

VERITRA

Trust, Verified.

K O R E A D I D · S S I F U L L S T A C K

발급·검증·지갑·관리, 한 스택으로 끝내는 한국형 DID.

K-DID 레거시와 국제 표준(eIDAS 2.0 · ISO 18013-5 · OpenID4VC)을 잇는
Self-hosted Trust Triangle Stack — 데이터 주권을 그대로 유지하면서.

v1.0 · BSL 1.1 · www.hypercerts.com

K-DID는 작동한다. 그러나 국제 사회와 단절돼 있다.



표준 비호환

한국 모바일 신분증·금융인증서는 SD-JWT-VC / mdoc / OID4VCI 등 EU 의무 포맷 미지원. 2025-08 Biometric Update가 'non-compliant' 공식 지적.



Cross-border 단절

한국 발급 학위·의료면허·mDL이 EU·미국에서 인정 불가. EU 자회사·유학생·해외 진출 기업이 매번 별도 인증 절차를 반복.

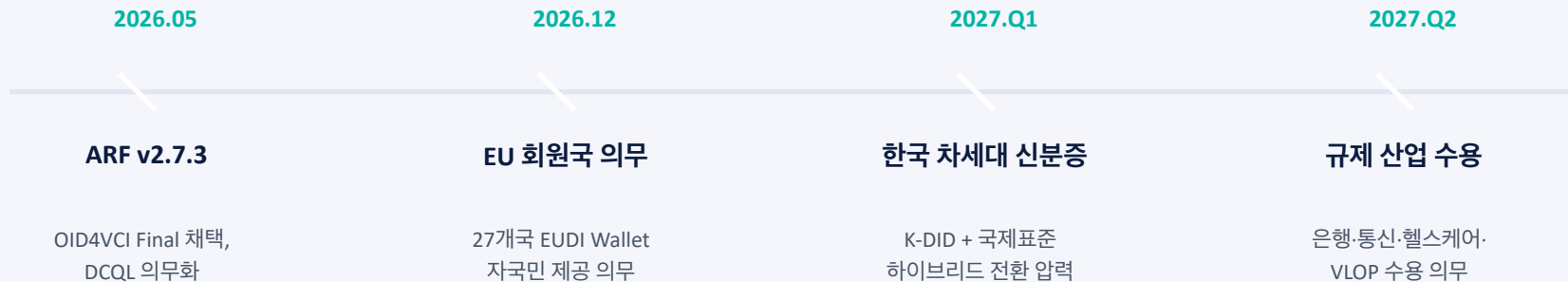


SaaS 종속 리스크

MS Entra · 글로벌 SaaS 종속 시 데이터 주권 상실. 금융·공공 규제 환경에서 외부 클라우드 의존은 컴플라이언스 부담.

결과: 한국에서 발급한 신원증명이 국제 사회에서 '없는 것'으로 취급된다. DID 서비스 업체에게는 **표준 호환 발급·검증 백본이 곧 시장 진입 자격이다.**

27개 회원국 + 3대 한국 트랙이 동시에 움직인다.



지금 표준을 채택하지 않은 한국 DID 사업자는 **2027년에는 EU·일본·ASEAN 시장 자격을 잃습니다.**

발급자 · 검증자 · 홀더 — 세 꼭짓점 모두 단일 소유권.

ISSUER 발급자	VERIFIER 검증자	WALLET 홀더 (참조 구현)
Java 17 / Spring Boot 3.4 - OID4VCI Final + FAPI2 보안 프로파일 - mdoc 양 흐름 (Pre-auth + Auth code) - HSM/KMS 3종 (AWS/Vault/Azure) - 자동 키 회전 + JWKS grace - 감사 해시체인 (전자금융 §15) ★ OIDF Conformance green	NestJS 10 / pnpm / Redis - OID4VP draft-28+ · DCQL native 9단계 검증 파이프라인 - Bitstring + Token + mdoc MSO - JARM 암호화 + 키 회전 - Webhook DLQ + Admin CRUD ★ OIDF Conformance green	React Native 0.85 · i18n 6lang - OID4VCI Pre-auth + TX code - DCQL credential_sets selector - JAR + JWE response + x5c - mDL/EU PID age-over-N UX - i18n 6개국어 (ko · en · de · fr · es · it) ★ OIDF Conformance green

다른 곳은 한두 층만 — 우리는 5층 전부.

L5	 트러스트 프레임워크	OpenID Federation 1.0 · entity config · trust chain resolver
L4	 프로토콜	OID4VCI 1.0 Final · OID4VP draft-28+ · DCQL · JARM · HAIP 1-2-3
L3	 폐기	W3C Bitstring SL + IETF Token SL + mdoc MSO status_list (3중)
L2	 신임장	SD-JWT-VC + mdoc(ISO 18013-5) + W3C VC JOSE(vc+jwt)
L1	 식별자	W3C DID Core 1.0 · did:ethr:besu (EVM 네이티브) · did:key

단일 저장소 군에서 5계층 전체 제공 — EU 레퍼런스·Procivis 외에는 비교 불가.

한국 DID 사업자 관점에서 본 표준·운영·주권 매트릭스.

