White paper técnico

Abraxas DLT Municipal · núcleo criptográfico y libro de diez lotes

Arquitectura, seguridad, auditoría interna, Contraloría técnica, ISO/TC 307

Municipalidad modelo de Las Encinas · Región de Valparaíso · Abraxas Intellect

---

Arquitectura, sello híbrido, fe pública de dos oficios, diez máquinas de estado, Groth16, RWA soulbound e interop 23516. Lo que el nodo hace y lo que todavía no.

· Sello: ML-DSA-65 (FIPS 204) AND ECDSA P-256 (FIPS 186-5). Una rama no promulga.

· Fe pública art. 63: clave del Alcalde clave del Secretario sobre el mismo payload. Revocada al dejar el cargo.

· Libro: diez lotes de Ley 18.695 como máquinas de estado. SHA-256 encadena. PoA 19 nodos.

· RWA DOM soulbound. CGR lee, no escribe. Groth16 prueba bits, no el decreto.

Clasificación: confidencial. Autoría: Alexis Fernando Franco Sánchez, Abraxas Intellect. El modelo no es el despliegue en las 345 comunas.

ÍNDICE

Capítulos

01 Identificación del producto
02 Tesis de diseño
03 Arquitectura
04 Criptografía
05 Fe pública de dos oficios
06 Diez lotes como máquinas de estado
07 Identidad, Groth16 y RWA
08 Perímetro, interop y amenazas
09 Paquete normativo

Identificación del producto

Abraxas DLT Municipal es una vertical pública permissioned sobre Ley N° 18.695. Comuna modelo: Las Encinas, Valparaíso. Autoría: Abraxas Intellect / Alexis Fernando Franco Sánchez. Hereda de Basalto el sello, el DID, el oráculo normativo y el interop 23516. No hereda el mercado.

Ficha técnica

Campo	Valor
Producto	Abraxas DLT Municipal
Spec	abraxas_municipal v100
Nodos PoA	19 (Las Encinas)
Hash del libro	SHA-256 FIPS 180-4
Sello de bloque	ML-DSA-65 ECDSA P-256
Fe pública	Dos oficios, mismo payload canónico
KEM de canal (perímetro)	ML-KEM-768 FIPS 203
ZK	Groth16 · IdViva · 269 R1CS · BN254
RWA	Permiso de edificación soulbound
Perímetro	Abraxas Security Suite v4.7.2
Interop	ISO/TS 23516 · digest SHA-256 · sin puente opaco
Clasificación	Confidencial · Abraxas Intellect

ALCANCE HONESTO

Este documento describe el núcleo y el modelo de Las Encinas. No es el despliegue en las 345 comunas de Chile. Groth16 vive en el escritorio; el libro Rust recibe el booleano ya verificado. Las claves de demostración no están en HSM.

Tesis de diseño

Una municipalidad no es un mercado. El decreto no se tokeniza: se protocoliza. El permiso de edificación no se cede: es expediente. Contraloría no escribe el libro comunal: lo lee. Esas tres frases son invariantes. Si una implementación las viola, deja de ser este producto.

El AND es el modo operativo. Quórum 6/8 AND fe pública. Partida AND visación AND decreto. Junta AND acuse. Notificación AND sentencia. ZK AND RSH. DOM AND pago AND CIP AND fe. Composición AND visación AND fe. Una rama verdadera no promulga. OR nunca cierra un acto de Ley 18.695.

POLÍTICO

El alcalde exige por escrito que ningún decreto se considere protocolizado con una sola rama criptográfica ni con un solo oficio.

ADMINISTRATIVO

Secretaría protocoliza cuando el verificador híbrido de las dos claves de fe dice uno. Tesorería no gira sin decreto.

TÉCNICO

verify = ML-DSA-65 ∧ P-256 en el bloque. verify_fe = firma_alcalde ∧ firma_secretario sobre canonical_fe. SHA-256 encadena el evento.

Arquitectura

El organismo de producción del libro es Rust. El escritorio es la cara administrativa. No se reescribe la SPA como nodo. El nodo no reimplementa el prover Groth16.

