The White Book of GNX Courage Text™

검증·라이선스 계약용 설명서 / Enterprise Licensing and Verification Paper

문서 유형	White Book
대상 독자	경영진, 보안전문가, 법무·구매·파트너 검증 담당자
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. 문서 목적과 검증 범위

1.1 문서 목적

The White Book of GNX Courage Text™는 리더, 보안전문가, 법무·구매·파트너 검증 담당자가 제품을 라이선싱 또는 파일럿 계약의 대상으로 판단할 수 있도록 작성된 검증·계약용 설명서다. 본 문서는 제품을 홍보 문구로 과장하지 않고, 실제 기술적 경계와 운영 책임을 명확히 구분한다. GNX Courage Text™의 목적은 전화번호 획득이 아니라, 번호를 공개하지 않은 상태에서 제한 시간 동안 허용된 첫 문장만 열어주는 것이다. 따라서 검증의 핵심은 “얼마나 많은 메시지를 전달하는가”가 아니라 “동의 없는 전달을 얼마나 확실히 차단하는가”에 있다.

1.2 검증 범위

검증 범위는 CTP - Courage Text Protocol, WNS 의미 토큰, Text Intent Capsule, SMS Claim, Consent Proof, Relay Session, Burn Record, 라이선스 테이블, 상태 기계, 운영 로그 통제, 백업·복구, 관리자 접근 통제, SMS 사업자 연동 전 안전 정지 정책까지 포함한다. 본 문서가 다루지 않는 범위는 실제 통신사 또는 SMS 사업자의 과금 정책, 각 국가별 통신 법령의 최종 법률 의견, 물리적 현장 운영 매뉴얼의 세부 행사 시나리오다. 해당 항목은 파일럿 계약 부속서 또는 DPA, SLA, 현장 운영 약정으로 분리한다.

1.3 엔터프라이즈 판정 원칙

엔터프라이즈 판정은 기능 시연이 아니라 통제 가능성에 의해 이루어진다. 요청자 생성, 수신자 자발 진입, 명시 동의, 제한 시간, 번호 비공개, 소각, 감사 증적, 장애 시 fail-closed 가 모두 결합되어야 한다. 어느 한 단계라도 우회 가능하면 라이선싱 대상이 아니라 실험 코드에 불과하다.

요약문 - 문서 목적과 검증 범위 장은 GNX Courage Text™를 기능 제품이 아니라 동의·보안·소각·라이선스 집행이 결합된 통제형 프로토콜로 판정하기 위한 기준을 정리한다.

2. 제품 및 프로토콜 정의

2.1 제품 정의

GNX Courage Text™는 요청자만 웹앱을 사용하고 수신자는 기본 문자앱만 사용하여, 양측 전화번호를 서로 공개하지 않은 채 첫 문장 수준의 문자 의사를 중계하는 일회성 통신 제품이다. 요청자는 상대방의 번호를 얻지 않으며, 수신자도 요청자의 번호를 알지 못한다. 서버는 번호를 관계 식별자가 아니라 임시 라우팅 입력으로만 취급한다. 노출 대상은 사용자에게 허용된 문자 본문과 상태뿐이다.

2.2 CTP 정의

CTP 는 Text Intent Capsule 을 생성하고, 공용 문자 관문으로 들어온 SMS Claim 을 열린 캡슐과 매칭한 뒤, 수신자의 명시 동의가 성립할 때만 Relay Session 을 여는 조건부 실행 제어 프로토콜이다. CTP 는 채팅 서비스가 아니라 상태 결합 실행 엔진이다. WNS 문자열 정규화, 내부 의미 토큰 생성, 시간·방향·상태 판단, 동의 검증, 중계 허용, 소각이 순차적으로 강제된다.

2.3 핵심 객체

Text Intent Capsule 은 요청자의 첫 문장, WNS 토큰, 시간·위치·방향 조건, 만료 시각을 포함한 임시 객체다. SMS Claim 은 수신자가 공용 번호로 보낸 자발적 진입 신호다. Consent Proof 는 수신자가 1 또는 동등한 확인 신호를 보냈다는 최소 감사 증적이다. Burn Record 는 본문·매핑·라우팅 토큰을 삭제했다는 운영 증거다.

객체	계약·검증상 의미	수명/통제
Text Intent Capsule	요청자가 열어둔 첫 문자 의사	60-180 초 TTL, 만료 후 burn
WNS Token	상대 묘사의 내부 실행 판단 토큰	외부 표시 금지, 세션 단위
SMS Claim	수신자의 자발적 문자 진입	검증 후 상태 전이
Consent Proof	명시 동의 감사 증적	최소 보존 또는 hash 보존
Burn Record	소각 완료 증적	정책 기반 보존

요약문 - 제품 및 프로토콜 정의 장은 GNX Courage Text™를 기능 제품이 아니라 동의·보안·소각·라이선스 집행이 결합된 통제형 프로토콜로 판정하기 위한 기준을 정리한다.

