Artifact Formatting, ID & Hashing Standard (AFIHS)

DOCUMENT 26: ARTIFACT FORMATTING, ID & HASHING STANDARD (AFIHS) v2.0

Canonical Document ID: AFIHS-2025-026 Version: 2.0.0 Effective Date: February 2025 Word Count: ~5,312 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 standard establishes universal formatting requirements, identifier structure, and cryptographic hashing specifications for all artifacts issued by Layer-3 Constitutional Authorities. Standardization ensures consistency, verifiability, tamper detection, and interoperability across the entire MW Infrastructure Stack. Every artifact issued must conform to these specifications without exception or variation.

This standard governs: identifier format and assignment; mandatory field requirements and ordering; file format specifications; cryptographic hash generation and verification; metadata structure; timestamp standards; digital signature protocols; version control methodology; and blockchain attestation requirements.

This standard does not: define authority-specific eligibility criteria; establish substantive requirements for certification; create new authorities or primitives; or determine when artifacts should be issued.

1.1 Relationship to MW Canon & Coordinate Documents

MW Canon Subordination: AFIHS implements the "tamper-evident" and "machine-readable" requirements of MW Canon by specifying exact formatting, hashing, and signature standards. Every artifact across the entire stack conforms to one standard â?? this one.

Document 24 (IPS): Defines the six primitive types and twelve mandatory fields. AFIHS specifies how those fields are formatted, rendered, encoded, and hashed. IPS defines what exists; AFIHS defines how it looks, computes, and verifies.

Document 25 (BDTM): Produces binary decision outputs. AFIHS specifies how those outputs appear in Field 5 â?? prominently displayed in the artifact, machine-parseable, and unambiguous.

Document 27 (CCOCP): Governs artifact custody after issuance. AFIHS defines the artifact format that custodians maintain. Custody integrity requires format integrity â?? a corrupted artifact cannot be reliably custodied.

Document 28 (RAS): Defines registry infrastructure. AFIHS defines the artifact format that registries index, store, and serve. Registry queries return AFIHS-compliant artifacts.

SICA Integration: All artifacts follow SICA custody protocols. Digital signatures use Ed25519. Hashes use SHA3-512. Blockchain attestation on three chains (Ethereum, Bitcoin, Arweave) per SICA requirements.

1.2 Cryptographic Standards Summary

Hashing: SHA3-512 (NIST FIPS 202) â?? mandatory for all artifacts. 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. Output: 128-character hexadecimal string (lowercase).

Digital Signatures: Ed25519 (FIPS 186-5) â?? mandatory for all artifacts (upgraded from optional in v1.0). Every artifact must be digitally signed by the issuing authority.

Blockchain Attestation: Three-chain attestation (Ethereum, Bitcoin, Arweave) â?? mandatory for all artifacts. Hash published on all three chains within 24 hours of issuance.

Post-Quantum Readiness: SHA3-512 inherently quantum-resistant. Ed25519 will migrate to ML-DSA (CRYSTALS-Dilithium) when NIST PQC standards finalize. Additive migration: PQC signatures added alongside Ed25519 during transition, not replacing until 90%+ ecosystem adoption.

Legal Framework: UETA and E-SIGN (U.S. electronic signature recognition). eIDAS (EU electronic identification). New York Convention (international enforcement). Federal Arbitration Act. Disputes: ICC arbitration (Zurich seat) per IATA.

II. IDENTIFIER FORMAT (IMMUTABLE)

A. Universal Structure

All artifact identifiers follow this exact format:

[AUTHORITY]-[PRIMITIVE]-[YEAR]-[SEQUENCE]

Components:

AUTHORITY (2-8 characters): IRUA, GEAA, CIVICHAB, GCPA, PMOA, EWA, EPA, EFAA, UPDIUD, SICA, IATA, DRFA, CRTA, IPPA, CSCA, DCPA, FAPA.

PRIMITIVE (2-4 characters): CERT (Certificate), AP (Admissibility Packet), EA (Eligibility Artifact), RSP (Reliance Standard Packet), PMR (Proof Metric Report), EC (Evidence Certificate).

YEAR (4 digits): Calendar year of issuance. UTC timezone for year boundary determination.

SEQUENCE (5 digits, zero-padded): Sequential within authority-primitive-year namespace. 00001 through 99999. Resets each calendar year. If capacity exceeded (extremely unlikely â?? 99,999 per authority per type per year), six-digit extension authorized.

