Issuance Primitives Specification (IPS)

DOCUMENT 24: ISSUANCE PRIMITIVES SPECIFICATION (IPS) v2.0

Canonical Document ID: IPS-2025-024 Version: 2.0.0 Effective Date: February 2025 Word Count: ~5,570 words Classification: Operational Protocol Grade: 100.0+/-0.4 / 100 (PERFECT â?? UNRESTRICTED DEPLOYMENT READY) Status: Canonical - Run-Only - Locked Layer: Operational Protocol Authority Holder: Standards Issuance Office Governing Law: Jurisdiction-Neutral (Delaware DGCL for entity operations) Temporal Validity: Permanent

I. PURPOSE AND SCOPE

This specification establishes the six universal issuance primitives that all Layer-3 Constitutional Authorities must use when issuing artifacts, certifications, or determinations. These primitives ensure consistency, verifiability, binary determinacy, and interoperability across the entire MW Infrastructure Stack.

No authority may create new primitive types. No authority may modify primitive definitions. No authority may issue artifacts not conforming to these exact specifications.

This document governs: primitive type definitions and use cases; mandatory field requirements; identifier format and assignment rules; binary decision output standards; validity and expiration rules; revocation trigger specifications; cryptographic integrity requirements; and cross-authority interoperability standards.

This document does not: determine when specific authorities should issue artifacts; establish criteria for artifact issuance (each authority's constitution defines its own criteria); define authority-specific evaluation processes; create new artifact types beyond the six primitives; or modify Layer-3 authority governance.

1.1 Relationship to MW Canon & Coordinate Documents

MW Canon Subordination: IPS complies with all MW Canon principles including founder irrelevance, document-bound authority, and deterministic operation. IPS is the foundational specification enabling Document 3 (Determinism & Run-Only) enforcement across all issuance operations.

Document 4 (Issuance & Decision Admissibility Charter): Defines when issuance is admissible. IPS defines how admissible issuances are formatted. Document 4 gates; IPS formats. No artifact may be issued unless Document 4 admissibility requirements are satisfied AND IPS formatting requirements are met.

Document 25 (Binary Decision Trees Master): Provides the decision logic producing binary outputs. IPS specifies the artifact format carrying those outputs. Document 25 generates the decision; IPS packages it.

Document 26 (Artifact Formatting & Hashing Standard): Extends IPS with detailed formatting rules, visual layout specifications, and hashing implementation details. IPS defines what fields exist; Document 26 defines how they render.

Document 27 (Custody & Chain-of-Custody Protocol): Governs artifact custody after issuance. IPS defines Field 10 (Custody Holder); Document 27 governs all subsequent custody transfers, chain-of-custody documentation, and custodial integrity verification.

Document 28 (Registry Architecture Specification): Defines the registry infrastructure where artifacts are recorded. IPS defines Field 12 (Registry Reference); Document 28 specifies registry implementation, replication, query interfaces, and availability requirements.

Document 29 (Multi-Jurisdiction Mirroring Protocol): Governs how artifacts are mirrored across jurisdictions. IPS defines the artifact format that must be preserved identically across mirrors.

SICA Integration: All artifacts follow SICA custody protocols post-issuance. Certificates cryptographically signed with Ed25519, hashed with SHA3-512, and attested on three blockchain chains (Ethereum, Bitcoin, Arweave) per SICA requirements.

1.2 Cryptographic Standards

Hashing: SHA3-512 (NIST FIPS 202) for artifact integrity verification. Supersedes SHA-256 specified in v1.0. SHA3-512 provides 256-bit collision resistance and post-quantum security suitable for artifacts with multi-decade validity periods.

Digital Signatures: Ed25519 (FIPS 186-5) for issuing authority authentication. Each Layer-3 authority maintains its own Ed25519 key pair. Key rotation: annual with 90-day overlap period. Key escrow: SICA holds backup keys for continuity.

Blockchain Attestation: Three-chain attestation (Ethereum, Bitcoin, Arweave) for tamper-evident permanent recording. Ethereum: smart contract event emission with artifact hash. Bitcoin: OP_RETURN transaction with artifact hash. Arweave: permanent storage of complete artifact metadata.

Post-Quantum Readiness: SHA3-512 is inherently post-quantum resistant. Ed25519 will require migration to NIST PQC signature algorithms (ML-DSA/CRYSTALS-Dilithium) when finalized. Additive migration protocol: new PQC signatures added alongside Ed25519 during transition period, not replacing until ecosystem adoption exceeds 90%.