평가 축	Veritra	K-DID (레거시)	Hopae (SaaS)	MS Entra VID	walt.id / Sphereon
SD-JWT-VC 발급/검증	●	○	●	○	●
mdoc (ISO 18013-5)	●	●	●	○	●
DCQL credential_sets	●	○	●	○	●
3중 폐기 (BSL+TSL+MSO)	●	○	●	○	●
OpenID Federation 1.0	●	○	●	●	●
Self-hosted (주권)	●	●	○	○	●
EVM 네이티브 폐기 (on-chain)	●	●	○	○	○
감사 해시체인 §15	●	●	●	●	○
★ OIDF Conformance green	●	○	○	○	○

● 완전 지원 ● 부분 지원 ○ 미지원

출처: 본 프로젝트 v1.0 + 2026-Q2 공개자료 종합

draft 추적이 아니라, 시험 결과로 말합니다.

OPENID FOUNDATION



OIDF Conformance

SD-JWT-VC + mdoc
(negative 테스트 포함)

✓ 2026-09-03 실행

발급자 62 · 검증자 10 · 지갑 12 모듈을
전부 실행. negative(거부) 테스트 포함,
실패 0건.

임팩트 ★ 스위트 5.1.44 · 84개 모듈 · 실패 0

OPENID FOUNDATION



HAIP 1.0

High Assurance
Interoperability Profile

✓ 2026-09-03 실행

EUDI Wallet 상호운용 프로파일.
attestation client auth, transaction_data,
VCT integrity, x5c chain 풀 적합성.

임팩트 EU 회원국 PID 발급/검증 진입 자격

OPENID FOUNDATION



FAPI 2.0

Security Profile
FINAL

✓ 2026-09-03 실행

PAR · PKCE(S256) · DPoP 홀더 결속 ·
redirect_uri allowlist · 인가코드 1회성.
Issuer 플랜에서 전 항목 통과.

임팩트 금융권 수준 인가 보안 요건 충족

실행 주체 OpenID Foundation 이 배포하는 컨포먼스 스위트를 **저희가 직접 실행한 결과**입니다. OIDF 공식 인증(certification)과는 구분됩니다.

출시 시점부터 동봉된 프로덕션 운영 풀셋.



HSM/KMS 3종

AWS KMS · HashiCorp Vault · Azure Key Vault.
env 한 줄 변경으로 전환.



자동 키 회전 + JWKS

ETSI TS 119 471 §6.4.3 grace period.
무중단 회전, active+retired 동시 노출.



감사 해시체인

append-only JSON Lines + SHA-256.
전자금융감독규정 §15 / GDPR 호환.



mTLS · Rate · Idempotency

PKCS12 + TLSv1.3 only.
Bucket4j 이중 버킷, Redis SETNX 24h.



Prom · OTel · Grafana

tail-sampling으로 에러->500ms·신용 흐름
100% 보존. 알림 룰 동봉.



FAPI2 Security Profile

PAR · PKCE(S256) · DPoP(jkt) · JAR.
attest_jwt_client_auth, 금융권 수준 보안.

온프레임 · 사설망 · Besu 자가운영. SaaS Lock-in 없이 금융·공공 보안 검수 통과.

지금 매출이 발생하는 5개 트랙.

공공



공공 모바일 신분증

K-DID → 국제표준 가교
발급자.
EBSI 정렬 + mdoc 인증 + Self-
hosted.

금융



금융 KYC 재사용

1회 KYC 6~12 USD → VC
재사용 시
수십 센트. HSM + \$15 감사 호
환.

교육



대학 학위·수료증

글로벌 검증 가능 학위
발급.
6개국어 학생 지갑 +
Federation trust chain.

헬스 / 자격



헬스·자격 증명

진단서·예방접종·면허.
장기 검증, mdoc MSO +
Bitstring on-chain.

모빌리티



mDL 모바일 운전면허

ISO 18013-5 풀스택.
age-over-N (술·담배·운전) UX,
BLE 로드맵.

6주 시스템 인계 → 6개월cross-border 능력 확보까지.

1

+6주

계약 직후

시스템 인계

- 환경 셋업 (Helm 차트)
- 기존 시스템 API 연동
- 운영 인계 워크숍
- ODF green 호환성 시연

마일스톤 발급/검증 end-to-end 정상 작동

2

+3개월

보안·규모 확장

엔터프라이즈 운영

- HSM/KMS 연동 (3종)
- 자동 키 회전 운영화
- mTLS · rate · idempotency
- OpenID Federation 트러스트 체인

마일스톤 월 100만 건 처리 환경 + 보안
감사 자료

3

+6개월

선택 · Cross-border

Cross-border 능력 확보

*외부 기관 일정에 따라 변동가능

- EBSI 호환 정합성 확보
- mdoc 외부 검사기관 인증 지원
- Wallet 생체인증 · App Attest
- did:web · did:jwk 추가

마일스톤 EU 발급 호환 + EUDI Ref Wallet 시연

한국 DID, 이제 국제 시장으로.

Veritra와 함께

K-DID 레거시를 지키면서 eIDAS 2.0 · ISO 18013-5 시장에 진입하세요.

01 PoC 신청

4~6주 무료 평가
발급·검증 1건 end-to-end

02 기술 워크숍

Trust Triangle 아키텍처
반일 온사이트 세션

03 라이선스 협의

도입 상담 · NDA 후 상세
5년 TCO 맞춤 산출