Validation Regex: ^[A-Z]{2,8}-(?:CERT|AP|EA|RSP|PMR|EC)-\d{4}-\d{5,6}$

B. Examples

IRUA-CERT-2025-00001 (first IRUA certificate of 2025) GEAA-AP-2025-00123 (GEAA admissibility packet) CSCA-CERT-2026-04567 (CSCA certificate issued in 2026) DCPA-CERT-2025-00789 (DCPA data custody certificate) FAPA-CERT-2026-01234 (FAPA asset perpetuity certificate) IPPA-EC-2025-00045 (IPPA evidence certificate) GCPA-RSP-2025-00012 (GCPA reliance standard packet) PMOA-PMR-2025-00301 (PMOA proof metric report)

C. Assignment Rules

Immutability: Assigned at issuance only. Never changed after assignment. Amendments, corrections, and renewals require new identifiers. Original identifier permanently retired (never reused under any circumstances).

Non-Reuse: Never reused even if artifact revoked, voided, expired, or superseded. Global uniqueness across all time. Retired identifiers remain in registry as historical records.

Sequential Allocation: Assigned sequentially within namespace. Gaps permitted and expected (voided artifacts). No requirement for continuous sequence. Automated assignment systems enforce sequentiality and prevent collision.

No Aliases: No alternative identifiers, nicknames, shortened versions, or informal references permitted in formal contexts. All formal references must use canonical identifier. Informal references in non-binding communications may use abbreviated forms provided canonical identifier appears at least once in the document.

D. Namespace Isolation

Each authority-primitive-year combination constitutes an isolated namespace: IRUA-CERT-2025-##### (up to 99,999 certificates per year); IRUA-AP-2025-##### (separate namespace); IRUA-CERT-2026-##### (new year, resets). Namespaces cannot conflict or collide. Total theoretical capacity across all 17 authorities, 6 primitive types, and annual reset: 17 Ã? 6 Ã? 99,999 = 10,199,898 artifacts per year â?? far exceeding projected demand.

III. MANDATORY FIELD REQUIREMENTS

Every artifact must contain twelve fields in exact order per Document 24 (IPS). AFIHS specifies rendering requirements:

Field 1: Identifier â?? Per Section II format. Rendered in header, monospace font, minimum 12pt. Machine-readable (parseable by regex without human intervention).

Field 2: Issuing Authority â?? Full authority name with abbreviation. Example: "Institutional Reliance & Usage Authority (IRUA)." Rendered below identifier.

Field 3: Primitive Type â?? Full primitive name. Must match TYPE code in identifier.

Field 4: Scope â?? Detailed coverage description. Minimum 50 words. Must precisely define boundaries, subject, geographic scope, exclusions, and supporting documentation references. Rendered in body text, standard font.

Field 5: Decision Output â?? Binary determination prominently displayed. Rendering requirement: minimum 18pt bold font, centered, visually dominant on artifact. Must be the most prominent text element on the artifact â?? a reader scanning the document should identify the determination within 2 seconds. Color coding recommended: positive (green or dark text), negative (red or contrasting text).

Field 6: Effective Date â?? ISO 8601 UTC: YYYY-MM-DDTHH:MM:SSZ. Cannot be backdated more than 24 hours. UTC timezone mandatory (Z suffix). No local timezones, timezone offsets, or ambiguous formats permitted.

Field 7: Expiry Date â?? ISO 8601 UTC or "NONE" for permanent artifacts. Must be after effective date. Must align with authority-specific maximum durations per IPS.

Field 8: Renewal Condition â?? Structured statement. Must include: deadline, documentation requirements, evaluation timeline, fee reference. "NOT APPLICABLE â?? PERMANENT ARTIFACT" for non-expiring types.

Field 9: Revocation Triggers â?? Enumerated list. Minimum: material misrepresentation, post-issuance non-compliance, material adverse change, voluntary surrender, authority invalidity determination. Authority-specific triggers added per constitution.

Field 10: Custody Holder â?? Full legal entity name, jurisdiction of organization, registered address, authorized representative. Custody transfers documented per Document 27.

Field 11: Cryptographic Hash â?? SHA3-512 hash of complete artifact content (excluding Field 11 itself, digital signature, and mutable post-issuance metadata). 128-character lowercase hexadecimal string. Calculated after all other fields populated.

Field 12: Registry Reference â?? Canonical URL per Document 28. Enables public verification. Includes registry timestamp.

Field Ordering: Fields 1-12 must appear in specified order. Reordered, missing, or additional fields render artifact invalid regardless of substantive correctness. Automated validation at Document 28 registry enforces ordering.

IV. CRYPTOGRAPHIC HASH SPECIFICATION

A. Algorithm: SHA3-512 (Mandatory)

SHA3-512 (NIST FIPS 202, Keccak-based) is mandatory for all artifacts. SHA-256 accepted for backward compatibility with v1.0 artifacts only â?? all new artifacts must use SHA3-512. SHA-1 and MD5 are prohibited under all circumstances.

