LM — Catálogo General de Tokens (v2)

Perfil híbrido: contenido privado off-chain + identidad/estado/auditoría tokenizados (on-chain cuando convenga)

Uso interno — ontología, operación, legal, contabilidad e implementación técnica.

Fecha: 2026-01-29 | Versión: v2.0

Objetivo: mantener un catálogo semántico único y añadir un mapeo de implementación para blockchain (sin duplicar el catálogo).

Este v2 añade una plantilla estándar de ficha con campos de asentamiento (on-chain/off-chain/híbrido), tipo de artefacto on-chain, prueba criptográfica, control de acceso y modelo de custodia.

1. Definición base y principios de implementación

Un token es una entidad digital que representa un hecho/derecho/relación/documento/habilidad o permiso, con identidad criptográfica, estado verificable, historia auditable y permisos de acceso.

Principio híbrido: el contenido sensible (PII, contratos completos, datos bancarios, PDFs, imágenes) vive en sistemas privados (cliente o LM Vault); la cadena registra identidad, estado, permisos y pruebas (hashes, firmas, timestamps).

Principio de no duplicación: no creamos un “catálogo cripto” separado; añadimos un Blockchain Profile que mapea cada token a su representación técnica.

1.1 Plantilla estándar de ficha de token (v2)

• Definición: qué representa y qué NO representa.

• Campos mínimos (semánticos): el conjunto más pequeño para operar y auditar.

• Ciclo de vida: estados principales (state machine).

• Relaciones: tokens que referencia o que lo referencian.

• Evidencia: qué documentos se adjuntan (EvidenceToken) y en qué momento.

• Asentamiento: OFF-CHAIN | ON-CHAIN | HÍBRIDO (por defecto, y excepciones).

• Artefacto on-chain: registro/estado, eventos, NFT/1155, anclaje (Merkle root), etc.

• Tipo de prueba: hash(archivo), hash(bundle), merkle_root, firma, tx hash, timestamp.

• Control de acceso: PermissionToken/OPA/política, y qué se publica vs se cifra.

• Custodia: cliente (self-custody), MPC/custodio, LM-managed (si aplica) y rotación.

2.1 EvidenceToken

Definición: Puntero verificable a documento/evidencia privada (PDF, imagen, XML, audio) cifrada. Guarda hash, metadatos y vínculo con el token que respalda.

Campos mínimos: evidence_id, hash, type, storage_uri, created_at, linked_to, permission_ref

Ciclo de vida: CAPTURED → HASHED → VERIFIED → LOCKED → SUPERSEDED

Relaciones: Se enlaza a ContractToken, InvoiceToken, PayrollRunToken, PacketToken, etc.

Evidencia: El archivo vive off-chain (cliente o LM Vault). La cadena guarda hash, timestamp, tipo y referencia.

Implementación (perfil): HÍBRIDO: archivo cifrado off-chain; on-chain: hash + URI (opcional) + refs de permisos. Prueba: hash(archivo) y/o merkle_root de PacketToken.

2.2 PermissionToken

Definición: Permiso/consentimiento gobernable para acceder, compartir o procesar datos. Define quién, qué, por cuánto tiempo y bajo qué propósito.

Campos mínimos: permission_id, principal_ref, resource_ref, scope, purpose, expires_at, granted_by, status

Ciclo de vida: ACTIVE → EXPIRED → REVOKED

Relaciones: Se aplica a EvidenceToken, ClientDossierToken, PacketToken y cualquier recurso sensible.

Evidencia: Adjuntar evidencia de consentimiento cuando aplique (EvidenceToken o AttestationToken).

Implementación (perfil): ON-CHAIN (o híbrido): registrar concesión/revocación como eventos. No publicar PII: usar principal_ref y resource_ref opacos. Prueba: firma + timestamp.

2.3 PolicyToken

Definición: Regla formal versionada que controla decisiones automáticas (umbrales, quórum, excepciones, ventanas de tiempo) en pagos, acceso y cierres.