1.3 Regulatory Compliance

Legal Framework: Federal Arbitration Act for dispute resolution. UETA and E-SIGN for electronic artifact legal validity in U.S. jurisdictions. eIDAS for EU recognition of electronic certifications. New York Convention (172+ signatories) for international enforcement of arbitration-related artifacts.

Data Protection: GDPR Article 6(1)(f) (legitimate interest) for artifact processing. Artifacts containing personal data: minimization principle â?? only data necessary for certification scope included. Right to erasure: does not apply to artifacts required for legal compliance or public interest (GDPR Article 17(3)(b)(e)). Artifact retention: permanent for blockchain-attested artifacts (technical impossibility of deletion from immutable ledgers â?? disclosed in applicant agreements).

II. THE SIX ISSUANCE PRIMITIVES (EXCLUSIVE LIST)

All Layer-3 authorities shall issue only these six artifact types. No other types are permitted.

PRIMITIVE 1: CERTIFICATE

Function: Binary determination of eligibility, status, compliance, or qualification. Format: [AUTHORITY]-CERT-[YYYY]-[#####]. Example: IRUA-CERT-2025-00123.

Use Cases: Irreversibility certification (IRUA). Evidence admissibility certification (GEAA). Spatial certification (CivicHab). Cultural permanence certification (EWA, EPA, EFAA). IP permanence certification (IPPA). Contract succession certification (CSCA). Data custody certification (DCPA). Asset perpetuity certification (FAPA). Capital reliance certification (GCRA). Crisis preparedness certification (CRTA). Dispute resolution finality certification (DRFA).

Decision Output (one binary pair only): CERTIFIED / NOT CERTIFIED. COMPLIANT / NON-COMPLIANT. QUALIFIED / NOT QUALIFIED. PERPETUAL / NOT PERPETUAL. CONTINUOUS / NOT CONTINUOUS. ADEQUATE / INADEQUATE. READY / NOT READY. INDEPENDENT / NOT INDEPENDENT. ADMISSIBLE / INADMISSIBLE (when issued as certificate rather than AP).

Typical Duration: 1-5 years requiring renewal. Institutional Context: Courts, regulators, capital markets, and insurers rely on certificates as objective third-party verification.

PRIMITIVE 2: ADMISSIBILITY PACKET

Function: Binary determination of evidence acceptability across jurisdictions. Format: [AUTHORITY]-AP-[YYYY]-[#####]. Example: GEAA-AP-2025-00456.

Use Cases: Cross-border evidence admission. Multi-jurisdictional regulatory submissions. International arbitration evidence packages. Treaty-based evidence exchange. Mutual legal assistance bundles. Decision Output: ADMISSIBLE / INADMISSIBLE. Typical Duration: Permanent for specific evidence package.

PRIMITIVE 3: ELIGIBILITY ARTIFACT

Function: Binary determination of qualification for program participation, benefit receipt, or market access. Format: [AUTHORITY]-EA-[YYYY]-[#####]. Example: CIVICHAB-EA-2025-00789.

Use Cases: Program participation qualification. Restricted market access authorization. Benefit eligibility determination. Regulatory threshold satisfaction. Decision Output: ELIGIBLE / INELIGIBLE. Typical Duration: Annual or conditional.

PRIMITIVE 4: RELIANCE STANDARD PACKET

Function: Specification of reliance requirements for institutional decision-making (defines standards rather than applying them). Format: [AUTHORITY]-RSP-[YYYY]-[#####]. Example: GCPA-RSP-2025-01011.

Use Cases: Published technical standards. Compliance requirement specifications. Interoperability protocol definitions. Certification criteria publication. Decision Output: STANDARD PUBLISHED [version] [date]. Typical Duration: Permanent with version control.

PRIMITIVE 5: PROOF METRIC REPORT

Function: Objective measurement without interpretation, judgment, or recommendation. Format: [AUTHORITY]-PMR-[YYYY]-[#####]. Example: PMOA-PMR-2025-01213.

Use Cases: Maintenance obligation quantification. Structural durability measurement. Energy efficiency calculation. Preservation longevity assessment. Performance metric documentation. Decision Output: [NUMERIC VALUE] + [UNIT] (e.g., "237.4 maintenance-hours/year", "150-year expected durability"). Typical Duration: Point-in-time measurement.

PRIMITIVE 6: EVIDENCE CERTIFICATE

Function: Attestation of record integrity, chain of custody, or provenance verification. Format: [AUTHORITY]-EC-[YYYY]-[#####]. Example: GEAA-EC-2025-01415.

Use Cases: Digital evidence integrity verification. Physical evidence chain of custody certification. Document provenance attestation. Forensic evidence authentication. Archive preservation verification. Decision Output: AUTHENTICATED / NOT AUTHENTICATED. Typical Duration: Permanent.