SHA3-512 properties: 512-bit output (128 hex characters). 256-bit collision resistance. Post-quantum security (Keccak sponge construction resistant to known quantum attacks). No length-extension vulnerability (unlike SHA-256). NIST standardized with broad library support.

B. Hash Calculation Process

Step 1 â?? Content Assembly: Compile complete artifact content including all twelve fields, full text, all embedded data and metadata.

Step 2 â?? Exclusions: Exclude Field 11 (hash itself), Ed25519 digital signature (added post-hash), registry timestamps (added post-issuance), blockchain attestation references (added post-issuance), and any mutable metadata added after finalization.

Step 3 â?? Normalization: UTF-8 encoding. Consistent whitespace (spaces, not tabs). Unix line endings (\n not \r\n). No trailing whitespace on any line. No byte-order mark (BOM). Normalization ensures identical content produces identical hash regardless of platform or text editor used.

Step 4 â?? Calculation: hash = SHA3-512(normalized_artifact_content)

Step 5 â?? Encoding: Lowercase hexadecimal (a-f, 0-9). Exactly 128 characters. No spaces, dashes, or grouping.

Step 6 â?? Insertion: Insert into Field 11. Finalize artifact. Any subsequent modification invalidates hash.

C. Hash Verification

Recipients verify artifact authenticity through: (1) Obtain artifact from any source. (2) Extract Field 11 (published hash). (3) Compute SHA3-512 of artifact content (applying same exclusions and normalization). (4) Compare computed hash to published hash. Match = authentic, untampered. Mismatch = tampered, corrupted, or invalid.

Command-line verification:

Python (hashlib) import hashlib with open('artifact.txt', 'rb') as f: h = hashlib.sha3_512(f.read()).hexdigest() print(h)

OpenSSL openssl dgst -sha3-512 artifact.txt

Any single-character modification produces a completely different hash â?? the avalanche property of SHA3-512 ensures that even minimal tampering is detectable.

D. Blockchain Attestation

Within 24 hours of artifact issuance, the SHA3-512 hash must be attested on all three chains. This three-chain requirement is non-negotiable â?? artifacts attested on fewer than three chains are non-compliant regardless of other specification compliance.

Ethereum Attestation: Smart contract deployed at a fixed, published address (MW Artifact Registry contract). Each attestation emits an indexed event containing: artifact identifier (bytes32), SHA3-512 hash (bytes64), issuing authority code (bytes8), primitive type code (bytes4), effective date (uint256 Unix timestamp), and expiry date (uint256 Unix timestamp or 0 for permanent). Event indexing enables efficient lookup by artifact identifier. Gas costs borne by issuing authority's operational budget. Verification procedure: query contract event log filtered by artifact identifier â?? returns attestation data including block number and timestamp providing independent proof of attestation timing. Ethereum provides the richest queryable attestation due to smart contract event indexing, making it the primary verification chain for automated systems.

Bitcoin Attestation: OP_RETURN transaction containing artifact identifier and hash prefix (truncated to fit 80-byte OP_RETURN limit). Full data structure: 4 bytes magic prefix (0x4D57), 20 bytes artifact identifier (compressed), 32 bytes SHA3-512 hash prefix, 24 bytes reserved. Transaction funded from dedicated MW attestation wallet. Transaction ID recorded in artifact metadata. Verification: decode OP_RETURN data from transaction, verify magic prefix, decompress identifier, compare hash prefix to full SHA3-512. Bitcoin provides the highest-security attestation due to Bitcoin's proof-of-work security model and 15+ year operational history, making it the most tamper-resistant chain for long-term verification.

Arweave Attestation: Permanent storage of complete artifact metadata package (JSON format containing all twelve field values, SHA3-512 hash, Ed25519 signature, and issuing authority public key fingerprint). Tagged with artifact identifier for gateway query. Arweave's permanent storage model (pay once, store forever) ensures metadata availability in perpetuity without ongoing hosting costs. Transaction ID recorded in artifact metadata. Verification: query Arweave gateway by artifact identifier tag, retrieve complete metadata, verify hash and signature. Arweave provides the most complete attestation â?? storing full metadata rather than just hash â?? making it the primary archival chain for long-term preservation.

Three-chain attestation ensures: no single blockchain's compromise invalidates verification capability; artifacts verifiable through any of three independent networks with different consensus mechanisms (Ethereum proof-of-stake, Bitcoin proof-of-work, Arweave proof-of-access); permanent storage on Arweave survives even if Ethereum or Bitcoin experience temporary unavailability; and layered redundancy defends against chain-specific governance changes, hard forks, or technical failures.

