Chain of Custody Formalisation in Digital Forensics:

The Modulign ^EVID Architecture as a Registry-Based Evidentiary Framework

Vincent Gonzalez

Independent Scholar

modulign.org · VinceGonzalez@me.com

2026

Target: Journal of Digital Investigation · Digital Evidence and Electronic Signature Law Review

Abstract

Digital chain of custody remains a frequently litigated and consequential vulnerability in forensic evidence proceedings. Existing frameworks — NIST SP 800-86, ISO/IEC 27037, the ACPO Good Practice Guide — establish procedural requirements for evidence handling but share a foundational architectural feature: chain of custody is implemented as a procedural record appended to evidence after collection, making its integrity dependent on the conduct of collecting officers and the reliability of documentary processes external to the evidence itself. This paper argues that the Modulign Standard — a Dimensional Address Grammar for Observable Reality (DAG-OR) — addresses this vulnerability at its structural root by integrating chain-of-custody documentation into the evidence-grade registration event itself, rather than maintaining it as a separable procedural layer.

Under the Modulign ^EVID protocol, chain of custody is not a procedural record attached to an observation after the fact: it is architecturally embedded in the observation's classification act. The append-only ledger, cryptographic signature chain, and observer competence gate collectively make chain-of-custody documentation a structural property of evidence-grade registration within the Modulign system rather than a compliance artefact maintained alongside it. The paper demonstrates that Modulign-classified digital evidence provides a strong formal basis for satisfying the authentication requirements of Federal Rule of Evidence 901(b)(9), supports compliance with the integrity requirements of ISO/IEC 27037, and materially strengthens defensibility under the preservation obligations of Zubulake v. UBS Warburg (S.D.N.Y. 2003) and Federal Rule of Civil Procedure 37(e) — through architectural properties rather than procedural compliance steps alone.

The Modulign Standard is a published specification. It has not yet been independently validated through empirical testing, adopted by a recognised standards body, or subjected to adversarial scrutiny in legal proceedings. This paper's claim is that the formal architecture is logically sound, that it addresses a genuine and recurring vulnerability in digital evidence practice, and that it is designed to operate within — not to replace — existing evidentiary doctrine.

1. The Structural Problem in Digital Chain of Custody

1.1 The Recurring Vulnerability

Chain-of-custody challenges are among the most frequently litigated grounds for attacking digital evidence in legal proceedings. Courts routinely evaluate whether gaps in the handling record affect the admissibility or weight of digital evidence, and the outcomes are inconsistent across jurisdictions and fact patterns.

The challenge is structurally predictable. In existing frameworks, chain of custody is a documentary record produced alongside evidence, not a property of the evidence's registration. The record can be incomplete, altered, lost, or challenged on the basis of officer conduct. Each link in the chain depends on a human actor's compliance with procedural requirements that are external to the evidence and unverifiable from the evidence's internal properties.

In United States v. Comprehensive Drug Testing, Inc. (621 F.3d 1162, 9th Cir. 2010), the Ninth Circuit addressed the handling of digital evidence in complex seizures, emphasising the need for protocols that prevent commingling and ensure that only authorised material is reviewed. In Lorraine v. Markel American Insurance Co. (241 F.R.D. 534, D. Md. 2007), Judge Grimm produced the most comprehensive judicial treatment of digital evidence authentication under the Federal Rules of Evidence, identifying the persistent gap between the sophistication of digital evidence and the adequacy of authentication foundations. In United States v. Bansal (663 F.3d 634, 3d Cir. 2011), the Third Circuit evaluated chain-of-custody objections to digital evidence, holding that defects went to weight rather than admissibility — but only after extensive litigation over the handling record. In State v. Kandies (467 S.E.2d 67, N.C. 1996) and its progeny, courts articulated the standard that the proponent must establish a reasonable probability that the evidence has not been altered — a standard that procedural records can support but cannot guarantee.

These cases illustrate a consistent pattern: chain-of-custody disputes over digital evidence are frequently litigated, generate significant uncertainty, and are resolved through case-specific evaluation of procedural records whose completeness and reliability are themselves at issue. Courts have generally held that chain-of-custody defects go to weight rather than admissibility unless the defect is sufficiently serious to undermine a reasonable probability of integrity. The determination of what constitutes "sufficiently serious" is ad hoc, and the procedural records on which it depends are vulnerable to the very gaps that generate the dispute.