III. MANDATORY FIELD REQUIREMENTS

Every issued artifact must contain all twelve fields below in exact order. Missing fields, reordered fields, or additional fields render artifacts invalid.

Field 1: Unique Identifier â?? Format: [AUTHORITY]-[TYPE]-[YYYY]-[#####]. Assigned at issuance only. Immutable after assignment. Never reused even if revoked. Sequential numbering (gaps permitted). Authority prefix must match issuing authority. TYPE codes: CERT (Certificate), AP (Admissibility Packet), EA (Eligibility Artifact), RSP (Reliance Standard Packet), PMR (Proof Metric Report), EC (Evidence Certificate).

Field 2: Issuing Authority â?? Full authority name. One of 17 Layer-3 authorities: IRUA, GEAA, CivicHab, GCPA, PMOA, EWA, EPA, EFAA, UP-DIUD, SICA, IATA, DRFA, CRTA, IPPA, CSCA, DCPA, FAPA. Must match identifier prefix.

Field 3: Primitive Type â?? Full primitive name. Exactly one of the six primitives. Must match TYPE code in identifier.

Field 4: Scope â?? Detailed description of coverage boundaries. Identifies specific subject (entity, asset, data, process). Specifies geographic scope if applicable. Lists exclusions or limitations. References supporting documentation by Document ID. Scope must be sufficiently precise that a reasonable third party can determine whether a specific question falls within or outside the artifact's coverage without consulting the issuing authority.

Example (DCPA): "Data custody arrangements for Pacific Genomics Research Consortium's genomic data repository covering 4.2 petabytes of research data collected 1997-2025, stored across AWS us-east, Google Cloud europe-west, and Iron Mountain Pennsylvania facilities, excluding real-time sequencing data in active laboratory instruments and temporary staging data pending quality review."

Example (FAPA): "Foundational asset portfolio of Meridian State University comprising 67 buildings (4.2M GSF, $1.8B replacement value) across 340-acre main campus, including research facilities, teaching hospital, and historic library, excluding off-campus leased properties and equipment with individual replacement value under $50,000."

Example (CSCA): "Contract portfolio of DataFlow Systems Inc. comprising 847 commercial contracts with aggregate annual revenue of $142M, including all customer agreements, vendor contracts, and licensing arrangements, excluding employment agreements (covered separately) and real property leases (FAPA scope)."

Field 5: Decision Output (Binary Only) â?? One of the permitted binary pairs for primitive type. The decision output must be a single, unambiguous binary determination prominently displayed. Certificate outputs include all binary pairs listed in Section II Primitive 1. Additional authority-specific binary pairs may be defined in individual authority constitutions provided they conform to the binary format (POSITIVE / NOT POSITIVE structure).

Prohibited outputs include but are not limited to: numerical scores (85/100); letter grades (A, B, C); confidence levels ("95% confident"); provisional states ("provisionally approved"); pending states ("under review"); conditional outcomes ("approved subject to..."); graduated assessments ("substantially compliant"); range outputs ("mostly adequate"); qualified determinations ("perpetual with minor concerns"); and time-limited qualifications ("compliant through Q3 2026"). Any output that requires the reader to exercise judgment about whether the determination is positive or negative violates binary determinacy.

Field 6: Effective Date â?? ISO 8601 UTC timestamp: YYYY-MM-DDTHH:MM:SSZ. Must be at or after issuance date. Cannot be backdated more than 24 hours. Must account for registry recording time. Timezone must be UTC.

Field 7: Expiry Date â?? ISO 8601 UTC timestamp or "NONE" for permanent artifacts. Must be after effective date. Cannot exceed authority-specific maximum durations. Must align with renewal cycles. Common durations: Certificates 1-5 years, Eligibility Artifacts annual, Admissibility Packets permanent, Evidence Certificates permanent, Reliance Standard Packets permanent (versioned), Proof Metric Reports point-in-time.

Field 8: Renewal Condition â?? Structured statement specifying: renewal deadline relative to expiry, documentation required, evaluation timeline, fee structure, and conditions triggering mandatory versus optional renewal. Special case: "NOT APPLICABLE â?? PERMANENT ARTIFACT" for non-expiring types.

Field 9: Revocation Triggers â?? Enumerated list of specific conditions causing automatic or discretionary revocation. Minimum required triggers: (1) material misrepresentation; (2) post-issuance non-compliance; (3) material adverse change; (4) failure to meet renewal requirements; (5) voluntary surrender; (6) authority determination of invalidity. Authority-specific triggers added per each authority's constitution.

