GNX Co., Ltd.

LOGICNOID AIPhone™

The White Book of GNX Logicnoid AIPhone™

검증·라이선스 계약용 설명서

리더/보안전문가/라이선스 실사용 백서

문서 등급	Confidential - Licensing / Verification Draft v1.0
작성 기준일	2026-04-29
작성 근거	제공 소스코드, 특허 출원/명세 자료, 법인 및 통신사업 증빙 문서
용도	라이선스 협상, 기술 검증, 보안 실사, 운영 참조
공백 제외 본문 글자 수	5,252자 이상
비고	운영 비밀값, 개인식별번호, 원문 자격증명은 본 문서에서 재기재하지 않음

커버서

본 문서는 GNX Logicnoid AIPhone™ 및 연계 도메인 logicnoid.com, 안전.한국의 라이선싱 및 기술 검증을 위해 작성된 공식 정리본이다. 제공된 실행 소스와 출원 명세서, 출원 사실 증명, 우선심사 결정, 법인/사업자/통신 관련 증빙을 기준으로 기술적 주장과 현행 구현을 분리하여 정리하였다. 문서의 목적은 투자자, 리더, 보안전문가, 기술실사 담당자가 동일한 기준으로 시스템의 원리, 권리화 근거, 보안 통제, 운영 구조, 보완 조건을 검토할 수 있도록 하는 데 있다. 법률 의견서 또는 외부 보안인증서가 아니며, 정식 계약 전에는 별도 법률 검토, 침투시험, 개인정보 영향평가, 클라우드 구성 검토가 병행되어야 한다.

목차

근거 자료 색인

자료	실사상 의미
AIPhone 출원사실증명원	특허-2026-0014512, 출원일 2026.01.25, 명칭: 전화번호 비노출 기반 텍스트 식별자 통신 아이덴티티 보안 통신 시스템
AIPhone 명세서	실제 전화번호 비노출, 텍스트 식별자, 디스플레이 레디, 상호 의존적 세션, 마켓플레이스 엔진 등 권리 구성
KIPO WNS 명세서	문자열 입력 정규화, 내부 전용 의미 해석 토큰, 상태 결합 판단, 강제 경유 실행 제어 구조
WNS 우선심사결정서	출원번호 10-2026-0010237, 우선심사대상 인정 통지
법인/사업자/통신 증빙	GNX Co., Ltd. 법인성, 사업자등록, 통신판매업 신고, 부가통신사업 신고 확인 자료
theLogoofLogicnoidcom.txt	EC2 배치 메인 로직 엔진으로 제공된 Python 기반 서비스 코드와 프런트엔드/신호 처리 로직

제1장 라이선스 검증 개요

1.1 문서 목적과 제출 범위

GNX Logicnoid AIPhone™의 백서는 기술을 과장 없이 검증 가능한 단위로 분해하여 제시하는 라이선싱용 문서이다. 본 시스템의 중심 가치는 실제 전화번호를 공개하지 않고 텍스트 기반 식별자를 통신 주소와 표시 아이덴티티로 사용하는 점, 그리고 문자열을 단순 주소가 아니라 실행 제어 입력으로 해석하는 점에 있다. 제공된 소스는 Python 기반 단일 서비스 엔진으로 확인되며, WNSLogic 클래스, 암호화된 vault 파일, gWN 등록/로그인, ZET 원장, 안전.한국 수신망, PrivateCall 및 S2S 신호 연계, WebRTC성 신호 송수신, 관리자 엔드포인트를 포함한다. 라이선스 테이블에서 본 문서는 기술 설명, 권리화 근거, 보안 통제, 계약 범위를 하나의 공통 언어로 묶는 기준문서 역할을 한다.