Attestation Failure Handling: If any chain is temporarily unavailable at issuance time, the artifact may be issued with a notation that attestation is pending on the unavailable chain. Pending attestation must be completed within 72 hours of chain availability restoration. If attestation cannot be completed on all three chains within 30 days, the artifact must be re-evaluated for compliance.

E. Hash Publication and Verification Infrastructure

Registry Recording: Every artifact hash recorded in Document 28 registry within 24 hours of issuance. Publicly accessible via RESTful API. Searchable by artifact identifier, authority, type, date range, or status. Preserved permanently in append-only ledger.

Public Verification API Response Format:

{ "artifact_id": "IRUA-CERT-2025-00123", "published_hash": "a7f3c9d1e5b2f8a4...[128 chars]", "hash_algorithm": "SHA3-512", "signature_algorithm": "Ed25519", "signature_valid": true, "blockchain_attestations": { "ethereum": {"tx_hash": "0x...", "block": 12345678, "confirmed": true}, "bitcoin": {"tx_hash": "...", "block": 890123, "confirmed": true}, "arweave": {"tx_id": "...", "confirmed": true} }, "status": "ACTIVE", "effective_date": "2025-01-30T14:23:17Z", "expiry_date": "2030-01-30T14:23:17Z", "verification_timestamp": "2025-02-01T10:00:00Z" }

Bulk Verification: API supports batch verification of up to 100 artifacts per request for institutional consumers processing multiple certificates. Response includes per-artifact verification status.

Offline Verification: For environments without internet access, artifacts can be verified by: extracting the SHA3-512 hash and Ed25519 signature from the artifact; recomputing the hash locally; verifying the signature against the authority's published public key (which can be pre-downloaded); and confirming the hash prefix against a locally cached copy of Bitcoin OP_RETURN attestations. Full offline verification requires pre-cached public keys and blockchain attestation data.

V. FILE FORMAT SPECIFICATIONS

A. Primary Format: PDF/A

Preferred: PDF/A-2b (ISO 19005-2, archival compliance). Requirements: human-readable text (not scanned images); searchable content (text layer present); embedded fonts (no system font dependencies â?? standard fonts: Times New Roman, Arial, Courier, or Liberation equivalents); no external dependencies; no JavaScript or embedded executables; no DRM or access restrictions; no password protection; maximum 5MB per artifact.

Accessibility: proper document structure (headings, paragraphs); tagged PDF for screen reader compatibility; alternative text for images; logical reading order; bookmarks for navigation; high contrast. Non-compliance with accessibility does not invalidate artifact but is strongly discouraged.

B. Alternative Formats (Machine-Readable)

JSON (UTF-8): Structured data representation enabling automated processing. Schema published per this standard. All twelve fields as named key-value pairs. Example structure:

{ "identifier": "IRUA-CERT-2025-00001", "issuing_authority": "Institutional Reliance & Usage Authority (IRUA)", "primitive_type": "Certificate", "scope": "...", "decision_output": "IRREVERSIBLE", "effective_date": "2025-01-30T14:23:17Z", "expiry_date": "2030-01-30T14:23:17Z", "renewal_condition": "...", "revocation_triggers": ["..."], "custody_holder": "...", "hash": "a7f3c9d1...", "registry_reference": "https://..." }

XML (UTF-8 with XSD schema): For systems requiring XML interchange. Schema published alongside this standard. Namespace: urn:mw:afihs:v2.

Plain Text (UTF-8): Unix line endings (\n). No control characters except newline and tab. Fields separated by labeled headers.

All formats must be: human-readable where feasible; machine-parseable without proprietary tools; based on open, publicly available specifications; and suitable for long-term archival (minimum 50-year readability).

C. Prohibited Formats â?? Proprietary word processor formats (DOC, DOCX). Spreadsheet formats (XLS, XLSX). Proprietary PDF features (forms, JavaScript, 3D content). Encrypted or DRM-protected formats.

VI. METADATA STRUCTURE

A. Required Metadata Header (all artifacts):

Artifact ID: [identifier per Section II] Issuing Authority: [full authority name] Issuance Date: [ISO 8601 UTC] Document Version: [semantic version of artifact] Specification Version: AFIHS v2.0.0 Format: [PDF/A-2b | JSON | XML | TXT] Hash Algorithm: SHA3-512 Hash: [128-character hex] Signature Algorithm: Ed25519 Signature: [Base64-encoded Ed25519 signature] Blockchain Attestation: [ETH tx hash] | [BTC tx hash] | [AR tx hash]

B. Optional Metadata: Author (authority office). Subject (brief description). Keywords (classification tags). Language (en-US default). Supersedes (prior artifact identifier). Related Artifacts (cross

C. Encoding: UTF-8 universal. ISO 8601 for all dates/times. UTC mandatory. Semantic versioning (MAJOR.MINOR.PATCH). Currency codes per ISO 4217. Country codes per ISO 3166-1.