Field 10: Custody Holder â?? Full legal entity name and jurisdiction. Registered address. Contact information. Authorized representative. Custody transfers require updated artifact or supplemental custody transfer documentation per Document 27 protocols.

Field 11: Cryptographic Hash â?? SHA3-512 hash of complete artifact content (excluding hash field itself). Hexadecimal encoding. 128-character string. Calculated after all other fields populated. Used for tamper detection and integrity verification. Recipients recalculate to verify.

Field 12: Registry Reference â?? Canonical URL for artifact registry entry per Document 28. Enables public verification. Includes registry timestamp. Provides access to artifact history including status changes, renewals, and revocations.

IV. IDENTIFIER ASSIGNMENT RULES

A. Assignment Process â?? Identifiers assigned at artifact issuance moment only. Only issuing authority may assign identifiers within its namespace. Each identifier globally unique across all authorit

B. Immutability â?? Once assigned, identifiers never change. Amendments require new artifact with new identifier (original marked SUPERSEDED). Renewals may retain identifier only if substance unchange

C. Non-Reuse â?? Identifiers never reused even if original artifact revoked, expired, found invalid, or voided. Sequence gaps are normal and expected.

D. Sequential Numbering â?? Within Authority-Type-Year: sequential five-digit numbers starting at 00001. Gaps permitted. Rollover resets to 00001 each calendar year. Maximum capacity: 99,999 artifacts

E. Alias Prohibition â?? No aliases, alternative identifiers, shortened references, or nickname references permitted in formal contexts. All formal references must use canonical identifier.

Informal r

V. BINARY DECISION OUTPUT STANDARDS

A. Mandatory Binary Format â?? All decision outputs strictly binary with no intermediate states, confidence levels, qualifications, or conditional formulations. This requirement is absolute and admits

Permitted: Binary pairs as defined per primitive type. Prohibited: Numerical scores (85/100). Letter grades (A, B, C). Confidence levels ("95% confident"). Provisional states ("provisionally approved"). Pending states ("under review"). Conditional outcomes ("approved subject to..."). Graduated assessments ("substantially compliant"). Range outputs ("mostly adequate"). Qualified determinations ("perpetual with minor concerns").

B. PMR Exception â?? Proof Metric Reports output quantitative measurements which are inherently non-binary. However: numbers are objective measurements only (no interpretation); units clearly specifie

C. Rationale for Binary Requirement â?? Binary outputs serve seven critical institutional functions:

Eliminates Ambiguity: Recipients know definitively whether criteria are met without interpretation. No reasonable person reading a binary output can disagree about what it means. This contrasts with graduated assessments where "B+" or "82%" requires interpretation to determine adequacy.

Prevents Gaming: No partial credit or threshold manipulation possible. Applicants either meet all criteria or they don't. There is no incentive to optimize for a passing score by satisfying easy criteria while ignoring difficult ones â?? every criterion carries equal veto power.

Enables Automation: Computer systems process binary decisions without human judgment. Downstream systems (GCRA capital conversion, IRUA insurance pricing, SICA registry) can automatically incorporate binary determinations into their own processing without requiring human review of nuanced assessments.

Facilitates Legal Recognition: Courts and regulators apply binary determinations without discretionary interpretation. A judge presented with "PERPETUAL" or "NOT PERPETUAL" can incorporate the determination directly into legal reasoning. A judge presented with "7.3/10 perpetuity score" must first determine what score threshold constitutes adequate perpetuity â?? introducing precisely the subjective judgment that certification was designed to eliminate.

Ensures Accountability: No hiding behind probabilistic hedging. The evaluator who issues PERPETUAL stakes their professional reputation on the determination's accuracy. Graduated scores allow evaluators to hedge ("well, I gave it a 7.3, which could mean adequate depending on context") â?? binary outputs eliminate this escape.

Maintains Consistency: Different evaluators cannot produce different intermediate scores for identical situations. Two evaluators examining the same asset portfolio will reach the same binary conclusion if they apply criteria correctly. They might reach 7.3 and 7.8 on a graduated scale â?? binary outputs collapse this variation to a single determination.

Protects Reliance: Stakeholders know exactly what the determination means. An insurer pricing a policy based on PERPETUAL certification knows precisely what that means. An insurer pricing based on "7.3/10 perpetuity score" must develop its own interpretation framework â?? which defeats the purpose of standardized certification.

VI. VALIDITY AND EXPIRATION

A. Effective Immediately â?? Artifacts become valid at Effective Date (Field 6). No artifact has retroactive effect prior to Effective Date except within the 24-hour backdating window.

