The Blue Book of GNX Courage Text™

공식 설명서·운영 매뉴얼·기술 참고서 / Enterprise Operations Manual

문서 유형	Blue Book
대상 독자	운영자, 구축 담당자, 기술지원, 보안 운영, 현장 파트너
버전	v1.1 Enterprise Draft
작성 기준	원본 White Book v1.0, CTP 운영 검증 산출물, EC2 배포 기준
보안 등급	Confidential - Licensing / Enterprise Review
발행일	2026-05-07

목차

1. 사용 설명 범위와 독자

1.1 문서 목적

The Blue Book of GNX Courage Text™는 제품 운영자, 구축 담당자, 현장 파트너, 기술지원 담당자, 보안 운영자가 실제 시스템을 이해하고 운영할 수 있도록 작성된 공식 설명서·매뉴얼·참고서다. 백서가 라이선싱 판단과 검증 계약을 위한 문서라면, 청서는 사용 흐름, 운영 절차, 장애 대응, API 참조, 보안 운영을 설명하는 실무 문서다.

1.2 독자별 사용 방식

리더는 전체 원리와 운영 책임을 확인한다. 개발자는 API 와 상태 전이를 확인한다. 보안 담당자는 동의, 암호화, 로그 마스킹, 관리자 접근 통제를 확인한다. 현장 운영자는 요청자 안내, 수신자 안내, 부적합 사용처 차단 기준을 확인한다. SMS 사업자 담당자는 inbound webhook, outbound queue, route secret TTL, 실제 provider credential 투입 조건을 확인한다.

요약문 - 사용 설명 범위와 독자 장은 현장 운영자가 시스템을 안전하게 실행하고 검증할 수 있도록 구체 절차, endpoint, 상태, 장애 대응 기준을 제시한다.

2. 역할과 기본 객체

2.1 주요 역할

요청자는 웹앱 또는 PWA 에서 첫 문장 intent 를 생성하는 사용자다. 수신자는 별도 앱을 설치하지 않고 기본 문자앱으로 공용 번호에 진입하는 사용자다. 시스템 운영자는 intent, license, audit, outbound queue, burn 상태를 관리한다. SMS provider 는 공용 문자번호 수신과 발송 인프라를 제공한다. 계약 관리자는 라이선스 한도와 사용 조건을 관리한다.

2.2 기본 객체

Text Intent Capsule 은 messageCipher, requester token, WNS token, expiresAt, state 를 포함한다. SMS Claim 은 수신자의 inbound 번호와 본문을 토큰화한 진입 기록이다. Consent Proof 는 수신자가 확인 또는 거절을 명시했다는 감사 증적이다. Outbound Message 는 실제 SMS provider 가 붙기 전에는 queued_not_sent 또는 failed_no_route 로 남을 수 있다. Route Secret 은 원본 번호를 평문 저장하지 않고 제한 시간 암호문으로 보관하는 임시 라우팅 입력이다.

요약문 - 역할과 기본 객체 장은 현장 운영자가 시스템을 안전하게 실행하고 검증할 수 있도록 구체 절차, endpoint, 상태, 장애 대응 기준을 제시한다.

3. 요청자 웹앱 운영 방식

3.1 요청자 화면

요청자는 https://hokssi.com/app 에 접속한다. 라이선스 키, requester id, WNS 묘사, 첫 문장, TTL, 선택적 위치·방향 정보를 입력한다. 현재 위치 입력 버튼은 브라우저 geolocation 권한이 허용될 때 좌표를 채운다. 제출이 성공하면 intent id 와 view token 이 생성되며, PWA 는 상태 endpoint 를 주기적으로 조회한다.

3.2 작성 기준

첫 문장은 짧고 비압박적이어야 한다. 연락처 요구, 상업적 권유, 위협, 성적 표현, 미성년자 대상 표현, 반복 접근 문구는 정책상 부적합하다. WNS 는 상대 묘사를 너무 구체적인 개인정보로 만들지 말고 현장에서 수신자가 스스로 확인 가능한 범위의 중립적 단서로 작성한다.

3.3 상태 조회

상태 조회는 /v1/intents/:id/status?view_token=... 형식으로 수행된다. view token 은 요청자에게 한 번만 제공되는 임시 조회 권한이다. 운영 로그에는 query string 이 남지 않도록 설정되어야 한다. token 이 없거나 틀리면 intent_not_found_or_token_invalid 가 반환된다.