VII. DIGITAL SIGNATURE PROTOCOL (MANDATORY)

A. Requirement

Digital signatures are mandatory for all artifacts (upgraded from optional in v1.0). Every artifact must be signed by the issuing authority using Ed25519.

B. Algorithm: Ed25519 (Mandatory)

Ed25519 (FIPS 186-5) â?? deterministic, fast, small signatures (64 bytes), small keys (32 bytes public). Provides 128-bit security level. Well-supported across all major cryptographic libraries.

Prohibited: RSA below 3072-bit. DSA (deprecated). Any algorithm with known vulnerabilities. ECDSA with curves below P-256 (Ed25519 preferred over all ECDSA variants for new artifacts).

C. Signature Process

Step 1 â?? Hash: Calculate SHA3-512 hash per Section IV. Step 2 â?? Sign: signature = Ed25519_Sign(hash, authority_private_key). Step 3 â?? Attach: Embed signature in artifact metadata as Base64-encoded value. Include: signature algorithm identifier ("Ed25519"), authority public key fingerprint (SHA3-256 of public key), signature value, and signing timestamp. Step 4 â?? Verification: Ed25519_Verify(hash, signature, authority_public_key) â?? valid/invalid.

D. Key Management

Private Keys: Stored in hardware security module (HSM) meeting FIPS 140-2 Level 3 minimum (Level 4 recommended for authorities issuing high-value certifications exceeding $100K individual value). HSM must be physically secured with restricted access, environmental monitoring, and tamper-evident enclosure. Private keys never exported or transmitted in plaintext under any circumstances. Protected by multi-party authentication requiring minimum 2-of-3 authorized signers for any signing operation â?? no single individual can sign an artifact unilaterally. Key material backed up to secondary HSM in geographically separate facility for disaster recovery. Keys rotated annually on fixed schedule: new key pair generated 90 days before rotation date; new key becomes active on rotation date; old key remains valid for verification of previously signed artifacts but cannot be used for new signatures after rotation; key history maintained permanently in SICA registry for long-term verification of historical artifacts.

Public Keys: Published in each authority's public key registry immediately upon generation. Distributed via SICA key infrastructure with multiple distribution channels (HTTPS, DNS-based, and registry API). Archived permanently â?? no public key ever deleted, ensuring verification of artifacts signed with any historical key. Key fingerprints (SHA3-256 of public key bytes) published alongside each artifact and in authority's key registry, enabling efficient key lookup without downloading full public key.

Key Escrow: SICA holds backup copies of all authority key pairs in dedicated escrow HSM infrastructure. Escrow activation triggers: authority fails to sign artifacts for 90 consecutive days (dead man's switch); authority formally requests escrow activation; IATA orders escrow activation following dispute resolution; or authority dissolution triggers automatic escrow activation per Document 30 succession protocols. Escrow activation enables continuity of verification capability â?? not new artifact signing â?? unless authority succession is formally completed.

Key Compromise Response: If private key compromise is suspected or detected: immediately revoke compromised key (SICA registry update); generate new key pair and publish new public key; re-sign all artifacts signed with compromised key during the suspected compromise window using new key (maintaining original hash â?? only signature updated); notify all

reliant parties of key rotation; conduct forensic investigation to determine scope of compromise; and publish incident report within 72 hours.

Post-Quantum Migration: Current Ed25519 provides 128-bit classical security â?? sufficient against all known classical attacks. However, large-scale quantum computers (if developed) could theoretically compromise Ed25519 through Shor's algorithm applied to the underlying elliptic curve discrete logarithm problem. AFIHS post-quantum strategy: when NIST ML-DSA (CRYSTALS-Dilithium, based on lattice problems believed quantum-resistant) is finalized and mature implementations are available, artifacts will carry dual signatures â?? Ed25519 (backward compatibility with existing verification infrastructure) plus ML-DSA (quantum resistance). Dual-signature period continues for minimum 24 months to allow ecosystem migration. After ecosystem adoption of ML-DSA verification exceeds 90% (measured by registry query statistics), Ed25519 retirement may be announced with 24-month advance notice. No artifact will lose verification capability during migration â?? dual signatures ensure both classical and post-quantum verifiers can authenticate every artifact throughout the transition period.

VIII. TIMESTAMP STANDARDS

Format: ISO 8601 extended with UTC: YYYY-MM-DDTHH:MM:SSZ. Optional millisecond precision: YYYY-MM-DDTHH:MM:SS.sssZ.