Campos mínimos: policy_id, domain, rules_ref, thresholds, quorum, version, status, approved_by

Ciclo de vida: DRAFT → ACTIVE → DEPRECATED

Relaciones: Referenciado por PaymentBatchToken, ApprovalRequestToken, MonthlyCloseToken.

Evidencia: EvidenceToken de aprobación y cambios de política.

Implementación (perfil): ON-CHAIN (recomendado para auditabilidad): publicar versión + hash(rules_ref) + eventos de activación. El texto completo puede vivir off-chain.

2.4 ApprovalRequestToken / AuthorizationSignatureToken

Definición: Solicitud de aprobación multi-rol y firmas humanas vinculadas a un alcance (pago, cierre, cambio de cuenta, etc.).

Campos mínimos: approval_request_id, scope_ref, required_roles, quorum, expires_at, status; y signature_id, signer_ref, role, method, timestamp, scope_ref

Ciclo de vida: OPEN → PARTIALLY_SIGNED → APPROVED/REJECTED/EXPIRED; firmas: RECORDED

Relaciones: Se usa con PolicyToken, AuthChallengeToken y PaymentBatchToken.

Evidencia: EvidenceToken opcional (capturas, comprobantes, justificantes).

Implementación (perfil): ON-CHAIN: eventos de firma y resultado; scope_ref apunta a PacketToken o PaymentBatchToken. Prueba: firma + tx hash + timestamp. No guardar secretos.

3. Mapeo maestro: tokens vs asentamiento y representación

Este cuadro define el perfil por defecto. En implementación real se ajusta por cliente (SaaS, BYOC, on-prem) y por requerimientos regulatorios.

Token	Asentamiento por defecto	Artefacto/representación	Tipo de prueba	Nota de privacidad
Token	HÍBRIDO	Eventos + refs	hash + firma	Minimizar PII.
TokenIdentity	HÍBRIDO	Eventos + refs	hash + firma	Minimizar PII.
EvidenceToken	HÍBRIDO	Registro + hash + puntero (URI) + permisos	hash(archivo) o hash(bundle)	Contenido cifrado off-chain; on-chain solo hash/URI metadatos mínimos.
PermissionToken	ON-CHAIN (o híbrido)	Eventos + estado (state machine) / registro	firma + timestamp + hash(scope)	No guardar secretos ni PII; guardar refs y pruebas.
PolicyToken	ON-CHAIN (o híbrido)	Eventos + estado (state machine) / registro	firma + timestamp + hash(scope)	No guardar secretos ni PII; guardar refs y pruebas.
GovernanceToken	ON-CHAIN (o híbrido)	Eventos + estado (state machine) / registro	firma + timestamp + hash(scope)	No guardar secretos ni PII; guardar refs y pruebas.
LeadToken	HÍBRIDO	Identidad de entidad + refs (no PII) + permisos	hash(refs) + firmas	PII/IDs fiscales siempre off-chain, referenciados.
ClientToken	HÍBRIDO	Identidad de entidad + refs (no PII) + permisos	hash(refs) + firmas	PII/IDs fiscales siempre off-chain, referenciados.
QuoteToken	HÍBRIDO	Eventos + refs	hash + firma	Minimizar PII.
DealToken	HÍBRIDO	Eventos + refs	hash + firma	Minimizar PII.
ContractToken	HÍBRIDO	Eventos + refs	hash + firma	Minimizar PII.
ClientDossierToken	HÍBRIDO	Identidad de entidad + refs (no PII) + permisos	hash(refs) + firmas	PII/IDs fiscales siempre off-chain, referenciados.
WorkOrderToken	HÍBRIDO	Eventos + estado; evidencia off-chain	hash(evidencia) + firma	Fotos, ubicaciones precisas, datos sensibles: off-chain.
TaskToken	HÍBRIDO	Eventos + estado; evidencia off-chain	hash(evidencia) + firma	Fotos, ubicaciones precisas, datos sensibles: off-chain.
QARecordToken	HÍBRIDO	Eventos + estado; evidencia off-chain	hash(evidencia) + firma	Fotos, ubicaciones precisas, datos sensibles: off-chain.
DisputeToken	HÍBRIDO	Eventos + estado; evidencia off-chain	hash(evidencia) + firma	Fotos, ubicaciones precisas, datos sensibles: off-chain.
AttestationToken	HÍBRIDO	Eventos + estado; evidencia off-chain	hash(evidencia) + firma	Fotos, ubicaciones precisas, datos sensibles: off-chain.
WorkerToken	HÍBRIDO	Identidad de entidad + refs (no PII) + permisos	hash(refs) + firmas	PII/IDs fiscales siempre off-chain, referenciados.

