicnoid.co.kr · www.logicnoid.co.kr · api/admin/verify/docs.logicnoid.co.kr · AWS EC2 · CloudFront · AWS WAF
문서 통제	본 문서는 계약 전 검토 및 엔터프라이즈 보안 심사 목적의 공식 설명 자료이며, 운영 secret, admin private key, DB 원본 dump, 장기 토큰을 포함하지 않습니다.

목차

1. 운영 개념과 시스템 표면

1.1 시스템의 표면

GNX Identity-to-Execution Logic Engine 은 여러 표면으로 운영된다. logicnoid.co.kr 루트 도메인은 EC2 A 레코드 기반 직접 랜딩 표면으로 유지한다. www.logicnoid.co.kr 은 CloudFront 및 AWS WAF 경유 대표 공개 검증 표면이다. api.logicnoid.co.kr 은 WNS, Bident, Display, Execution, Audit API 표면이며, admin.logicnoid.co.kr 은 signed admin challenge 기반 관리자 표면이다. verify 와 docs 표면은 evidence verification 및 문서 제출 패키지를 위한 확장 표면이다.

1.2 엔진 구성요소

실제 엔진은 AWS EC2 내부에서 Node.js, PostgreSQL, Redis, Nginx, Certbot, systemd, CloudFront, AWS WAF 로 운영된다. gnx-i2e systemd 서비스가 127.0.0.1:3300 에서 엔진을 실행하고, Nginx 가 origin 과 local routing 을 담당한다. CloudFront 와 AWS WAF 는 www, api, admin, verify, docs 표면을 보호한다.

1.3 운영자가 기억할 원칙

- 실패는 오류가 아니라 LOCKED_BY_DESIGN 정책일 수 있다.
- 공개 표면은 원문 저장소가 아니다.
- raw admin token, raw tunnelTicket, public vault, gnxceo fallback 은 금지 구조다.
- 실행권한은 one-time opaque executionHandle 로만 발급된다.
- 문서, 테스트, 백업, WAF, DNS 상태를 게이트 기준으로 관리한다.

요약문 운영 관점에서 엔진은 사이트 하나가 아니라 도메인 표면, API, systemd 프로세스, DB, Redis, WAF, 문서 패키지가 결합된 검증 생태계다. 운영자는 각 표면의 역할과 경계를 구분해야 한다.

2. 7 단계 엔진 흐름 매뉴얼

2.1 WNS Commit

입력 문자열은 실행 대상이 아니라 실행 전단 증거로 처리된다. WNS commit 은 입력을 정규화하고 fingerprint 와 receipt 를 생성한다. 운영자는 status:WNS_COMMIT_ACCEPTED, gateState:COMMITTED, plaintextRetained:false, rawTokenReturned:false 를 확인한다.

2.2 ZKV Anchor 와 Bident Session Proof

ZKV Anchor 는 원문 자격증명을 저장하지 않고 anchor 와 salt 기반 검증 구조를 제공한다. Bident Resonance 는 신원 검증과 세션 증거를 결합한다. 인증 성공은 실행권한이 아니라 실행 전 증거인 session proof 다.

2.3 Display Interlock 과 Execution Authorization

Display 또는 policy condition 이 충족되지 않으면 execution authorize 는 실패한다. WNS receipt, Bident session, target identity, nonce, audience, display 또는 condition proof 가 결합될 때 one-time executionHandle 이 발급된다.

2.4 Execution Consume 과 Replay 차단

발급된 executionHandle 은 짧은 TTL 과 audience binding 을 가진다. consume 후 used_at 처리 및 Redis key 삭제로 재사용을 차단한다. 동일 handle 또는 nonce 재사용은 LOCKED_BY_DESIGN 또는 replay rejected 상태로 처리된다.

2.5 Audit Hash Chain

핵심 이벤트는 receipt, evidence_hash, prev_hash, event_hash 로 audit chain 에 기록된다. 운영자는 /v1/audit/:receipt 와 Evidence Verification CLI 로 receipt 구조와 chain-file 연속성을 확인한다.

요약문 7 단계 흐름의 핵심은 입력을 곧바로 실행하지 않는 것이다. 입력은 증거가 되고, 신원과 세션은 proof 가 되며, 표시상태와 정책조건이 결합된 뒤에만 1 회성 실행권한이 발급된다.

3. API 와 검증 표면 사용 설명

3.1 Health 와 Product 확인

운영자는 먼저 /health/ready 에서 ok:true, product, state:READY, db:READY, redis:READY, publicVaultEnabled:false, rawAdminTokenReturned:false, rawTunnelTicketReturned:false 를 확인한다. /v1/public/product 는 제품 정의, 비주장 경계, 모듈 목록을 반환한다.

3.2 WNS Evidence 생성

POST /v1/evidence/wns-commit 은 입력 문자열을 WNS evidence 로 변환한다. 응답에는 receipt, fingerprint, gateState:COMMITTED, plaintextRetained:false, rawTokenReturned:false 가 있어야 한다.

3.3 Execution API

프로덕션 실행 경로는 /api/v1/execution/authorize 와 /api/v1/execution/consume 으로 분리된다. 구 /api/v1/policy/evaluate 는 410 으로 격하되어 demo/production 경로 혼합을 방지한다.