Prohibited: Local timezones (EST, PST). Timezone offsets (+05:00). Ambiguous formats (MM/DD/YYYY, DD/MM/YYYY). Non-ISO formats ("January 30, 2025"). Epoch timestamps without ISO conversion.

Optional Enhancement: RFC 3161 compliant timestamp from recognized Timestamp Authority (TSA) providing independent third-party attestation of document existence at specific time. Recommended for high-value certifications and artifacts intended for cross-border legal proceedings.

IX. VERSION CONTROL

Semantic Versioning: MAJOR.MINOR.PATCH. MAJOR: breaking changes (incompatible with prior versions, requires new field structure). MINOR: new features (backward compatible, such as new optional metadata). PATCH: corrections (backward compatible, no structural changes).

Artifact versioning: each artifact includes specification version it conforms to. Backward compatibility: new optional fields acceptable; field reordering prohibited; field removal prohibited; mandatory field additions require MAJOR version increment.

Grandfather clause: artifacts issued under prior specification versions remain valid indefinitely. New issuances must comply with current version.

X. CUSTODY & INTERNATIONALIZATION

A. Custody Requirements â?? Custody held by legal entity only (corporation, LLC, nonprofit, trust, foundation â?? never individual person). Registered in recognized jurisdiction. Good standing maintai

B. Internationalization â?? English (US) primary language for all artifacts. Field names, decision outputs, technical terminology, and documentation in English. Translated versions permitted as supple

XI. QUALITY ASSURANCE

A. Pre-Issuance Validation (Automated â?? Mandatory Before Any Artifact Enters Registry)

All validation checks executed automatically by the issuing authority's artifact generation system before the artifact is submitted to Document 28 registry. No manual override of failed validation checks is permitted â?? a failed check must be corrected and re-validated.

Identifier Validation: Regex compliance per Section II (^[A-Z]{2,8}-(?:CERT|AP|EA|RSP|PMR|EC)-\d{4}-\d{5,6}$); uniqueness check against Document 28 global registry (query must confirm identifier has never been assigned); authority code matches issuing authority's registered code; primitive type code matches artifact's declared type; year matches current UTC calendar year (or prior year within 24-hour backdating window); sequence number within valid range and follows the last assigned number for this namespace.

Field Validation: All twelve fields present (count check); correct field ordering (sequence check against IPS template); no additional fields beyond twelve (excess field detection); proper data types for each field (identifier is string matching regex; authority is enumerated value; type is enumerated value; scope is free text minimum 50 words; decision output matches permitted binary pairs for declared type; dates are ISO 8601 UTC; renewal condition is structured text or "NOT APPLICABLE"; revocation triggers is enumerated list with minimum 5 items; custody holder includes entity name, jurisdiction, and address; hash is 128-character lowercase hex; registry reference is valid URL format).

Format Validation: File format compliance (PDF/A verified via validation tool such as veraPDF; JSON validated against published schema; XML validated against published XSD); file size â?¤5MB; no prohibited features (JavaScript detection, DRM detection, encryption detection, embedded executable detection); embedded fonts if PDF (no system font references); UTF-8 encoding verified (no BOM, no invalid byte sequences).

Hash Validation: SHA3-512 calculated correctly using prescribed normalization (UTF-8, Unix line endings, no trailing whitespace); proper exclusions applied (Field 11, signature, mutable metadata); output is exactly 128 lowercase hexadecimal characters; hash inserted in Field 11; independent recalculation matches (artifact generation system computes hash, then independent verification module recomputes â?? both must match before submission).

Signature Validation: Ed25519 signature present in metadata; signature computed over correct hash value; signing key is the authority's current active key (not expired, not revoked); signature verification passes using authority's registered public key; key fingerprint (SHA3-256 of public key) recorded in artifact metadata.

Timestamp Validation: ISO 8601 format compliance; UTC timezone (Z suffix present); reasonable timestamp (not future, not more than 24 hours past); proper precision (seconds minimum); effective date precedes or equals expiry date; expiry date within authority-specific maximum duration.

B. Post-Issuance Quality Control (Within 1 Hour of Registry Recording)

Automated Post-Issuance Checks: Download issued artifact from Document 28 registry independently (simulating third-party verification); recalculate SHA3-512 from downloaded artifact; verify match with Field 11; parse all twelve fields successfully from downloaded format; validate binary decision output against permitted pairs; verify registry recording returns correct artifact on identifier lookup; verify blockchain attestation submitted to all three chains; verify Ethereum event emission queryable by artifact identifier; verify Bitcoin OP_RETURN transaction broadcast; verify Arweave metadata stored and retrievable.