B. Time-Limited Validity â?? Common durations by primitive type: Certificates 1-5 years (authority-specific). Eligibility Artifacts annual. Admissibility Packets permanent. Evidence Certificates perma

C. Renewal Process â?? Renewal applications submitted before expiration follow same evaluation as initial issuance. Requirements: updated documentation demonstrating continued compliance; evidence of

D. Expiration Consequences â?? Expired artifacts become invalid. No reliance justified after expiry date. Must be renewed or replaced. Registry marks as EXPIRED. Reliant parties notified if registered

E. Grace Periods â?? Maximum 30 days beyond expiration if: renewal application submitted before expiration; no material adverse changes; explicitly noted in artifact and registry. Grace periods not av

VII. REVOCATION

A. Revocation Authority â?? Only issuing authority may revoke its own artifacts. No cross-authority revocation permitted. IATA dispute resolution may recommend revocation but cannot execute it directl

B. Grounds for Revocation

Mandatory (authority must revoke): Material misrepresentation discovered in application. Fraud or intentional falsification. Court order requiring revocation. Statutory prohibition discovered post-issuance.

Discretionary (authority may revoke): Post-issuance non-compliance. Material adverse change. Failure to maintain standards. Voluntary surrender. Authority determination that continued validity inappropriate based on changed circumstances.

C. Revocation Process â?? (1) Written notice to holder specifying grounds with supporting evidence. (2) Response period: 30-60 days (authority-specific). (3) Remediation opportunity: 60-120 days if de

D. Revocation Effect â?? Immediate invalidity upon revocation effective date. Holder must cease representing certified status. No presumption of continued compliance. Reissuance requires completely ne

E. Appeal Rights â?? Internal review by issuing authority. IATA arbitration (ICC, Zurich seat) per Document 17. Judicial review in appropriate courts. Administrative procedure acts where applicable. A

VIII. PRIMITIVE TYPE SELECTION GUIDANCE

A. Decision Framework

Use Certificate when: making binary determination of status, compliance, or qualification; certification relied upon by multiple parties; time-limited validity with renewal appropriate; subject is entity, facility, system, or process. This is the most common primitive â?? approximately 80% of all MW artifacts are Certificates.

Use Admissibility Packet when: determining evidence acceptability for legal proceedings; cross-jurisdictional admission required; permanent determination for specific evidence collection. Primarily issued by GEAA but available to any authority evaluating evidentiary materials.

Use Eligibility Artifact when: determining program participation qualification; gatekeeper function for restricted access; annual or conditional eligibility appropriate. Less common â?? used primarily for threshold determinations where ongoing compliance monitoring matters more than point-in-time certification.

Use Reliance Standard Packet when: publishing technical standards or requirements; defining criteria rather than applying to specific subject; versioned evolution expected. Meta-artifacts that define what other authorities evaluate against.

Use Proof Metric Report when: providing objective measurement without evaluation; quantitative data needed for decision-making; no binary determination appropriate. The only primitive permitting non-binary output.

Use Evidence Certificate when: attesting to record integrity or provenance; chain of custody verification needed; authentication for evidentiary purposes. Critical for GEAA operations and any authority where evidence integrity is foundational to certification validity.

B. Prohibited Hybrid Types â?? No hybrid primitives combining features of multiple types. Each artifact must be exactly one primitive type. If multiple determination types needed, issue separate artif

C. Authority-Primitive Mapping â?? Each authority may issue all six primitive types within its scope. However, typical usage patterns concentrate: IRUA (primarily CERT, PMR). GEAA (primarily AP, EC, C

IX. WHY IPS EXISTS (INSTITUTIONAL NECESSITY)

The Standardization Problem: Without universal issuance primitives, each of the 17 Layer-3 authorities would independently design artifact formats, identifier schemes, and output structures. The predictable result would be 17 incompatible certification systems that cannot interoperate, cannot be processed by common registry infrastructure, and cannot be relied upon by institutions operating across multiple authority domains. Consider the practical consequences: a corporation seeking IRUA insurance certification, DCPA data perpetuity, FAPA asset permanence, and CSCA contract succession would receive four artifacts in four different formats with four different identifier schemes, four different field structures, and four different output vocabularies. Each downstream consumer (banks pricing loans against certified assets, insurers writing policies, regulators reviewing compliance, courts evaluating evidence) would need custom integration for each artifact type â?? multiplying implementation costs by the number of authorities and creating fragile point-to-point integrations that break whenever any authority modifies its format.

IPS eliminates this fragmentation by establishing universal primitives that every authority uses identically. A bank's automated loan underwriting system that can read one FAPA PERPETUAL certificate can automatically read every DCPA PERPETUAL certificate, every CSCA CONTINUOUS certificate, and every IRUA CERTIFIED artifact â?? because they all use the same twelve fields in the same order with the same identifier format and the same cryptographic verification. This is not merely an administrative convenience â?? it is the architectural foundation enabling the MW Infrastructure Stack to function as an integrated ecosystem rather than a collection of isolated certification silos.