Crates del núcleo

Crate	Oficio
abraxas-crypto	HybridKeypair, sign/verify AND, SHA-256
abraxas-chain	PoA, header, extrínseco, génesis
abraxas-identity	DID abraxas/cbc, issue, revocación de asiento
abraxas-seal	Sello de documento y canonical_fe
abraxas-oracle	Dictamen apto / no apto / observado
abraxas-perimeter	Security Suite 4.7.2, MITRE, fail-closed
abraxas-municipal	Libro de diez lotes, oficios de fe, RWA
abraxas-runtime	apply, itinerario, passthrough 23516, pilares
abraxas-node	CLI: itinerario, fe, identity, seal, protect

Cada acto que entra al runtime: DID bien formado; hop regional solo con sello y digest de 64 hex; cinco pilares (NeuroFirewall, Escudo cuántico, Identidad, Oráculo, Gobernanza); máquina del lote; bloque PoA firmado. Parent del primer bloque = génesis SHA-256 de abraxas-dlt-municipal|las-encinas|ley-18.695|genesis.

Dos capas de sello

El nodo sella el bloque con un par híbrido de autoridad PoA. La fe pública del decreto es otra capa: dos pares de oficio. Confundirlas es el error que este diseño se niega a cometer.

Criptografía

Primitivas de producción

Primativa	Norma	Uso	Qué no hace
ML-DSA-65	FIPS 204	Rama PQ de firma	No cifra ni hashea
ECDSA P-256	FIPS 186-5	Rama clásica, afín a Ley 19.799	No sobrevive sola a Shor
SHA-256	FIPS 180-4	Libro, digest, huella	No es firma
ML-KEM-768	FIPS 203	Canal al abrir Quantum Gate	No sella el decreto
Groth16 / BN254	Circom 2.2.2	Prueba de identidad viva	No es fe pública

verify_and rechaza firma PQ o EC vacía (Incomplete) y rechaza la misma clave en los dos oficios (SameOffice). El test hybrid_roundtrip firma «Ley 18.695 art. 63 fe pública Las Encinas» y exige que un mensaje adulterado falle.

fips204 0.4 y @noble/post-quantum implementan ML-DSA-65. Ninguno es módulo CMVP. La rama P-256 camina sobre una pila más madura (WebCrypto / p256). El AND cubre esa asimetría de madurez. SLH-DSA (FIPS 205) está en doctrina como paracaídas; no está implementado.

AULA FRENTE A PRODUCCIÓN

Ring-LWE n=8 y Schnorr de pizarra son aula. Producción es ML-DSA-65 □ P-256. Confundir el aula con el nodo es el mismo error que confundir Groth16 con la fe del Secretario.

Fe pública de dos oficios

El payload canónico es JSON estable: alg, art 63, comuna, decretoId, kind decreto, ley 18.695, org Abraxas Intellect, sesionId, title. Alcalde y Secretario firman esos bytes. protocolizar verifica las dos firmas contra las claves vigentes de los oficios.

1. instalar_oficios: dos HybridPublic distintas en el libro.
2. firmar_alcalde / firmar_secretario: cada uno verifica su DID, su clave vigente y su firma sobre el canónico.
3. protocolizar: quórum 6/8 □ ambas firmas □ oficios vigentes □ oficios distintos.
4. dejar_cargo: vigente=false; la privada se apaga en el escritorio.
5. asumir_cargo: par nuevo. El DID del asiento no cambia. Hay que volver a firmar.

Si el Alcalde deja el cargo después de firmar y antes de protocolizar, el decreto no nace. Si asume con clave nueva, las firmas viejas no verifican. Eso no es un bug: es el art. 63.

Diez lotes como máquinas de estado

Itinerario

Lote	Predicado	Cierre
1 Gobierno	6/8 □ fe pública	arts. 56 y 63
2 Hacienda	partida □ visación □ decreto	Título IV · D.L. 3.063
3 SECPLA	hito □ PRC vigente	art. 21
4 Barrio	junta □ acuse ≤20 días	Ley 19.418
5 JPL	notificación □ sentencia	Ley 15.231
6 Región	postulación □ adjudicación · hop 23516	Ley 19.175
7 Ventanilla	ZK □ RSH booleanos	arts. 4 y 25
8 Observatorio	CGR lee	Ley 20.285 · 10.336
9 DOM	ZK □ pago □ CIP □ DOM □ fe	LGUC 116
10 Cierre	composición □ visación □ fe	art. 67

La cuenta pública del lote 10 no se arma si falta un lote anterior. El itinerario ejecuta 40 actos, 40 bloques. ceder en DOM siempre falla: el permiso no es un mercado.