1.2 What Existing Standards Provide

Three frameworks dominate digital forensic practice.

NIST Special Publication 800-86 (Guide to Integrating Forensic Techniques into Incident Response, 2006) establishes best practices for digital evidence handling and recommends cryptographic hashing as the foundational integrity mechanism. The hash verifies that a file has not been altered between two points in time. It does not verify the conditions of collection, the competence of the collector, or the soundness of pre-hash handling.

ISO/IEC 27037:2012 (Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence) specifies procedural requirements for the full handling chain. The standard requires documentation of each phase. But the documentation is a separable procedural layer — it can be challenged, supplemented, or impeached independently of the evidence's content.

The ACPO Good Practice Guide for Digital Evidence (2012) establishes the four-principle framework — lawful authority, minimisation of handling, audit trail maintenance, and responsibility — that has governed digital forensic practice in United Kingdom jurisdictions. The ACPO guide remains historically significant and widely cited, though UK practice has evolved through subsequent NPCC, CPS, and Forensic Science Regulator guidance. Its four principles remain the canonical articulation of foundational requirements.

These frameworks share a common architecture: chain of custody is a procedural layer imposed on top of digital evidence. The hash proves the file was not altered after hashing; it does not prove the pre-hash

handling was sound, the collection was lawful, or the observer was competent. The result is a persistent practical vulnerability. Chain-of-custody challenges regularly succeed in impeaching the reliability of the handling record — not because the evidence is substantively unreliable, but because the procedural record contains gaps that a skilled advocate can exploit.

1.3 The Proposed Response

The Modulign Standard addresses this vulnerability not by strengthening the procedural layer but by integrating chain-of-custody documentation into the evidence registration event itself, so that the two are not maintained as separable records. The remainder of this paper describes how that integration works, what it achieves, and what it does not achieve.

2. The ^EVID Architecture: Chain of Custody as Embedded Property

The Modulign Standard introduces the ^EVID meta flag as a classification status within the Modulign registry, not as a label appended to evidence after the fact. This distinction is architecturally fundamental and must be stated precisely.

A label is attached to evidence after the evidence exists as an independent object. It is separable: it can be removed, overwritten, or challenged independently of the evidence. The evidence's identity does not depend on the label.

A classification status within the Modulign registry is a property of the evidence's formal identity within the system. An observation bearing ^EVID was registered through a specific protocol whose completion is a precondition for evidence-grade status under the Standard. The status does not describe what happened to the evidence after collection. It records the epistemic architecture under which the evidence entered the registry.

The critical qualification: ^EVID status is a property of the evidence's existence within the Modulign registry. It is not a metaphysical claim about the evidence's ontological status. The evidence — the digital file, the image, the log entry — exists independently of the registry. What the registry provides is a formal, verifiable, tamper-resistant record of the conditions under which the evidence was registered, classified, and preserved. That record is structurally inseparable from the evidence's identity within the system, rather than maintained as a separate procedural document.

2.1 The Append-Only Ledger

Standard Modulign classifications use mutable logs: entries can be superseded by newer entries with later timestamps. Evidence-grade classifications use an append-only ledger: no classification entry can be deleted or modified after emission. A subsequent classification that supersedes an earlier one produces a new timestamped entry with a cryptographic link to the prior entry. The earlier record remains in the ledger permanently.

The legal significance is direct. Evidence preservation obligations under Zubulake v. UBS Warburg (220 F.R.D. 212, S.D.N.Y. 2003) and Federal Rule of Civil Procedure 37(e) require parties to preserve electronically stored information once litigation is reasonably anticipated. The Modulign append-only ledger materially strengthens defensibility under these obligations: within the registry, deletion of classification records is not architecturally possible.