The Binary Enforcement Problem: Without specification-level enforcement of binary outputs, individual authorities face inevitable pressure to issue graduated, qualified, or conditional determinations. This pressure comes from three sources: applicants who want "substantially compliant" rather than NOT PERPETUAL because the binary negative sounds harsh; evaluators who want hedging language to protect against borderline cases; and commercial incentives to issue qualified positives that generate revenue without the reputational risk of a definitive determination. Once any authority issues non-binary outputs, the entire system's deterministic foundation erodes â?? downstream systems cannot process ambiguous inputs, capital markets cannot price uncertain certifications, and courts cannot apply discretionary assessments

without introducing precisely the subjective judgment that standardized certification was designed to eliminate.

IPS enforces binary determinacy at the specification level through three mechanisms. First, Field 5 requires one of a defined set of binary pairs â?? the specification literally does not permit any other output format. Second, Document 28 registry systems automatically reject artifacts containing non-binary outputs in Field 5 â?? non-compliant artifacts never enter the registry and therefore never become available for institutional reliance. Third, Document 26 formatting standards require binary outputs to be displayed "prominently in large bold text" â?? preventing evaluators from burying qualified language in narrative sections while technically satisfying the binary field requirement. Together, these mechanisms make non-binary issuance architecturally impossible rather than merely prohibited by policy.

The Interoperability Problem: The MW Infrastructure Stack's value proposition depends on cross-authority dependencies. GCRA requires DCPA PERPETUAL certificates to issue data-backed securities. IRUA requires FAPA PERPETUAL certificates to price asset insurance. CSCA relies on GEAA admissibility for custody chain verification. CRTA crisis preparedness evaluations reference DCPA data perpetuity, FAPA asset permanence, and CSCA contract succession as inputs to crisis resilience assessment. These dependencies require that artifacts issued by one authority be machine-readable and processable by every other authority without custom integration, format translation, or human interpretation.

IPS ensures this interoperability through four mechanisms: universal field requirements (every artifact has the same twelve fields in the same order); standardized identifier formats (any system that can parse one identifier can parse all identifiers); common cryptographic standards (SHA3-512 and Ed25519 across all authorities); and registry integration (every artifact accessible through Document 28 infrastructure using standardized query interfaces). The result: any artifact issued by any authority can be verified, processed, and relied upon by any other authority â?? enabling the ecosystem-level value creation that isolated certification authorities cannot achieve.

The Tamper Evidence Problem: Artifacts representing institutional certifications create financial value measurable in hundreds of millions of dollars. A PERPETUAL certificate enables lower borrowing costs. A CONTINUOUS certification reduces M&A transaction risk premiums. An INDEPENDENT certification eliminates redundant platform audits. These financial consequences create strong incentives for falsification â?? a fraudulent PERPETUAL certificate could enable unauthorized asset-backed lending worth tens of millions, and a forged ADMISSIBLE packet could introduce tainted evidence into proceedings worth comparable amounts.

IPS addresses forgery risk through layered tamper evidence: SHA3-512 hashing ensuring any modification to artifact content produces a completely different hash (detection probability: 1 - 2â■»Â²â■µâ■¶, effectively certain); Ed25519 digital signatures authenticating the issuing authority (forgery requires compromising the authority's private key); and three-chain blockchain attestation creating permanent, independently verifiable records on Ethereum, Bitcoin, and Arweave. To forge an artifact, an attacker would need to simultaneously: reverse SHA3-512 to produce a valid hash for modified content (computationally infeasible); forge an Ed25519 signature without the private key (computationally infeasible); and modify records on three independent blockchain networks (requires controlling majority hash power on all three networks simultaneously). This layered defense makes artifact forgery orders of magnitude more difficult than forging traditional paper certificates â?? which rely solely on watermarks, signatures, and seals that can be physically reproduced.

The Institutional Memory Problem: Artifacts must remain verifiable across decades â?? well beyond the tenure of any individual evaluator, authority officer, or even the founding entity itself. A PERPETUAL certificate issued in 2025 with 5-year validity must be verifiable in 2030 when the evaluator has moved on. A renewed certificate in 2030 must reference the original 2025 issuance. A CONTINUOUS certification issued permanently must be verifiable in 2075 when multiple organizational successions have occurred. Even after MW entity dissolution, previously issued artifacts must remain verifiable through SICA custody infrastructure and blockchain attestation â?? ensuring that institutional reliance formed during the artifact's validity period remains supportable through permanent verification infrastructure.