Identidad, Groth16 y RWA

DID: did:abraxas:encinas:{asiento}. Se hereda did:cbc:. Las verticales no inventan identidad. identity_hash es SHA-256 del asiento, nombre, cargo, foto y org.

IdViva.circom: 269 constraints. Públicos [stmt, ok]. El dispositivo extrae bits; el circuito prueba AND de identidad viva y un nullifier Poseidon. No es un Merkle del padrón RUN. BN254 ofrece del orden de cien bits clásicos y es un blanco más barato para Shor que P-256. No es la firma del decreto.

RWA del DOM: token de expediente administrativo, soulbound. mintear exige ZK pago CIP firma DOM fe. transferir_rwa siempre err. El plano no es un título negociable.

Perímetro, interop y amenazas

- Fail-closed: una capa que cierra cierra la puerta.
- Quantum Gate sella ALLOW/BLOCK con ML-DSA-65 P-256. ALLOW sin sello verificado degrada a BLOCK.
- El paso abierto encapsula en ML-KEM-768 (cosechar ahora, descifrar después).
- Honor/Huawei: cerrar no apaga. El centinela permanece en el libro local.
- Homoglyph: lista blanca de anfitriones oficiales. Punycode y c1aveunica cierran.
- MITRE en el hop: T1218 LOLBin, T1105 transferencia, T1059 intérprete, T1566 phishing, T1027 ofuscación. Volcado y PE MZ no llegan a la puerta.
- Catálogo anclado: 39.450 firmas, tope de mezcla 50.000. El persist no guarda el catálogo. La 4.7.2 tira el cajón envenenado al arrancar y cambia la llave.
- Oráculo: CISA KEV, CIRCL, URLhaus, ThreatFox, OpenPhish, Feodo, SSLBL, MalwareBazaar, Phishing Army.
- La 4.6.1 queda en el historial. La 4.7.0 es la base MITRE. La 4.7.1 no vaciaba el cajón. Las 4.5.6 a 4.5.9 no se distribuyen. No es antivirus: SENTINEL 5.0.5 cubre disco y memoria sentada.

ISO/TS 23516: passthrough solo con sello híbrido y digest SHA-256 de 64 hex. Puente opaco prohibido. CGR no escribe. El oráculo normativo dictamina NoApto si hay ficha en claro, cesión de permiso, ECDSA sola o puente opaco.

Lo que este white paper no promete

- PKI de 19 pares con ceremonia y HSM.
- Módulo FIPS 140 validado CMVP.
- KDF(ECDH ML-KEM) de expediente completo — el KEM está en la puerta, no en cada plano.
- SLH-DSA desplegado.
- Schnorr sobre secp256k1 como firma de producción del decreto (producción es P-256 ML-DSA-65).

Paquete normativo

- Ley 18.695 · orgánica constitucional de municipalidades
- Ley 19.799 · documentos electrónicos y firma electrónica
- Ley 19.628 y Ley 21.719 · datos personales
- Ley 20.285 · transparencia
- Ley 21.180 · transformación digital del Estado
- Ley 21.383 · neuroderechos
- LGUC / OGUC art. 116 · permiso de edificación
- Ley 19.418, 15.231, 19.175, D.L. 3.063, Ley 10.336
- FIPS 204 / 186-5 / 203 / 180-4
- ISO 22739, ISO 23257, ISO/TS 23516, NCh-ISO 27001:2023
- W3C DID Core 1.0 · W3C VC 2.0

Referencia de producto para el oráculo: «Abraxas DLT Municipal Ley 18.695 híbrido ML-DSA FIPS 204 arquitectura 23257 vocabulario 22739 interop 23516 SGSI 27001». Sin esa cadena, ECDSA sola transgrede FIPS 204.