What the ledger does not do. The append-only property prevents deletion of records within the ledger. It does not prevent: failure to collect evidence in the first place; incomplete or selective registration; loss or

corruption of evidence before ingestion into the system; withholding of evidence that was never registered; hardware-level corruption of the ledger storage medium; or compromise of signing keys. Spoliation can occur through any of these vectors despite the ledger's append-only property. The ledger materially reduces post-ingestion tampering risk and creates a durable preservation record for registered evidence. It does not eliminate all forms of spoliation or evidence loss. The paper's claim is the narrower one: that within the scope of registered evidence, the architecture provides stronger preservation guarantees than procedural compliance alone.

2.2 The Cryptographic Signature Chain

Every ^EVID ledger entry bears a cryptographic signature. The verification structure is:

$$\text{Verify}(C_i, t_i, \sigma_{i-1}, \sigma_i, pk) = \text{TRUE}$$

A verification failure at position i indicates that the ledger was tampered at position i or later. The chain structure means that no single tampered entry is locally undetectable: tampering at any point propagates forward, breaking all subsequent verification checks.

Attribution follows formally: the holder of the signing key produced entry i at time t_i, and the signature provides cryptographic evidence of that fact. This supports attribution and integrity in a manner consistent with the principles reflected in the Electronic Signatures in Global and National Commerce Act (E-SIGN, 15 U.S.C. § 7001 et seq.) and the Uniform Electronic Transactions Act (UETA). Those statutes facilitate legal effect for electronic records and signatures; the evidentiary sufficiency of any particular signature still depends on implementation, key management, attribution evidence, and surrounding facts. The Modulign signature chain provides the technical foundation; the legal conclusion remains the court's.

2.3 The Observer Competence Gate

Not all Modulign classifications are ^EVID-eligible. The Standard specifies an observer competence hierarchy:

Competence Level	Description	^EVID Eligibility
:T — Trained	Applied full CDP at least once under supervision	Not eligible without additional qualified review
:E — Expert	Domain specialist with demonstrated classification accuracy	Eligible with two independent expert classifiers (:E×2)
:A — Authority	Registry-certified domain authority	Eligible independently

The two-expert consensus requirement for :E-level ^EVID eligibility reflects a principle found across evidentiary frameworks: independent corroboration strengthens reliability. The multi-examiner confirmation requirements in accredited forensic laboratories under ASCLD/LAB and ANAB standards, the two-witness rule in federal perjury prosecutions (18 U.S.C. § 1621), and the corroboration requirements for accomplice testimony in many state jurisdictions all embody this principle. The Modulign Standard encodes the corroboration requirement into the classification grammar, making it a precondition for evidence-grade registration rather than a post-hoc compliance check.

The observer competence gate serves a second function: it creates a registry-verifiable, machine-readable record of examiner qualification at the time of classification. This supplements — but does not replace — the existing expert qualification process under Daubert v. Merrell Dow Pharmaceuticals (509 U.S. 579, 1993) and its progeny.

3. Authentication Under Federal Rule of Evidence 901(b)(9)

Federal Rule of Evidence 901(b)(9) provides that evidence may be authenticated by "evidence describing a process or system and showing that it produces an accurate result." As Judge Grimm observed in Lorraine, this provision was designed with digital evidence squarely in mind, because digital evidence often cannot be authenticated by a witness who "saw" it in the way that a physical object can. Authentication of digital evidence turns substantially on the reliability of the process that produced or preserved it.

The Modulign Classification Decision Protocol (CDP) is designed to function as exactly the kind of documented, reproducible process that Rule 901(b)(9) contemplates. The eight-step CDP specifies: observation identification and GSI-ID assignment; domain classification with mandatory competence annotation; dimensional coordinate assignment (realm, locus, medium); confidence scoring (0.00–1.00 scale) with mandatory reasoning record; relation mapping (causal, sequential, derivational links); meta-flag assignment (including ^EVID / ^PROV determination); ledger entry emission with cryptographic signature; and registry confirmation and hash verification.

The CDP's output — a canonical MGN code with attached JSON record — encodes the domain classification, locus, observer identity, competence level, confidence score, and reasoning chain in a machine-parseable, human-readable format. This record provides a formal basis for authentication testimony under Rule 901(b)(9) and expert testimony under Rule 702: the witness can describe the process (the CDP), identify its specific application to the evidence at issue, and point to the verifiable record that documents both.