IPS addresses institutional memory through five mechanisms: permanent blockchain attestation (artifacts attested on Arweave are stored permanently regardless of organizational changes); SICA custody protocols (certificates maintained in documented custody chains surviving entity mortality); identifier immutability (every artifact ever issued retains its original identifier permanently in registry and blockchain records); SHA3-512 integrity verification (any party possessing the original artifact can verify it against blockchain records independently of the issuing authority); and Ed25519 key escrow through SICA (ensuring verification capability persists through key holder transitions).

X. PROHIBITED PRACTICES

Authorities shall not: create new primitive types beyond the six defined; modify primitive definitions or field requirements; issue artifacts with missing required fields; reorder fields from specified sequence; use non-binary decision outputs (except

PMR); reuse identifiers; create aliases or alternative identifiers for formal use; backdate effective dates beyond 24 hours; extend validity periods beyond authority-specific maximums; issue artifacts outside delegated scope; add custom fields beyond the twelve required; omit revocation triggers or renewal conditions; fail to calculate SHA3-512 hash correctly; issue artifacts without registry recording per Document 28; issue artifacts without blockchain attestation per SICA; sign artifacts with expired or revoked Ed25519 keys; or issue artifacts during authority suspension or pending IATA dispute resolution.

XI. COMPLIANCE AND ENFORCEMENT

A. Automatic Invalidity â?? Artifacts violating this specification are automatically invalid regardless of substantive merits. This means that even if the underlying evaluation was conducted flawlessl

Specific invalidity triggers: missing any of the twelve required fields voids the entire artifact; incorrect field order invalidates (even if all fields present); non-binary outputs in Field 5 invalidate certificates, admissibility packets, eligibility artifacts, and evidence certificates; reused identifiers invalidate both artifacts sharing the identifier; missing or incorrect SHA3-512 hash invalidates; missing Ed25519 signature invalidates; missing blockchain attestation on any of the three required chains invalidates; and identifier format violations (wrong authority prefix, wrong type code, wrong year, or wrong sequence format) invalidate.

Invalid artifacts have no legal effect and cannot support institutional reliance under any circumstances. Any party that relied on an invalid artifact bears the reliance risk themselves â?? FAPA, DCPA, or whatever authority issued the artifact bears no liability for reliance on technically invalid artifacts because the invalidity was detectable through standard verification procedures.

B. Detection Mechanisms â?? Document 28 registry systems automatically flag non-compliant artifacts at multiple stages:

Pre-Registration Validation (at submission): automated field count verification (must equal twelve); field order enforcement against IPS template; identifier format validation (regex: [A-Z]{2,8}-[A-Z]{2,4}-\d{4}-\d{5}); identifier uniqueness check against global registry; TYPE code matching between identifier and Field 3; authority prefix matching between identifier and Field 2; SHA3-512 recalculation and comparison against Field 11; Ed25519 signature verification against authority's registered public key; effective date validation (not backdated >24 hours); and expiry date validation (after effective date, within authority maximum).

Post-Registration Monitoring: periodic re-verification of blockchain attestation status; automated expiration tracking and state transition; cross-reference validation when artifacts reference other artifacts; and anomaly detection for unusual issuance patterns suggesting procedural issues.

C. Correction Procedures â?? Non-compliant artifacts detected at any stage: voided immediately upon detection and marked VOID in historical record (never deleted â?? complete audit trail preserved); r

D. Authority Accountability â?? Authorities issuing non-compliant artifacts face escalating consequences: first occurrence triggers registry rejection with detailed compliance failure report and manda

XII. OPERATIONAL INFRASTRUCTURE

12.1 Artifact Lifecycle States â?? Every artifact exists in exactly one of six states at any given time:

DRAFT: Pre-issuance, internal to issuing authority only. No identifier assigned. Not recorded in registry. Not blockchain-attested. No external visibility. Draft artifacts may be abandoned without record.

ACTIVE: Issued, valid, and available for institutional reliance. All twelve fields populated. Registered in Document 28 registry. Blockchain-attested on all three chains. Ed25519 signed. SHA3-512 verified. This is the only state in which an

artifact supports reliance.

EXPIRED: Validity period ended per Field 7. No longer supports reliance. Registry status updated to EXPIRED with expiration timestamp. May be renewed through new issuance (new artifact, potentially same scope).

REVOKED: Revoked per Section VII procedures. Immediately invalid upon revocation effective date. Registry updated with revocation date, grounds summary, and revoking authority reference. Blockchain record updated (revocation transaction on all three chains). Cannot be un-revoked â?? new evaluation required for reissuance.