1.2 검증 가능한 주장

검증 가능한 주장은 다섯 가지로 압축된다. 첫째, AIPhone 명세는 원본 전화번호를 통신 경로와 UI에서 직접 노출하지 않는 구조를 목표로 한다. 둘째, 텍스트 기반 식별자는 단순 닉네임이 아니라 통신 대상 지정, 표시, 권한, 희소성 등급, 거래 가능성을 결합한 통신 아이덴티티로 설계되어 있다. 셋째, WNS 명세는 문자열 입력을 정규화하고 내부 전용 의미 해석 토큰을 생성한 뒤 시스템 상태와 결합하여 실행을 허용 또는 차단하는 독립 실행 제어 레이어를 제시한다. 넷째, 현행 EC2 소스는 해당 개념의 서비스형 구현을 수행하되, 일부 보안 통제는 상용 보안 수준으로 보완되어야 한다. 다섯째, 법인 및 신고 자료는 사업 주체의 존재와 부가통신/통신판매 관련 기본 신고 사실을 뒷받침한다.

1.3 상용화 전제 조건

본 백서는 완성 인증서가 아니라 라이선스 검증본이다. 따라서 정식 계약 전에는 비밀값 회전, KMS 기반 암호화 전환, 관리자 권한 분리, 감사 로그 무결성, 개인정보 처리흐름 정리, 침투시험, 클라우드 인프라 다이어그램, 서비스수준협약이 완결되어야 한다. 현행 소스에는 비밀값이 코드 또는 환경 기본값에 존재하는 정황이 있으므로 문서에는 실제 값을 재기재하지 않았고, 계약 전 즉시 폐기 및 회전을 전제한다.

> 요약문: 제1장은 백서의 기능을 라이선스 제출용 검증 프레임으로 정의한다. 핵심은 AIPhone의 전화번호 비노출 통신 아이덴티티, WNS의 문자열 기반 실행 제어, EC2 코드의 구현 상태, 그리고 계약 전 보안 보완 조건을 분리해 판단하는 것이다.

제2장 권리화 및 법인성 근거

2.1 AIPhone 권리 포지션

AIPhone 출원 자료는 실제 전화번호 또는 이메일 등 원본 식별자를 일방향 암호화 토큰으로 변환하고, 사용자가 선점한 텍스트 식별자와 매핑하여 통신 주소 및 표시 식별자로 사용하는 보안 통신 시스템을 설명한다. 중요한 차별점은 수신 단말의 기본 수신 화면 또는 최상위 표시 레이어에서 텍스트 식별자를 표시하고, 디스플레이 레디 신호가 확인된 조건에서만 통신 세션을 형성한다는 상호 의존적 트랜잭션 구조이다. 이 포지션은 통화 경험, 개인정보 보호, 피싱 억제, 아이덴티티 자산화의 네 축으로 설명된다.

2.2 WNS 실행 제어 포지션

WNS 명세는 문자열 식별자를 네트워크 주소 또는 도메인 이름 해석 결과와 분리하여 처리한다. 입력 문자열은 대소문자 정규화, 유니코드 정규화, 구분자 표준화, 순서 고정 등을 거쳐 내부 전용 의미 해석 토큰으로 변환되고, 해당 토큰과 현재 시스템 상태가 결합되어 실행 가능 여부가 판단된다. 정규화 또는 토큰 생성 또는 행위 조건 판단 중 어느 하나가 생략되면 실행 제어부가 동작하지 않는다는 강제 경유 구조가 권리의 핵심이다. 이는 도메인/네임레지스트리와 충돌하지 않는 별도의 실행 통제 레이어로 주장될 수 있다.

2.3 사업 주체와 신고 체계

제공된 법인등기, 사업자등록, 통신판매업신고, 부가통신사업신고 관련 증빙은 GNX Co., Ltd.가 소프트웨어 개발, 전자상거래, 정보통신, 데이터 관리 서비스와 연관된 사업 주체임을 보여준다. 라이선스 실사에서는 원본 증빙의 진위 확인, 대표권, 인감, 사업 범위, 신고 범위, 개인정보 처리방침, 약관, 결제대행 또는 계좌입금 처리 방식이 계약 조건과 일치하는지 확인해야 한다. 증빙은 권리 및 사업 주체의 출발점이지, 보안 인증 또는 서비스 적법성 전체를 대체하지 않는다.