`요청자 기본 절차: /app 접속 -> License Key 입력 -> requester id 입력 -> WNS 작성 -> 첫 문장 작성 -> TTL 선택 -> 현재 위치 입력 선택 -> Intent 생성 -> status polling 확인.`

요약문 - 요청자 웹앱 운영 방식 장은 현장 운영자가 시스템을 안전하게 실행하고 검증할 수 있도록 구체 절차, endpoint, 상태, 장애 대응 기준을 제시한다.

4. 수신자 SMS Claim 및 동의 방식

4.1 수신자 진입

수신자는 GNX 앱을 설치하지 않는다. 공용 문자번호로 “GNX”, “응답”, 또는 서비스가 정한 claim 신호를 보낸다. 시스템은 열린 intent 후보를 찾고, 후보가 하나로 수렴하면 확인 문자를 queue 에 넣는다. 후보가 복수이면 WNS challenge 를 통해 추가 확인을 요구할 수 있다.

4.2 동의와 거절

수신자가 1 을 보내면 Consent Proof 가 생성되고 Relay Session 이 열린다. 수신자가 2 또는 STOP 에 준하는 거절을 보내면 해당 세션은 REJECTED 또는 BURNED 로 전이된다. 동의가 없으면 첫 문장은 전달되지 않는다. 수신자의 침묵은 동의가 아니라 만료 및 소각으로 처리한다.

4.3 SMS provider 상태

실제 provider credential 이 없으면 시스템은 SMS_PROVIDER=unconfigured 상태로 유지한다. 이 경우 outbound queue 는 안전 정지되며 sent 로 표시되지 않는다. 실제 사업자 API URL, 인증 방식, 등록 발신번호가 확보된 뒤에만 provider adapter 를 활성화한다.

요약문 - 수신자 SMS Claim 및 동의 방식 장은 현장 운영자가 시스템을 안전하게 실행하고 검증할 수 있도록 구체 절차, endpoint, 상태, 장애 대응 기준을 제시한다.

5. 관리자 운영 절차

5.1 라이선스 발급

관리자는 /v1/admin/license/accounts endpoint 로 라이선스 계정을 생성한다. legal_name, product_code, plan_code, max_monthly_intents, max_active_sessions, expires_at 을 지정할 수 있다. 응답의 license_key_once 는 한 번만 표시되므로 즉시 안전한 비밀 저장소에 보관한다.

5.2 사용량 확인

관리자는 /v1/admin/licenses 로 라이선스별 월간 intent 수와 active session 수를 확인한다. max_active_sessions 를 초과하면 새 intent 는 license_active_session_quota_exceeded 로 차단된다. 라이선스가 없으면 license_key_required 또는 invalid_or_inactive_license 가 반환된다.

5.3 백업과 복구

운영자는 /usr/local/bin/hokssi-db-backup.sh 로 PostgreSQL custom dump 를 생성한다. 비파괴 복구 리허설은 hokssi_restore_check 같은 임시 DB 에 pg_restore 를 수행한 뒤 table count 와 주요 테이블 존재 여부를 확인하고 삭제한다. 운영 DB 에 직접 복구할 때는 CONFIRM_RESTORE=yes 를 요구하는 보호 스크립트를 사용한다.

요약문 - 관리자 운영 절차 장은 현장 운영자가 시스템을 안전하게 실행하고 검증할 수 있도록 구체 절차, endpoint, 상태, 장애 대응 기준을 제시한다.

6. API·상태·데이터 참조

6.1 주요 API

GET /health 는 시스템 생존성 확인이다. POST /v1/intents 는 intent 생성이다. GET /v1/intents/:id/status 는 view token 이 있는 요청자 상태 조회다. POST /v1/sms/inbound 는 SMS 사업자 inbound webhook 이다. POST /v1/consent 는 동의 처리 webhook 이다. /v1/admin/*는 관리자 키와 IP allowlist 가 필요하다. /v1/system/*는 EC2/localhost 만 허용한다.

6.2 상태 참조

OPEN 은 요청자가 intent 를 생성한 상태다. CLAIMED_BY_SMS 는 수신자 SMS Claim 이 들어온 상태다. AMBIGUOUS 는 후보가 복수이거나 점수가 낮은 상태다. CONSENT_PENDING 은 확인 문자가 준비된 상태다. RELAY_OPEN 은 수신자 동의가 완료된 상태다. BURN_PENDING 은 만료 또는 종료 직전 상태다. BURNED 는 본문·매핑·임시 토큰 삭제가 끝난 종료 상태다.