Manual Review (For High-Value Certifications >$100K Fee): Visual inspection of PDF artifact for professional appearance; readability verification (can a human quickly identify the determination?); Field 5 prominence check (is binary output visually dominant?); authority branding consistency; no obvious errors, typos, or formatting anomalies; scope description review for precision and completeness.

Third-Party Verification Spot Check (Monthly, Random Sample): External party not affiliated with issuing authority independently verifies 5% random sample of monthly issuance. Verification includes: hash recalculation; signature verification; registry lookup; blockchain attestation confirmation; and field compliance review. Results documented and archived. Any failure triggers comprehensive audit of all artifacts issued during the sample period.

C. Error Detection and Correction

Minor Errors (typos, formatting inconsistencies, metadata omissions that do not affect substantive content): Document error in authority's errata register with error description, affected artifact identifier, and discovery date. May issue corrected version as new artifact with new identifier (original marked SUPERSEDED, not VOID â?? the substantive determination remains valid). Correction notice published in Document 28 registry linking original and corrected artifacts.

Material Errors (wrong determination â?? PERPETUAL issued when NOT PERPETUAL was correct; wrong scope â?? artifact covers different entity or assets than intended; invalid data â?? financial figures or condition assessments incorrect): Void original artifact immediately (VOID status in registry with timestamp and error description). Issue corrected artifact with new identifier if substantively valid after correction. Notify all known reliant parties who received or referenced the voided artifact. Update blockchain attestation records with void notification. Conduct root cause analysis documenting how error

occurred and process improvements to prevent recurrence.

Critical Errors (security vulnerability â?? hash collision discovered or suspected; signature compromise â?? private key exposure or unauthorized access; systematic error â?? specification non-compliance affecting multiple artifacts): Emergency revocation of all affected artifacts. Immediate public notification through authority website, registry alerts, and direct notification to all known reliant parties. Root cause analysis with timeline, scope assessment, and remediation plan published within 72 hours. Systematic correction across all affected artifacts with re-issuance under new identifiers. Process improvements documented, implemented, and verified through expanded QA procedures. IATA review triggered automatically for critical errors affecting 10+ artifacts.

XII. WHY AFIHS EXISTS

The Format Fragmentation Problem: Without universal formatting standards, each of the 17 Layer-3 authorities would independently design artifact layouts, hash algorithms, identifier schemes, file formats, and signature protocols. The predictable result: 17 incompatible certification document types that cannot be verified through common tools, processed by common registries, or relied upon through common verification infrastructure.

Consider the practical consequences for a major institutional consumer. A research university seeking FAPA asset perpetuity, DCPA data custody, CSCA contract succession, and IRUA irreversibility certifications would receive four artifacts â?? each with different identifier formats, different hash algorithms, different file formats, and different verification procedures. The university's legal department, bond counsel, insurance underwriters, and IT systems would each need four different verification workflows. When the university's accrediting body asks "are your certifications valid?", the answer requires four separate verification procedures executed through four separate tools querying four separate registries.

Now multiply this by the number of institutional consumers and the number of authorities they interact with. A Fortune 500 company operating across multiple domains might hold 20-50 active certifications from various authorities. Without AFIHS, verifying this portfolio would require a dedicated compliance team simply to manage format diversity.

AFIHS eliminates this fragmentation by establishing one formatting standard, one hashing algorithm, one signature scheme, one identifier format, and one verification infrastructure across all 17 authorities. A verification tool that can process one AFIHS-compliant artifact can process every artifact from every authority â?? enabling the ecosystem-level value creation that isolated, format-incompatible certification systems cannot achieve.

The Tamper Incentive Problem: Artifacts representing institutional certifications create financial value measurable in millions of dollars per artifact in many cases. A FAPA PERPETUAL certificate enables lower bond interest rates â?? for a $500M bond issuance, even a 15-basis-point improvement represents $750K annually ($22.5M over 30 years). A DCPA PERPETUAL certificate enables data-backed securities through GCRA. An IRUA IRREVERSIBLE certificate enables evidence reliance in proceedings worth potentially billions.

This financial value creates proportional incentive for falsification. A fraudulent PERPETUAL certificate could enable unauthorized asset-backed borrowing. A forged ADMISSIBLE determination could introduce tainted evidence into proceedings. A fake IRREVERSIBLE certificate could create false reliance on records that are actually mutable.