Token	Asentamiento por defecto	Artefacto/representación	Tipo de prueba	Nota de privacidad
IncidentToken	HÍBRIDO	Estado y agregados on-chain; detalle off-chain	hash(bundle) + firma	Cumplimiento/regulado: minimizar exposición, usar agregados/refs.
PayrollRunToken	HÍBRIDO	Estado y agregados on-chain; detalle off-chain	hash(bundle) + firma	Cumplimiento/regulado: minimizar exposición, usar agregados/refs.
PayrollDeductionToken	HÍBRIDO	Estado y agregados on-chain; detalle off-chain	hash(bundle) + firma	Cumplimiento/regulado: minimizar exposición, usar agregados/refs.
RemittanceToken	HÍBRIDO	Estado/permiso on-chain; detalles off-chain	hash(bundle) + firma + conciliación	Datos bancarios off-chain; on-chain solo refs, montos agregados si es aceptable.
ROEToken	HÍBRIDO	Estado y agregados on-chain; detalle off-chain	hash(bundle) + firma	Cumplimiento/regulado: minimizar exposición, usar agregados/refs.
T4BatchToken	HÍBRIDO	Estado y agregados on-chain; detalle off-chain	hash(bundle) + firma	Cumplimiento/regulado: minimizar exposición, usar agregados/refs.
WSIBToken	HÍBRIDO	Estado y agregados on-chain; detalle off-chain	hash(bundle) + firma	Cumplimiento/regulado: minimizar exposición, usar agregados/refs.
EHTToken	HÍBRIDO	Estado y agregados on-chain; detalle off-chain	hash(bundle) + firma	Cumplimiento/regulado: minimizar exposición, usar agregados/refs.
FundingRequestToken	HÍBRIDO	Estado/permiso on-chain; detalles off-chain	hash(bundle) + firma + conciliación	Datos bancarios off-chain; on-chain solo refs, montos agregados si es aceptable.
PaymentBatchToken	HÍBRIDO	Estado/permiso on-chain; detalles off-chain	hash(bundle) + firma + conciliación	Datos bancarios off-chain; on-chain solo refs, montos agregados si es aceptable.
PaymentToken	HÍBRIDO	Estado/permiso on-chain; detalles off-chain	hash(bundle) + firma + conciliación	Datos bancarios off-chain; on-chain solo refs, montos agregados si es aceptable.
ApprovalRequestToken	ON-CHAIN (o híbrido)	Eventos + estado (state machine) / registro	firma + timestamp + hash(scope)	No guardar secretos ni PII; guardar refs y pruebas.
AuthorizationSignatureToken	ON-CHAIN (o híbrido)	Eventos + estado (state machine) / registro	firma + timestamp + hash(scope)	No guardar secretos ni PII; guardar refs y pruebas.
AuthChallengeToken	ON-CHAIN (o híbrido)	Eventos + estado (state machine) / registro	firma + timestamp + hash(scope)	No guardar secretos ni PII; guardar refs y pruebas.
BankMovementToken	HÍBRIDO	Estado y agregados on-chain; detalle off-chain	hash(bundle) + firma	Cumplimiento/regulado: minimizar exposición, usar agregados/refs.