3.1 The Three-Layer Architecture and Evidentiary Requirements

The Modulign architecture separates three layers, each mapping onto a distinct evidentiary function:

Modulign Layer	Evidentiary Function	Key Property
Identity Layer (GSI-ID)	Exhibit identification	Immutable. Assigned at first registration. Anchors the Observational Ledger.
Classification Layer (MGN code)	Evidentiary characterisation	Dynamic. Updated when the observation changes. All historical entries permanent in ledger.
Semantic Layer (vector embedding, anomaly score)	Expert analysis	Optional. Supplementary. Never overrides Classification Layer.

The separation of the Identity Layer from the Classification Layer is forensically significant. Chain-of-custody challenges typically attack either the identity of evidence (substitution or mislabelling) or its integrity (alteration after collection). The GSI-ID's immutability and content addressing provide strong evidence against substitution claims: the identifier is cryptographically bound to the content at registration, and any substitution would produce a hash mismatch detectable through automated verification. The append-only ^EVID ledger provides strong evidence against alteration claims: any modification to the classification record after registration is detectable through the signature chain, and all prior entries are preserved.

Both attack vectors are addressed at the architectural level rather than depending solely on the procedural compliance of individual handlers. This does not eliminate the possibility of challenge — a court may still

evaluate the reliability of the system itself, the competence of the registering observer, or the conditions of initial collection. But it provides a substantially stronger foundation for authentication than a procedural record maintained separately from the evidence.

3.2 The Distinction Between System-Level Status and Legal Consequence

A point of precision applies throughout this paper. The Modulign architecture determines system-level status: whether evidence is registered, whether it bears ^EVID or ^PROV status, whether the signature chain verifies, whether the observer met competence thresholds. These are formal properties within the Modulign system.

Legal consequences — admissibility, weight, authenticity, sufficiency — remain the court's determination. A ^EVID classification provides the court with a strong formal record on which to base its authentication analysis. It does not preempt judicial gatekeeping. A court may still evaluate the reliability of the Modulign system itself under Daubert or Frye; hear testimony about the conditions of initial collection; consider challenges to signing key management; assess whether the system was properly implemented in the specific case; and weigh the evidence in light of all circumstances. The architecture provides the record. The court applies the law.

4. The Best Evidence Rule and Digital Originals

The best evidence rule (Federal Rules of Evidence 1001–1008) requires production of the original writing, recording, or photograph when its content is at issue. For digital evidence, the question of what constitutes an "original" is non-trivial. Rule 1001(d) provides that for electronically stored information, an "original" is "any printout — or other output readable by sight — if it accurately reflects the information."

The Modulign GSI-ID provides a formal basis for resolving this question. The GSI-ID is assigned at first registration and is immutable. The Observational Ledger anchored by the GSI-ID is the complete timestamped history of every MGN code ever assigned to that observation stream. Any output — printout, digital file, transmitted record — that carries the GSI-ID and matches the Observational Ledger hash provides strong evidence that it accurately reflects the registered information.

This does not eliminate the need for testimony in all cases. A court may require testimony about the system's reliability, the registration conditions, or the chain of events between registration and production. But the architecture substantially reduces the testimonial burden by providing an automated, verifiable mechanism for establishing that a given output corresponds to the registered record.

5. The ^PROV Quality Gate

The Modulign Standard contains an internal quality-control mechanism. Any classification produced without a domain competence annotation, or with a confidence score below 0.60, automatically receives the ^PROV (provisional) meta flag. Provisional classifications are not eligible for ^EVID status and are marked within the system as below evidence-grade.

This is not an "exclusionary rule" in the legal sense — it is not a court-enforced doctrine excluding evidence for constitutional or policy reasons. It is an internal quality gate: a system-level threshold that distinguishes evidence-grade registration from provisional registration, and marks the distinction in the classification record itself.