요약문: 제2장은 권리화 근거를 AIPhone과 WNS라는 두 축으로 정리한다. AIPhone은 전화번호 비노출 통신 세션과 표시 제어, WNS는 문자열 의미 해석 토큰과 실행 강제 경유 구조에 초점을 둔다. 법인/사업 증빙은 계약 상대방의 기본 적격성 근거로 사용한다.

제3장 기술 구조와 차별성

3.1 전화번호 비노출 통신 아이덴티티

AIPhone의 기술 메시지는 원본 번호가 통신 관계의 중심이 되지 않도록 하는 것이다. 사용자는 gWN 또는 텍스트 식별자를 통해 호출되고, 수신자는 전화번호 대신 검증된 식별자를 확인한다. 이 구조는 실제 구현에서는 WebRTC 신호, 이메일 알림, 안전.한국 공개 수신망, PrivateCall, S2S 연동으로 분기된다. 발신자의 offer가 일정 시간 수락되지 않으면 이메일 경보가 발송되고, PrivateCall은 globalgnx.com과의 S2S 경로를 통해 독립 신호 전달을 시도한다. 라이선스 문서에서는 이 구조를 개인정보 최소화형 통신 레이어로 설명할 수 있다.

3.2 문자열 의미 해석 실행 제어

WNSLogic 구현은 normalize와 tokenize 함수를 통해 문자열을 정규화하고 해시 기반 토큰을 산출한다. 등록과 로그인에서는 gWN 상태, owner, category, MCSS, CSS, SCSS, ZET 잔액, birth date가 결합되어 내부 접근 여부가 결정된다. 이는 WNS 명세의 전체 범위를 완전 구현한 형태라기보다, 문자열 식별자와 세션 토큰을 서비스 행위의 관문으로 사용하는 초기 구현으로 보아야 한다. 향후 라이선스 버전에서는 정규화 규칙, 토큰 수명, 상태 조건, 실행 정책을 별도 정책 엔진으로 분리하여 검증 가능성을 높이는 것이 바람직하다.

3.3 현행 EC2 구현과 서비스 모듈

소스 기준 서비스는 127.0.0.1:8000에서 구동되는 ThreadingSimpleServer와 NobleHandler로 구성되어 있고, 외부 도메인 연결은 리버스 프록시 또는 별도 네트워크 계층을 전제로 해석된다. 데이터 저장은 gnx_registry, safe_registry, bank ledger, zet bank, applied registry, privatecall registry 등 vault 파일군으로 분리되어 있다. 주요 엔드포인트는 /ignite, /register, /api/signal/send, /api/signal/receive, /api/zet/charge, /api/zet/transfer, /safe/register, /safe/login, /api/bank_webhook, /api/s2s/inbound, /admin/users 등이다. 구현은 빠른 증명과 데모에는 유리하지만, 엔터프라이즈 라이선스에는 데이터베이스, 큐, 캐시, 키관리, 감사 로그, API 게이트웨이가 필요하다.

요약문: 제3장은 기술 차별성을 구현 관점에서 설명한다. AIPhone은 전화번호 노출을 줄이고 텍스트 식별자 중심 통신을 형성하며, WNSLogic은 문자열/세션 토큰을 관문으로 사용한다. 현행 코드는 개념 증명과 초기 서비스 엔진 성격이 강하므로 상용화 버전의 보안 아키텍처 분리가 필요하다.

제4장 보안 실사 기준과 통제 체계

4.1 식별자/세션/토큰 통제

현행 소스는 MCSS, CSS, SCSS 개념을 통해 마스터 식별, 회전형 표시 코드, 세션 검증 코드를 구분한다. /api/zet/transfer 및 /api/signal/send는 발신자와 SCSS를 비교하여 일부 행위를 제한한다. 다만 예외 사용자, 숫자형 발신자, 전역 캔버스 처리, 관리자 라우트 등은 정교한 권한 모델로 재정의되어야 한다. 계약 전 보안 기준은 모든 민감 엔드포인트에 대해 인증, 권한, 세션 만료, 재전송 방지, IP/디바이스 바인딩, 감사 이벤트 기록을 요구해야 한다.