Token	Asentamiento por defecto	Artefacto/representación	Tipo de prueba	Nota de privacidad
ValueTransferToken	HÍBRIDO	Eventos + estado; evidencia off-chain	hash(evidencia) + firma	Fotos, ubicaciones precisas, datos sensibles: off-chain.
InvoiceToken	HÍBRIDO	Estado contable on-chain; comprobantes off-chain	hash(comprobante) + firma	Evitar datos fiscales detallados en cadena; usar refs.
AccountsReceivableToken	HÍBRIDO	Estado contable on-chain; comprobantes off-chain	hash(comprobante) + firma	Evitar datos fiscales detallados en cadena; usar refs.
JournalEntryToken	HÍBRIDO	Estado contable on-chain; comprobantes off-chain	hash(comprobante) + firma	Evitar datos fiscales detallados en cadena; usar refs.
ExportBatchToken	HÍBRIDO	Estado contable on-chain; comprobantes off-chain	hash(comprobante) + firma	Evitar datos fiscales detallados en cadena; usar refs.
MonthlyCloseToken	ON-CHAIN (o híbrido)	Eventos + estado (state machine) / registro	firma + timestamp + hash(scope)	No guardar secretos ni PII; guardar refs y pruebas.
InventoryItemToken	HÍBRIDO	Estado y agregados on-chain; detalle off-chain	hash(bundle) + firma	Cumplimiento/regulado: minimizar exposición, usar agregados/refs.
InventoryEventToken	HÍBRIDO	Eventos + estado; evidencia off-chain	hash(evidencia) + firma	Fotos, ubicaciones precisas, datos sensibles: off-chain.
CostAllocationToken	HÍBRIDO	Eventos + estado; evidencia off-chain	hash(evidencia) + firma	Fotos, ubicaciones precisas, datos sensibles: off-chain.
SkillToken	HÍBRIDO	Estado y agregados on-chain; detalle off-chain	hash(bundle) + firma	Cumplimiento/regulado: minimizar exposición, usar agregados/refs.
CredentialToken	HÍBRIDO	Estado y agregados on-chain; detalle off-chain	hash(bundle) + firma	Cumplimiento/regulado: minimizar exposición, usar agregados/refs.
PerformanceToken	HÍBRIDO	Eventos + estado; evidencia off-chain	hash(evidencia) + firma	Fotos, ubicaciones precisas, datos sensibles: off-chain.
PacketToken	ON-CHAIN (o híbrido)	Eventos + estado (state machine) / registro	firma + timestamp + hash(scope)	No guardar secretos ni PII; guardar refs y pruebas.
ChainProfileToken	OFF-CHAIN + hash ON-CHAIN	Perfil de red confirmado por hash	hash(config) + firma de governance	Contiene endpoints/IDs; mantener privado; publicar hash y versión.
SmartContractDeploymentToken	ON-CHAIN	Direcciones de contratos + versión + ABI hash	hash(ABI) + tx hash	No sensibles; incluir metadatos técnicos.
OnChainTxToken	ON-CHAIN	Registro de transacción (tx) vinculada a scope	tx hash + receipt	No PII; vincular a scope_ref.

Token	Asentamiento por defecto	Artefacto/representación	Tipo de prueba	Nota de privacidad
WalletPrincipalToken	HÍBRIDO	Registro de wallet/actor + roles	firma wallet + issuer signature	No asociar PII directa; usar identity_refs.
CustodyAccountToken	HÍBRIDO	Cuenta custodia/MPC + policy refs	firma + attestations	IDs de custodia privados; publicar solo refs.
AnchorBatchToken	ON-CHAIN	Merkle root de lote + timestamp	merkle_root + tx hash	Sin contenido; solo root y metadatos.
KeyRotationToken	HÍBRIDO	Rotación de llaves y vigencias	firma old+new + governance	Mantener material de llaves fuera; registrar eventos/huellas.

4. Tokens de integración blockchain (añadidos en v2)

4.1 ChainProfileToken

Definición: Perfil técnico por cliente/entorno: red, método de anclaje, contratos activos, parámetros de fees, y reglas de publicación.