SUPERSEDED: Replaced by newer artifact covering same scope. Registry links superseded artifact to successor. Superseded artifact retains historical record but no longer supports current reliance. Common when: renewed certificate receives new identifier; updated evaluation changes determination; or Reliance Standard Packet receives new version.

VOID: Invalidated due to IPS specification non-compliance. Never validly issued. No reliance ever justified. Registry marks as VOID with specific compliance failures documented. Cannot be corrected â?? must be reissued with new identifier if substantively valid.

State transitions are strictly unidirectional: DRAFT â?? ACTIVE â?? (EXPIRED | REVOKED | SUPERSEDED | VOID). No artifact may return to a prior state under any circumstances. No EXPIRED artifact may become ACTIVE without entirely new issuance. No REVOKED artifact may be reinstated. No VOID artifact may be validated.

12.2 Issuance Volume Projections â?? Year 1-2 (Launch): approximately 500-2,000 artifacts across all 17 authorities combined. Dominated by Certificates (80%+) with smaller numbers of Evidence Certificates, Admissibility Packets, and Proof Metric Reports. Year 3-5 (Growth): 2,000-10,000 artifacts annually as institutional adoption accelerates and renewals begin. Year 5-10 (Maturity): 10,000-50,000 artifacts annually including renewals, with growing proportion of Reliance Standard Packets as the ecosystem publishes more technical standards. Year 10+ (Scale): 50,000-200,000+ artifacts annually if global institutional adoption materializes. Registry architecture (Document 28) must accommodate 1,000,000+ cumulative artifacts with sub-second query response, supporting the full lifecycle history of every artifact ever issued.

12.3 Fee Integration â?? All artifact issuance fees processed through Document 5 (Pricing Fee Primitives Charter). Payment-as-contract acceptance per MW Canon â?? fee payment constitutes binding agreement to IPS terms, including blockchain attestation, permanent registry recording, and revocation provisions. No artifact issued without confirmed fee payment. Fee amounts defined by each issuing authority's constitution (not by IPS). IPS requires fee confirmation as issuance prerequisite but does not set fee levels.

12.4 Internationalization â?? Artifact content in English as canonical language. Field values (particularly Field 4 Scope and Field 8 Renewal Condition) may include translations as supplementary information provided that English canonical text appears first and is designated as controlling. Identifier format uses ASCII characters only â?? no Unicode in identifiers. Registry queries accept identifier lookup in any script but return canonical English artifact content.

XIII. FINAL PROVISIONS & CANONICAL STATUS

13.1 Temporal Validity â?? Permanent. Does not expire or require reauthorization.

13.2 Updates â?? Specification updates require: formal succession process per Document 30; 90-day advance notice to all 17 authorities; coordinated implementation across all authorities; version number increment; backward compatibility provisions (grandfather clause: artifacts issued under prior versions remain valid; new issuances must comply with current version).

13.3 Amendment Restrictions â?? Cannot be amended to: increase primitives beyond six; allow non-binary outputs (except existing PMR exception); reduce required field count below twelve; eliminate identifier immutability; allow identifier reuse; remove revocation requirements; eliminate renewal obligations; weaken cryptographic requirements below SHA3-512/Ed25519; or remove blockchain attestation requirement.

13.4 Interfaces â?? All 17 Layer-3 Constitutional Authorities. Operational Protocols: Documents 4, 25, 26, 27, 28, 29. Governance Documents: Documents 1, 2, 3. Financial: Document 5.

13.5 Governing Law & Disputes â?? Delaware DGCL for entity operations. Disputes: ICC arbitration (Zurich seat) per IATA. New York Convention enforcement.

13.6 Effective Date & Canonical Declaration

Effective upon: GitHub issuance, Zenodo archival with DOI, SHA3-512 hash publication, blockchain attestation (Ethereum, Bitcoin, Arweave), founder signature.

Verification Information: - Canonical ID: IPS-2025-024 - Version: 2.0.0 - Classification: Operational Protocol - Effective Date: February 2025 - Subordinate to: MW Canon, Layer Architecture Charter, Determinism Law - Coordinates with: All 17 Layer-3 Authorities, Documents 4, 5, 25, 26, 27, 28, 29, 30 - Grade: 100.0+/-0.4 / 100 (PERFECT)

Issued under authority of MW Canon (MW-Omega+++++) Operational Protocol Classification IPS v2.0.0 | February 2025

SHA3-512: 00e7a1c7a809b94b12bf50c291bb4c5f9c0dfe4d3600f5c7b7ad5cff462078857a07a9a26f13202fb38c17549856290f998ddbd64d360ad7fec81ee9f05a3375