3. 보안·개인정보·동의 통제

3.1 동의 구조

CTP 의 동의는 세 단계다. 첫째, 요청자가 자기 의사를 생성한다. 둘째, 수신자가 앱 설치나 계정 생성 없이 공용 문자 관문으로 자발적으로 들어온다. 셋째, 수신자가 확인 메시지에 1 로 응답한다. 이 중 하나라도 없으면 중계는 열리지 않는다. “무단 전달”이 아니라 “자발적 응답”이 프로토콜의 중심 원리다.

3.2 개인정보 최소화

번호 비공개는 사용자 인터페이스 약속만으로 성립하지 않는다. 서버 내부에서도 원본 번호를 장기 고객 데이터베이스로 만들지 않고, HMAC 토큰 또는 TTL 암호화 라우팅 secret 으로만 다룬다. 운영자 화면에는 원본 번호가 표시되지 않아야 하며, 로그에는 문자 본문과 view token 을 남기지 않는다. 라우팅이 종료되면 복호 가능한 입력은 소각된다.

3.3 보안 통제

보안 기준은 TLS, 저장 시 암호화, rate limit, audit hash, 최소 권한 관리자, 관리자 IP allowlist, secret rotation, 백업·복구 검증, Docker log rotation, fail-closed 운영을 포함한다. SMS 사업자 credential 이 없거나 설정이 placeholder 인 경우 발송 성공으로 위장하지 않고 queued_not_sent 또는 안전 정지 상태로 남겨야 한다.

요약문 - 보안·개인정보·동의 통제 장은 GNX Courage Text™를 기능 제품이 아니라 동의·보안·소각·라이선스 집행이 결합된 통제형 프로토콜로 판정하기 위한 기준을 정리한다.

4. 엔터프라이즈 검증 기준

4.1 검증 기준

라이선싱 검증은 API 가 존재하는지만 보지 않는다. 생성, 상태 전이, 권한, quota, 소각, 로그 마스킹, backup restore, secret rotation 이 모두 작동해야 한다. 예컨대 license table 은 단순 기록이 아니라 max_monthly_intents 와 max_active_sessions 를 실제 실행 제어에 반영해야 한다. 무라이선스 intent 는 차단되어야 하며, 한도를 초과한 active session 은 429 로 거절되어야 한다.

4.2 수락 테스트

수락 테스트는 OPEN 생성, CLAIMED 또는 CONSENT_PENDING 전이, RELAY_OPEN, REJECTED, EXPIRED, BURNED 전이, 불법 전이 차단, 만료 worker 소각, admin key rotation, webhook secret rotation, query-token log masking, DB backup custom dump 생성, 비파괴 restore rehearsal 을 포함한다. 테스트 결과가 “성공처럼 보임”이 아니라 데이터베이스 상태와 로그에서 확인되어야 한다.

4.3 제한 조건

현재 SMS 실제 발송은 사업자 credential 과 등록 발신번호가 확보될 때까지 안전 정지 상태로 두는 것이 맞다. 이는 미완성이 아니라 안전한 경계 설정이다. 통신망 규칙을 우회하거나, 테스트 문자열로 실제 발송 성공을 흉내 내는 것은 검증 문서상 불합격 조건이다.

검증 항목	합격 기준	불합격 기준
라이선스	무라이선스 402, quota 초과 429	키 없이 생성 허용
소각	TTL 후 BURNED	만료 OPEN 잔존
로그	query token/본문 미기록	secret 또는 본문 노출
SMS	미설정 시 queued_not_sent	가짜 sent 표시

요약문 - 엔터프라이즈 검증 기준 장은 GNX Courage Text™를 기능 제품이 아니라 동의·보안·소각·라이선스 집행이 결합된 통제형 프로토콜로 판정하기 위한 기준을 정리한다.

5. 라이선스 계약 구조

5.1 라이선스 대상

라이선스 대상은 CTP 엔진, WNS 정규화·토큰화 로직, Text Intent Capsule 생성 흐름, consent proof 처리, burn manager, PWA 요청자 화면, 관리자 검증 endpoint, 운영 runbook 및 배포 패키지다. 라이선스 계약은 소스 코드 사용권, 배포권, 파트너 현장 운영권, API 이용권, 상표 사용권을 분리하여 설계해야 한다.

5.2 계약 제한

라이선시 또는 파트너는 전화번호 수집 서비스, 스팸 발송, 성인·미성년자 취약 환경 접근, 권력 불균형 환경에서의 반복 접근, 통신망 우회, 로그 원문 수집, 원본 번호 DB 화, 동의 없는 relay 강제 개방을 금지해야 한다. 위반 시 키 정지, 세션 폐기, 감사 로그 보존, 계약 해지 및 손해배상 조항이 필요하다.