Campos mínimos: profile_id, client_ref, chain_type, network_id, rpc_refs, contract_set_ref, anchoring_policy_ref, version, status

Ciclo de vida: DRAFT → ACTIVE → ROTATED → DEPRECATED

Relaciones: Referenciado por GovernanceToken, SmartContractDeploymentToken y AnchorBatchToken.

Evidencia: Evidencia de aprobación y cambios (GovernanceToken + EvidenceToken).

Implementación (perfil): OFF-CHAIN + hash ON-CHAIN: mantener endpoints y detalles privados; publicar hash(config) y versión para verificabilidad.

4.2 SmartContractDeploymentToken

Definición: Registro de despliegues de contratos: direcciones, versión, hash de ABI, y control de upgrades.

Campos mínimos: deployment_id, chain_profile_id, contract_name, address, abi_hash, version, deployed_by, deployed_at, status

Ciclo de vida: DEPLOYED → ACTIVE → UPGRADED → RETIRED

Relaciones: Relaciona GovernanceToken y OnChainTxToken (transacciones de despliegue).

Evidencia: EvidenceToken opcional (audit report, revisión).

Implementación (perfil): ON-CHAIN: la existencia del contrato es on-chain; el token organiza metadatos y gobierno. Prueba: tx hash + receipt + abi_hash.

4.3 OnChainTxToken

Definición: Referencia normalizada de transacción on-chain vinculada a un alcance (scope_ref): anclaje, aprobación, ejecución.

Campos mínimos: tx_token_id, chain_profile_id, tx_hash, scope_ref, kind, submitted_at, confirmed_at, status

Ciclo de vida: SUBMITTED → CONFIRMED → FAILED

Relaciones: Referenciado por ApprovalRequestToken, AnchorBatchToken, PaymentBatchToken (si aplica).

Evidencia: N/A (la prueba es el receipt on-chain).

Implementación (perfil): ON-CHAIN: registrar tx_hash y vincularlo a scope_ref. Prueba: receipt y confirmaciones.

4.4 WalletPrincipalToken / CustodyAccountToken / KeyRotationToken

Definición: Actores criptográficos (wallets) y cuentas de custodia (MPC/custodio), y eventos de rotación de llaves para demostrar continuidad y control.

Campos mínimos: wallet_id, principal_ref, pubkey_or_address, roles, status; custody_account_id, provider_ref, policy_ref; key_rotation_id, subject_ref, old_fingerprint, new_fingerprint, effective_at

Ciclo de vida: ACTIVE/REVOKED; y ROTATED por eventos

Relaciones: Se conecta con PermissionToken, GovernanceToken y AuthorizationSignatureToken.

Evidencia: EvidenceToken cuando haya verificación de custodio o auditoría.

Implementación (perfil): HÍBRIDO: datos sensibles de custodia fuera de cadena; en cadena se anclan huellas, vigencias y eventos de gobierno.

4.5 AnchorBatchToken

Definición: Anclaje por lotes: publica Merkle root de un conjunto de evidencias/eventos (PacketToken) para bajar costos y minimizar exposición.

Campos mínimos: anchor_id, packet_ref, merkle_root, anchored_at, tx_ref, status

Ciclo de vida: BUILT → ANCHORED → VERIFIED

Relaciones: Se relaciona con PacketToken y OnChainTxToken.

Evidencia: N/A (la raíz prueba integridad del paquete).

Implementación (perfil): ON-CHAIN: merkle_root + timestamp + tx hash. El paquete completo vive off-chain.

5. Notas y referencias

Este catálogo v2 es compatible con v1: mantiene semántica estable y añade un perfil de implementación blockchain. Debe versionarse (nombres ajustables; semántica estable).

Referencias: estándares de autenticación (WebAuthn/FIDO2), lineamientos de identidad digital (NIST), y prácticas de auditoría (append-only logs, hashes, Merkle trees).

Uso: para cada cliente, definir un ChainProfileToken y ajustar el mapeo por restricciones legales, residencia de datos y preferencias de despliegue (SaaS, BYOC, on-prem).