The legal significance of this mechanism is indirect but real. A proponent who presents a ^PROV classification in a legal proceeding without disclosing its provisional status has withheld material information about the evidence's epistemic grade within the classification system. In civil proceedings, this implicates the disclosure obligations of Federal Rule of Civil Procedure 26(a)(2), which requires expert witnesses to disclose all facts or data considered in forming their opinion, and Rule 26(e), which requires supplementation if previously disclosed information is incomplete or incorrect. In criminal proceedings, where the prosecution introduces ^PROV-classified evidence without disclosing the provisional designation, the non-disclosure may be relevant to Brady v. Maryland (373 U.S. 83, 1963) obligations — to the extent the provisional status is material to the evidence's reliability and the prosecution is aware of it. The Brady analysis is context-dependent: materiality, suppression, and prejudice must each be established on the facts of the case. The paper does not claim that non-disclosure of ^PROV status automatically constitutes a Brady violation; it claims that the ^PROV designation creates a formally documented epistemic limitation whose non-disclosure is relevant to existing disclosure obligations.

6. Relationship to Existing Digital Forensic Standards

The Modulign Standard does not replace NIST SP 800-86, ISO/IEC 27037, or the ACPO Good Practice Guide. It is designed to provide a formal classification and registration layer that these frameworks presuppose but do not themselves specify.

6.1 What Existing Standards Provide

NIST SP 800-86 recommends SHA-256 hashing for evidence integrity and establishes best practices for forensic technique integration. It does not specify a classification grammar, observer competence encoding, or formal reasoning record of the kind required for a complete authentication foundation under Rule 901(b)(9). ISO/IEC 27037 specifies handling procedures for digital evidence across the full lifecycle. It requires documentation of each phase but does not specify a formal language for encoding the epistemic status of the observation at the moment of collection, or a mechanism for binding that documentation to the evidence's formal identity. The ACPO Good Practice Guide requires audit trail maintenance and establishes foundational principles. It does not specify the structure of the audit trail with sufficient formalism to support automated verification or machine-readable competence assessment.

6.2 What Modulign Adds

The Modulign Standard is designed to provide the formal specification layer that sits beneath these procedural frameworks: a classification grammar encoding domain, locus, medium, observer, competence, and confidence in a structured, machine-parseable format; an identity system (GSI-ID) that binds the evidence's identifier to its content cryptographically at registration; a registration protocol (CDP) that documents the classification decision in a reproducible, verifiable format; a ledger architecture (append-only for ^EVID) that preserves the complete classification history; and a competence encoding (:T/:E/:A) that records examiner qualification at the time of classification.

A forensic collection procedure that satisfies the Modulign CDP's eight steps, observer competence requirements, and ^EVID protocol is designed to be implementable in a manner consistent with the requirements of NIST SP 800-86, ISO/IEC 27037, and the ACPO principles. The paper does not claim that Modulign compliance automatically satisfies those standards — that claim would require a clause-by-clause compliance mapping beyond this paper's scope. The paper claims that the Modulign architecture is designed to strengthen and formalise the evidentiary foundation that those standards' procedural requirements presuppose, and that the two layers are complementary.

7. Constitutional Considerations

7.1 The Confrontation Clause

When a Modulign ^EVID classification is introduced in a criminal proceeding — as evidence of the conditions under which digital evidence was registered — the classification functions as an expert assertion about the evidence's provenance and integrity. Under Crawford v. Washington (541 U.S. 36, 2004) and Melendez-Diaz v. Massachusetts (557 U.S. 305, 2009), forensic reports are testimonial, and their authors must be available for cross-examination.

The Modulign ^EVID protocol accommodates this requirement directly: the protocol requires a named, credentialed observer whose identity is recorded in the classification record. That person is the witness subject to confrontation. This mirrors the existing requirement for forensic analysts who produce laboratory reports, chain-of-custody affidavits, and expert certifications. The framework creates the record; the Constitution requires the record's author to be available for examination.

7.2 Due Process and Access Equity

If the Modulign framework becomes widely adopted, a practical concern arises: parties without access to the system may face a perceived disadvantage in proving the authenticity or integrity of their evidence. The framework is not, and must not become, a prerequisite for admissibility. Evidence that was not registered under the Modulign protocol remains admissible through all existing authentication pathways — witness testimony, circumstantial evidence, expert analysis, metadata examination, and any other method recognised under FRE 901. The Modulign framework provides an additional authentication pathway that is more formal, more verifiable, and more resistant to challenge than procedural records alone. It does not render existing pathways inadequate. The Standard is published under an open-access license and is freely available for implementation without license fees.