6.3 데이터 참조

license_accounts 와 license_keys 는 계약·사용량 집행을 담당한다. text_intents 는 intent 와 상태를 저장한다. sms_claims 는 inbound claim 을 기록한다. consent_proofs 는 동의 증적을 저장한다. outbound_messages 는 발송 queue 다. sms_route_secrets 는 TTL 라우팅 secret 이다. burn_records 와 audit_events 는 소각·감사 증적이다.

Endpoint	권한	운영 의미
GET /health	Public	API, DB, Redis 생존성 확인
GET /app	Public	요청자 PWA 화면
POST /v1/intents	License required	Text Intent Capsule 생성
GET /v1/intents/:id/status	View token required	요청자 상태 조회
POST /v1/sms/inbound	Webhook secret	SMS Claim 수신
GET /v1/admin/licenses	IP allowlist + admin key	라이선스 사용량 확인
상태	**의미**	**다음 조치**
OPEN	요청자가 intent 생성	Claim 대기 또는 만료
CONSENT_PENDING	확인 문자 준비	1 또는 2 대기
RELAY_OPEN	수신자 동의 완료	제한 시간 후 burn
REJECTED	거절	burn
BURNED	삭제 완료	종료

요약문 - API·상태·데이터 참조 장은 현장 운영자가 시스템을 안전하게 실행하고 검증할 수 있도록 구체 절차, endpoint, 상태, 장애 대응 기준을 제시한다.

7. 보안 운영과 장애 대응

7.1 보안 운영

운영자는 ADMIN_API_KEY 와 WEBHOOK_SECRET 을 주기적으로 rotation 한다. rotation 후 새 키가 200/202 를 반환하고 이전 키가 401 을 반환하는지 확인한다. Nginx 는 admin/system endpoint 를 IP allowlist 로 제한한다. Docker 로그와 Nginx 로그에는 view token, 원문 번호, 문자 본문이 남지 않도록 유지한다.

7.2 장애 대응

API 가 재기동될 때 일시적 502 가 발생할 수 있으나, /health 가 정상으로 돌아오면 복구된 것이다. worker 가 중단되면 만료 intent 가 BURNED 로 전이되지 않으므로 docker compose ps 와 worker 로그를 확인한다. PostgreSQL 이 unhealthy 이면 새 intent 를 받지 말고 backup 상태를 확인한다. SMS provider 오류는 sent 로 표시하지 않고 failed 또는 queued_not_sent 로 남긴다.

7.3 운영 명령

기본 점검 명령은 docker compose ps, curl -s https://hokssi.com/health | jq ., /usr/local/bin/hokssi-db-backup.sh, docker logs --tail=80 hokssi-api, docker logs --tail=80 hokssi-worker 이다. Nginx 설정은 sudo nginx -t 와 sudo nginx -T 로 검증한다. 인증서 갱신은 certbot renew --dry-run 으로 확인한다.

```
운영 점검 명령: cd /opt/hokssi && docker compose ps && curl -s https://hokssi.com/health | jq . && /usr/local/bin/hokssi-db-backup.sh
```

요약문 - 보안 운영과 장애 대응 장은 현장 운영자가 시스템을 안전하게 실행하고 검증할 수 있도록 구체 절차, endpoint, 상태, 장애 대응 기준을 제시한다.

8. 부록: 운영 체크리스트와 용어

8.1 운영 체크리스트

배포 후 확인할 항목은 HTTPS, /app 200, /health ok, DB healthy, Redis PONG, worker Up, admin allowlist, no-query log format, license quota enforcement, burn worker, backup 파일 생성, restore rehearsal, secret rotation, SMS provider safety mode 다. 이 중 하나라도 실패하면 상용 파일럿 전 상태로 되돌려야 한다.

8.2 용어

Intent 는 요청자가 연 첫 문장 의사다. Claim 은 수신자가 공용 문자번호로 진입한 사건이다. Consent 는 수신자가 명시적으로 1 또는 동등 신호를 보낸 상태다. Relay 는 번호 비공개 중계다. Burn 은 제한 시간 또는 거절 후 삭제다. License 는 사용량과 active session 을 집행하는 계약 단위다. View Token 은 요청자가 자기 intent 상태를 조회하는 임시 권한이다.

요약문 - 부록: 운영 체크리스트와 용어 장은 현장 운영자가 시스템을 안전하게 실행하고 검증할 수 있도록 구체 절차, endpoint, 상태, 장애 대응 기준을 제시한다.