4.2 데이터 보호와 로그

vault 저장은 문자열을 XOR 계열 방식으로 변환한 뒤 파일에 보관하는 구조로 보인다. 이는 평문 저장보다 나은 초기 보호 장치이나, 엔터프라이즈 보안 문서에서는 강한 암호화로 주장하기 어렵다. 라이선스 전환 시 AES-GCM 또는 ChaCha20-Poly1305, KMS/HSM 키관리, 키버전, 백업 암호화, 로그 내 개인정보 마스킹, 보존기간 정책, 삭제권 처리, 관리자 열람 승인 절차가 필요하다. MEMORY_LOGS와 server.log는 장애 분석에 유용하지만 조작 방지형 감사 로그로 보강되어야 한다.

4.3 라이선스 전 필수 보완

필수 보완은 네 그룹이다. 첫째, 비밀값 관리: 소스와 기본값에서 비밀을 제거하고 환경변수, Secret Manager, 회전 정책으로 이전한다. 둘째, 인증/권한: 관리자 API를 RBAC, MFA, mTLS, HMAC 서명으로 감싼다. 셋째, 인프라: EC2 단일 프로세스와 파일 락 기반 저장을 컨테이너, 관리형 데이터베이스, Redis, WAF, CloudWatch, 백업 정책으로 전환한다. 넷째, 규정 준수: 개인정보 처리방침, 약관, 통신 신고 범위, 결제/환불 절차, 데이터 국외 이전 여부, 침투시험 보고서를 계약 부속서로 만든다.

> 요약문: 제4장은 보안 실사를 위해 현재 기능과 상용 보완을 분리한다. 핵심 요구는 비밀값 회전, 강한 암호화, 관리자 권한 분리, 감사 로그 무결성, API 인증 강화, 인프라 고도화, 개인정보 문서화다.

제5장 라이선스 모델과 계약 검증 항목

5.1 라이선스 대상 자산

라이선스 대상은 상표/명칭, 출원 기술, 서비스 소스, 도메인 연결 구조, 운영 노하우, UI/UX 문구, 식별자 정책, ZET 및 gWN 운영 모델, 안전.한국 공개 수신망, PrivateCall 연동 구조로 나눌 수 있다. 계약서에는 AIPhone 명세의 권리 범위, WNS 명세의 실행 제어 개념, 실제 배포 가능한 코드 범위, 도메인/서버 이전 여부, 데이터 이전 여부, 유지보수 범위, 독점/비독점, 지역, 기간, 하위라이선스 가능성, 개선 발명의 귀속을 명확히 적어야 한다.

5.2 제공 범위와 제외 범위

제공 범위에는 문서화된 API, 배포 패키지, 운영 매뉴얼, 테스트 계정, 보안 보완 로드맵, 원본 증빙 사본, 교육 세션, 초기 이전 지원을 포함할 수 있다. 제외 범위에는 원문 비밀값, 개인 식별 정보, 미검증 결제 자동화, 외부 도메인 또는 제3자 계정의 소유권 이전, 특허 등록 확정 전 권리 보장, 운영체제 네이티브 콜 화면에 대한 제조사 권한 보장을 명시해야 한다. 특히 OS 레벨 오버레이/CallKit/Telecom Framework 권리 주장은 특허 명세상 범위와 실제 앱스토어 정책 또는 제조사 권한 사이의 차이를 분리해야 한다.

5.3 검증 체크리스트

라이선스 실사 체크리스트는 다음을 포함한다. 원본 특허 서류 및 출원 상태 확인, 법인 대표권 확인, 서버 접근권한 확인, 도메인 소유 및 DNS 확인, 소스 무결성 해시 산출, 비밀값 제거 확인, 의존성 목록 작성, API 권한 테스트, 개인정보 흐름도 작성, 침투시험, 데이터 삭제/백업 복구 시험, 장애 전환 시험, 이용약관 검토, 결제 및 환불 절차 검증, 신고 범위 검토, 운영 인수인계 리허설. 이 항목들은 계약 선결조건 또는 마일스톤 지급 조건으로 배치하는 것이 안전하다.