7.3 Judicial Gatekeeping

As discussed in Section 3.2, the court remains the ultimate gatekeeper. The Modulign system determines registration status within its own architecture; the court determines legal consequence. A Daubert or Frye challenge to the Modulign methodology itself is entirely appropriate and should be anticipated. The Standard's published specification, documented protocol, and open-access availability are designed to support that scrutiny. Whether the methodology satisfies Daubert's requirements — testability, known error rate, peer review, general acceptance — is a question that can only be resolved through the empirical and institutional validation process described in Section 9.

8. Implications for Digital Forensic Practice

8.1 Observer Certification

The observer competence gate (:T/:E/:A) provides a formal framework for forensic examiner qualification that maps onto existing professional certification structures — EnCase Certified Examiner (EnCE), GIAC Certified Forensic Examiner (GCFE), Certified Forensic Computer Examiner (CFCE), and comparable credentials — without replacing them. A Modulign competence designation for a certified forensic examiner provides the legal system with a machine-readable, registry-verifiable statement of qualification

that supplements the existing expert qualification process under Daubert. It does not substitute for that process: judicial qualification of an expert witness remains the court's function.

8.2 Multi-Jurisdiction Evidence

The Modulign jurisdiction annotation (§JUR) encodes the governing legal framework at the time of collection — for example, §US-FL for Florida state law, §EU-GDPR for EU data protection regulation, §INTL-ICC for International Criminal Court proceedings. Evidence registered under the Modulign protocol carries its jurisdictional context in the classification record itself. The jurisdiction annotation does not resolve conflicts of law — that remains a judicial and doctrinal question. It ensures that the jurisdictional context of collection is formally recorded and available for the court's analysis.

8.3 The Relation Registry as Provenance Evidence

The Modulign Relation Registry provides formally documented links between related observations: →CAU→ (causal predecessor), →SEQ→ (temporal sequence), and →DRV→ (derivation/provenance). These relation codes create a formally documented provenance architecture for derivative evidence. Every item collected from a crime scene that has been Modulign-registered bears a →DRV→ relation record linking it to the scene's GSI-ID. The derivation chain is encoded in the classification grammar and preserved in the append-only ledger, rather than maintained in a separate procedural record subject to independent challenge. The practical advantage is consolidation: multiple fragmented evidentiary records — collection logs, transfer forms, processing notes, storage records, hash reports — are integrated into a single verifiable provenance object anchored by the GSI-ID.

8.4 Data Protection Considerations

In jurisdictions subject to the GDPR or equivalent data protection legislation, the Modulign registry's recording of observer identities, competence annotations, and classification decisions raises data protection questions. Under GDPR Articles 17 (right to erasure) and 21 (right to object), data subjects have rights that may appear to conflict with the append-only architecture. The resolution lies in the GDPR's own exceptions: processing necessary for compliance with a legal obligation (Article 6(1)(c)), processing necessary for the establishment, exercise, or defence of legal claims (Article 9(2)(f)), and processing in the public interest for archiving or research purposes (Article 89). Evidence-grade forensic records fall squarely within these exceptions. Technical mitigations are also available: pseudonymisation of classifier identities within the ledger, with a separate key-management system that can respond to erasure requests by deleting the pseudonymisation key. This approach must be specified in any EU implementation of the framework.

9. The Adoption Pathway

A classification standard has practical value only to the extent it is adopted. This section identifies the stakeholders, steps, and conditions required for the Modulign ^EVID architecture to move from published specification to operational use.

9.1 Who Adopts

Forensic laboratories and examiners are the most natural first adopters. The framework supplements existing forensic workflows by providing a formal registration layer. Law enforcement agencies would adopt the framework as part of digital evidence handling procedures, alongside existing NIST and ISO-compliant workflows. E-discovery vendors and incident response teams are a second-tier adoption target. Courts adopt last, not first. Judicial adoption requires that the methodology has been independently

validated, implemented by practitioners, and tested in adversarial proceedings — exactly as with any forensic methodology subject to Daubert scrutiny.