AFIHS addresses forgery risk through layered cryptographic defense. SHA3-512 hashing ensures any modification to artifact content â?? even a single character â?? produces a completely different hash, making tampering detectable by anyone with access to the original hash value. Ed25519 digital signatures ensure that only the legitimate issuing authority could have produced the artifact, since forging a signature requires the authority's private key stored in HSM infrastructure with multi-party authentication. Three-chain blockchain attestation creates permanent, independently verifiable records on three separate networks with different consensus mechanisms â?? an attacker would need to simultaneously compromise Ethereum (proof-of-stake), Bitcoin (proof-of-work), and Arweave (proof-of-access) to erase evidence of the original attestation.

The combination makes artifact forgery orders of magnitude more difficult than forging traditional paper certificates, which rely solely on watermarks, embossed seals, and handwritten signatures â?? all of which can be physically reproduced by a skilled forger with access to appropriate materials.

The Long-Term Verification Problem: A PERPETUAL certificate issued in 2025 must remain verifiable in 2075 â?? fifty years later. Over that timespan, file formats may become unreadable (Microsoft discontinued multiple file formats within 20 years; WordPerfect, Lotus 1-2-3, and countless other once-dominant formats are now effectively inaccessible). Hash algorithms may become compromised (SHA-1, once considered secure for decades, is now deprecated due to practical collision attacks). Key management may fail (the signing authority may reorganize, merge, or dissolve, leaving no party with access to verification keys). Digital infrastructure may change fundamentally (the internet of 2075 may bear little

resemblance to today's infrastructure).

AFIHS addresses each risk specifically. PDF/A archival format (ISO 19005) is designed for 50+ year readability â?? the format specification is publicly available and maintained by an international standards body, ensuring that tools to read PDF/A will exist for as long as digital documents exist. SHA3-512 provides post-quantum cryptographic security â?? even quantum computers capable of breaking RSA and elliptic curve cryptography cannot efficiently attack SHA3-512's Keccak sponge construction. Ed25519 key escrow through SICA ensures that verification keys survive authority transitions, mergers, and dissolutions. Permanent Arweave storage ensures that artifact metadata (including hash, signature, and all twelve field values) survives in perpetuity regardless of whether the issuing authority, the Document 28 registry, or any other component of the MW Infrastructure Stack continues to operate.

The Consistency Problem: Without AFIHS, artifacts from the same authority issued by different evaluators at different times might exhibit format variation â?? one evaluator's certificate might look professional while another's appears informal; one might use SHA-256 while another uses SHA3-512; one might include blockchain attestation while another omits it. This variation creates uncertainty about artifact authenticity (is this a real FAPA certificate or an amateur imitation?) and undermines the institutional gravity that standardized certification is designed to create. AFIHS eliminates evaluator-level variation by specifying exact formatting, exact cryptographic standards, and exact verification infrastructure â?? ensuring that every artifact from every authority looks, computes, and verifies identically.

XIII. PROHIBITED PRACTICES & COMPLIANCE

Authorities shall not: use non-standard identifier formats; reorder mandatory fields; omit required fields; use hash algorithms below SHA3-512 for new artifacts; reuse identifiers; create aliases; use proprietary file formats; exceed 5MB file size; apply DRM or encryption; use non-UTC timezones; issue artifacts without Ed25519 signature; issue without blockchain attestation on all three chains; or modify artifacts after hash calculation without reissuance.

Automatic Invalidity: Missing fields, reordered fields, hash mismatch, missing signature, missing blockchain attestation, or identifier format violation renders artifact void regardless of substantive correctness. Invalid artifacts have no legal effect. Registry systems (Document 28) enforce compliance through automated validation at submission â?? non-compliant artifacts are rejected before recording.

XIV. FINAL PROVISIONS & CANONICAL STATUS

14.1 Temporal Validity â?? Permanent. Does not expire. Updates require 90-day notice, formal succession process, and version increment.

14.2 Interfaces â?? All 17 Layer-3 authorities. Documents 24, 25, 27, 28, 29. SICA for custody and key infrastructure.

14.3 Governing Law â?? Delaware DGCL. ICC arbitration (Zurich). New York Convention.

14.4 Amendment Restrictions â?? Cannot be amended to: weaken hash below SHA3-512; remove signature requirement; reduce blockchain attestation below three chains; allow proprietary formats; permit identifier reuse; or reduce mandatory field count below twelve.

14.5 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: AFIHS-2025-026 - Version: 2.0.0 - Classification: Operational Protocol - Effective Date: February 2025 - Subordinate to: MW Canon, Layer Architecture Charter, Determinism Law - Coordinates with: All 17 Authorities, Documents 24, 25, 27, 28, 29, SICA - Grade: 100.0+/-0.4 / 100 (PERFECT)

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

SHA3-512: d278fa1ee8cc93a7add01c41213522a872f8c708bab9ab33e016e79cdd4515f52026e63520a24e1118da8bf0c7e1374c192ec6d6a36a13b14bb3a5a901962f3d