> 요약문: 제5장은 라이선스 대상을 권리, 코드, 도메인, 운영 노하우, 데이터, 유지보수로 분해한다. 계약은 제공 범위와 제외 범위를 명확히 해야 하며, 보안/법무/운영 검증을 지급 및 이전 조건으로 연결해야 한다.

제6장 결론 및 실행 로드맵

6.1 계약 테이블용 핵심 메시지

GNX Logicnoid AIPhone™은 전화번호를 중심으로 형성된 통신 식별 체계를 텍스트 기반 검증 아이덴티티로 전환하려는 기술이다. WNS는 그 식별자를 실행 제어 입력으로 확장한다. 따라서 라이선스 메시지는 전화번호 비노출, 검증 표시, 실행 강제 경유, 식별자 자산화, 안전.한국과의 공공 안전형 수신망 확장이라는 다섯 문장으로 압축된다. 다만 보안전문가 앞에서는 현재 코드가 곧바로 대규모 상용 운영 인증을 의미하지 않는다는 점을 먼저 밝히고, 보완 로드맵을 제시하는 방식이 신뢰도를 높인다.

6.2 30/60/90일 추진안

30일 이내에는 비밀값 회전, 환경변수/Secret Manager 이전, 관리자 라우트 잠금, 소스 해시 고정, API 목록 정리, 법무 검토용 증빙 패키지를 완성한다. 60일 이내에는 데이터 저장소를 관리형 데이터베이스로 이전하고, Redis 기반 시그널링 큐, WAF, TLS, HMAC 서명, 감사 로그, CI/CD, 테스트 스위트를 구축한다. 90일 이내에는 침투시험, 개인정보 영향평가, 운영 매뉴얼 교육, 장애 복구 리허설, 라이선스 버전 태깅, 고객 환경 배포 절차를 완료한다.

6.3 최종 권고

본 기술은 라이선스 협상에 제출할 충분한 스토리와 권리화 자료를 갖추고 있다. 강점은 아이덴티티를 통신 표시와 실행 제어에 동시에 연결하는 구조적 독창성이다. 약점은 현행 구현이 단일 파일/단일 프로세스/파일 vault/내장 비밀값에 의존하는 초기 서비스 구조라는 점이다. 따라서 계약 문구는 “기술권리와 구현자산의 라이선스”로 설계하고, 상용 보안 수준은 보완 마일스톤 달성 후 확정하는 조건부 구조가 바람직하다.

> 요약문: 제6장은 최종 제출 전략을 제시한다. GNX는 기술 독창성, 권리화 진행, 사업 주체 증빙을 전면에 내세우되, 엔터프라이즈 보안 보완을 계약 마일스톤으로 제시해야 신뢰와 협상력을 동시에 확보할 수 있다.

부속 표준표

라이선스 실사 보완 매트릭스

영역	검증/보완 항목	계약상 배치
비밀값	코드/기본값 내 비밀 제거 및 즉시 회전	계약 전 필수
암호화	파일 변환 방식에서 KMS 연동 AEAD 암호화로 이전	상용 전 필수
관리자	RBAC, MFA, IP 제한, 이중 승인, 감사 로그	계약 부속서
S2S	공유키 비교에서 HMAC/mTLS/nonce 검증으로 강화	상용 전 필수
데이터	개인정보 흐름도, 보존기간, 삭제권, 백업 암호화	법무 검토
운영	침투시험, 장애복구 시험, SLA, 릴리스 태깅	마일스톤

요약문: 부속 표준표는 라이선스 협상에서 선결조건, 상용화 전 필수조건, 법무 검토조건, 마일스톤 조건을 구분하기 위한 표준 기준이다.

최종 고지

본 문서는 제공 자료를 기준으로 작성된 공식급 정리본이며, 외부 법률 의견서, 특허 등록 확정서, 보안 인증서, 개인정보 영향평가 결과서를 대체하지 않는다. 외부 제공 시에는 NDA, 원본 증빙 대조, 비밀값 제거 확인, 개인정보 마스킹을 선행해야 한다.