5.3 SLA 와 책임 경계

SLA 는 API 가용성, SMS provider 의존성, 세션 TTL 정확도, burn worker 정상 동작, 백업 보존, 장애 대응 시간을 구분해야 한다. SMS 사업자의 장애, 통신사 정책, 수신 단말의 문자 수신 실패는 플랫폼 고유 책임과 분리된다. 단, 시스템은 실패를 성공으로 표시해서는 안 된다.

요약문 - 라이선스 계약 구조 장은 GNX Courage Text™를 기능 제품이 아니라 동의·보안·소각·라이선스 집행이 결합된 통제형 프로토콜로 판정하기 위한 기준을 정리한다.

6. 운영 준비도와 감사 체계

6.1 운영 아키텍처

운영 기준 구성은 Nginx/HTTPS, API container, PostgreSQL, Redis, worker, backup script, log rotation, admin IP allowlist, secret rotation script 로 구성한다. PWA 는 /app 에서 제공하고, public API 는 license 또는 view token 으로 제한한다. admin/system endpoint 는 Nginx 레벨 allowlist 와 application key 를 함께 요구한다.

6.2 감사와 증적

감사는 본문을 보존하는 방식이 아니다. 상태 전이, 라이선스 생성, intent 생성, consent proof, burn record, outbound queue 상태, backup 수행 결과, rotation 결과를 hash 또는 최소 메타데이터로 기록한다. 감사 증적은 계약 분쟁, 보안 심사, 장애 사후 분석에 사용되며, 사용자 사생활을 침해하는 원문 보관으로 대체되어서는 안 된다.

6.3 장애 대응

장애 시 원칙은 fail-closed 다. API 가 비정상일 때 새 relay 를 열지 않고, 만료된 intent 는 worker 또는 수동 system endpoint 로 burn 한다. SMS provider 가 비정상이면 queued_not_sent 로 남기고 sent 로 표시하지 않는다. 로그가 secret 을 노출한 경우 즉시 log truncate, private archive, secret rotation 을 수행한다.

운영 기준 예시: HTTPS, Dockerized API/PostgreSQL/Redis/Worker, 관리자 IP allowlist, query-token 로그 제거, DB custom dump 및 비파괴 restore rehearsal, secret rotation rehearsal, SMS provider 미설정 안전 정지.

요약문 - 운영 준비도와 감사 체계 장은 GNX Courage Text™를 기능 제품이 아니라 동의·보안·소각·라이선스 집행이 결합된 통제형 프로토콜로 판정하기 위한 기준을 정리한다.

7. 상용화 로드맵과 최종 판정

7.1 상용화 단계

상용화는 Closed MVP, WNS 매칭 고도화, Production Pilot, Commercial Release 순서로 진행한다. Closed MVP 는 핵심 상태기계와 동의형 문자 중계를 증명한다. Pilot 은 공식 문자 회선, 신고·수신거부, 개인정보 영향 검토, 장애 대응 훈련을 포함한다. Commercial Release 는 운영 콘솔, 리스크 대시보드, 파트너 도입 패키지, 현장 교육을 포함한다.

7.2 최종 판정

GNX Courage Text™의 라이선싱 가능성은 “전화번호 이전의 첫 문장”이라는 제품 정의가 기술 구조와 운영 구조에서 일관되게 강제되는지에 달려 있다. 요청자와 수신자 모두에게 작은 용기를 허용하되, 거절과 침묵도 동일하게 존중되어야 한다. 제품이 커질수록 전달 능력보다 차단 능력이 더 중요하다.

요약문 - 상용화 로드맵과 최종 판정 장은 GNX Courage Text™를 기능 제품이 아니라 동의·보안·소각·라이선스 집행이 결합된 통제형 프로토콜로 판정하기 위한 기준을 정리한다.

8. 부록: 용어 및 수락 기준

8.1 용어

GNX Courage Text™는 번호 공개 없이 첫 문장만 여는 문자 기반 제품명이다. CTP 는 문자 의사 캡슐의 생성·매칭·동의·소각 프로토콜이다. WNS Token 은 상대 묘사를 주소가 아니라 내부 실행 판단 토큰으로 변환한 값이다. Burn 은 본문·토큰·라우팅 매핑·UI 상태를 제한 시간 후 삭제하는 절차다.

8.2 계약 수락 기준

계약 수락 기준은 첫째 무라이선스 intent 차단, 둘째 quota enforcement, 셋째 상태기계 불법 전이 차단, 넷째 view token 외 상태 조회 차단, 다섯째 query-token 로그 제거, 여섯째 backup/restore rehearsal, 일곱째 secret rotation rehearsal, 여덟째 SMS provider 미설정 시 안전 정지다.

요약문 - 부록: 용어 및 수락 기준 장은 GNX Courage Text™를 기능 제품이 아니라 동의·보안·소각·라이선스 집행이 결합된 통제형 프로토콜로 판정하기 위한 기준을 정리한다.