3.4 Verification CLI

Evidence Verification CLI 는 receipt 검증과 audit chain JSONL 연속성 검증을 수행한다. 고객사 보안팀은 서버 secret 없이도 receipt 구조, event_hash 포맷, prev_hash 연속성을 확인할 수 있다.

요약문 API 사용의 기본은 health, product, WNS commit, execution authorize/consume, audit verification 순서다. 공개 demo 와 production authorize 는 분리되어야 하고, 모든 상태는 JSON 증거로 재현되어야 한다.

4. 관리자·보안·WAF 운영

4.1 Signed Admin Challenge

신규 엔진은 raw admin token 을 반환하지 않는다. 관리자는 /v1/admin/challenge 로 challenge 를 받고 private key 로 서명한 뒤 /v1/admin/session/verify 를 통해 ADMIN_SESSION_BOUND 상태를 얻는다. 응답은 rawAdminTokenReturned:false 여야 한다.

4.2 CloudFront 와 AWS WAF

www, api, admin, verify, docs 표면은 CloudFront 및 AWS WAF 경유로 운영된다. WAF 는 public vault path 를 403 으로 차단하고, old policy endpoint 관찰, execution API rate limit, auth/register API rate limit, admin path count, AWS managed rule group 을 포함한다.

4.3 Domain Architecture Policy

logicnoid.co.kr 루트 도메인은 현재 EC2 A 레코드 기반 직접 랜딩 표면으로 유지한다. 루트 도메인의 CloudFront 일원화는 Route 53 Alias 또는 Gabia ALIAS/ANAME 지원 여부에 따라 후속 전환한다. origin.logicnoid.co.kr 은 CloudFront 원본 전용이다.

요약문 관리자 운영은 token 회수가 아니라 signed challenge 구조로 관리한다. WAF 는 engine 내부 차단 전에 edge 에서 위험 path 를 차단하며, 도메인 구조는 apex 와 enterprise 검증 표면을 명확히 분리한다.

5. 장애 대응과 일일 점검

5.1 일일 점검

매일 postgresql, redis-server, gnx-i2e, nginx 상태를 확인한다. 127.0.0.1:3300 LISTEN 상태, public health/ready, WAF 차단 403, production-readiness-gate PASS/PENDING 라인을 확인한다.

5.2 장애 좁히기

502 또는 API 무응답은 Nginx, gnx-i2e, Redis, PostgreSQL 순서로 좁힌다. 엔진은 systemd status 와 journalctl 로 확인하고, DB 는 psql, Redis 는 redis-cli ping 으로 확인한다. 명령어와 JSON 결과를 터미널에 다시 붙여넣어 실행하지 않도록 구분한다.

5.3 백업과 복구 원칙

운영 백업은 DB dump 와 파일 archive, systemd, Nginx 설정을 포함한다. admin_private_key.pem 이 포함될 수 있으므로 /opt/gnx/backups 는 root-only 700 으로 잠그고 SHA256SUMS 를 생성한다. 실제 백업 파일 없이 pg_restore 를 실행하지 않는다.

요약문 운영 안정성은 복잡한 기능보다 상태 확인 루틴, 로그 판독, 백업 잠금, WAF 확인, security acceptance 재실행 능력에 달려 있다.

6. 검증 절차와 인수시험 참고서

6.1 표준 검증 절차

표준 검증은 health/ready, WNS commit, CSRF, ZKV register, Bident resonance, display lock, execution authorize, execution consume, replay fail, audit receipt verification 순서로 수행한다. 허용 경로와 차단 경로를 모두 확인해야 한다.

6.2 보안 수용 기준

Security Acceptance Test 는 CSRF_REQUIRED, BIDENT_SESSION_REQUIRED, WNS_COMMIT_REQUIRED, DISPLAY_INTERLOCK_NOT_CONFIRMED, NONCE_REPLAY_REJECTED, EXECUTION_HANDLE_NOT_FOUND_OR_USED, PUBLIC_VAULT_REMOVED, POLICY_EVALUATE_MOVED 를 검증한다.

6.3 고객사 설명 기준

고객이 IAM 대체 여부를 묻는다면 “대체재가 아니라 execution evidence gate”라고 설명한다. 통신사는 display/session interlock 과 fraud signal adapter, 금융권은 suspicious transaction gate 와 case evidence receipt, AI/API 고객은 agent action preflight 와 API Gateway Evidence Gate 로 설명한다.

요약문 Blue Book 의 최종 목적은 운영자와 검증자가 같은 방식으로 제품을 설명하고 재현하게 만드는 것이다. 검증은 화면이 아니라 API 응답, receipt, 차단 상태, WAF 403, audit chain 으로 닫혀야 한다.

부록 A. 핵심 운영 파일

- /opt/gnx/identity2execution/engine/src/server.ts - 메인 엔진
- /opt/gnx/identity2execution/.env.production - 운영 환경/비밀값
- /etc/systemd/system/gnx-i2e.service - systemd 심장박동
- /etc/nginx/sites-available/gnx-i2e - Nginx 기본 혈관
- /etc/nginx/conf.d/gnx-i2e-origin.conf - CloudFront origin 전용 설정
- /opt/gnx/identity2execution/docs - 엔터프라이즈 제출 문서
- /opt/gnx/identity2execution/engine/tools/evidence-verifier.ts - Evidence Verification CLI