9.2 Adoption Sequence

The adoption pathway is: (1) publication and open review, completed (Zenodo, open-access, DOI: 10.5281/zenodo.19348703); (2) independent peer review, in progress; (3) pilot implementation by forensic laboratories, ideally in partnership with an accredited facility willing to run the protocol alongside existing workflows; (4) empirical validation, establishing classification reproducibility, observer agreement rates, and error rates; (5) certification infrastructure, engaging an independent accreditation body (analogous to ANAB for forensic laboratories) to certify classifiers against the Standard's published competence requirements — preventing the circularity of a standard that certifies its own certifiers; (6) adversarial testing in proceedings where opposing counsel can challenge the methodology under Daubert or Frye; (7) standards body engagement with NIST, ISO, or equivalent; and (8) judicial adoption by courts that have evaluated the methodology through the preceding steps.

9.3 Operational Questions

Several operational questions must be resolved through pilot implementation. Key management: how are signing keys generated, distributed, stored, and revoked? Key compromise would undermine the signature chain's integrity. Offline collection: how is evidence registered when the collecting officer lacks network access to the registry? Pre-registration evidence: how is evidence collected before the Modulign system was available brought into the registry? Competing registries: if multiple Modulign-compatible registries exist, how are they synchronised and how are conflicts resolved? These are implementation questions, not architectural objections. They are solvable through standard engineering and operational design. But they must be solved — and documented — before the framework can claim operational readiness.

10. Limitations

This paper proposes a formal framework and argues for its logical soundness. It does not claim that the framework is ready for immediate judicial adoption.

First, the Modulign Standard is a published specification. It has not been independently validated through empirical testing, adopted by a recognised standards body, or subjected to adversarial scrutiny in legal proceedings. The adoption pathway described in Section 9 identifies the steps required to address this limitation.

Second, the paper's case law survey, while covering significant precedents, is not exhaustive. A comprehensive empirical survey of judicial treatment of chain-of-custody disputes across jurisdictions would strengthen the problem identification.

Third, the paper claims that the Modulign architecture is designed to be compatible with NIST SP 800-86, ISO/IEC 27037, and the ACPO Good Practice Guide. This claim is based on architectural analysis, not on a clause-by-clause compliance mapping. A formal compliance mapping is necessary before the compatibility claim can be stated with full confidence.

Fourth, the framework addresses the registration, classification, and preservation dimensions of chain of custody. It does not address the collection dimension — the initial act of identifying and acquiring digital evidence from its source environment. Collection remains governed by existing procedural standards and legal authority requirements.

Fifth, the framework's security depends on the integrity of the cryptographic infrastructure. Advances in cryptanalysis or quantum computing could affect the long-term security of SHA-256 hashing and current signature schemes. The Standard's specification should be designed for algorithm agility — the ability to migrate to stronger cryptographic primitives as needed.

Sixth, the framework has not been tested in adversarial proceedings. The strongest claims in this paper — that the architecture provides a strong basis for 901(b)(9) authentication, that it strengthens Zubulake defensibility, that the ^PROV quality gate has disclosure implications — are analytical conclusions based on the architecture's formal properties. They have not been tested by opposing counsel, evaluated by judges, or subjected to the scrutiny that litigation provides. That testing is a necessary condition for the framework's maturity.

11. Conclusion

The chain-of-custody vulnerability in digital forensic evidence is architectural, not merely procedural. Existing frameworks address it by strengthening procedural requirements external to the evidence itself. The Modulign ^EVID architecture addresses it by integrating chain-of-custody documentation into the evidence-grade registration event, making the two structurally inseparable within the registry rather than maintaining them as independent records.

This paper has demonstrated that Modulign-classified digital evidence satisfying the ^EVID protocol provides a strong formal basis for authentication under Federal Rule of Evidence 901(b)(9); supports compliance with the integrity standards of ISO/IEC 27037 and the hashing requirements of NIST SP 800-86; materially strengthens defensibility under the preservation obligations of Zubulake and FRCP 37(e) by preventing deletion of classification records within the ledger; and provides the court with a verifiable, machine-readable record of examiner qualification, classification reasoning, and provenance history.

The observer competence gate encodes examiner qualification into the classification record. The ^PROV quality gate marks below-threshold classifications as provisional, creating formally documented epistemic limitations whose non-disclosure in proceedings implicates existing obligation frameworks. The Relation Registry provides a unified provenance architecture that consolidates fragmented handling records into a single verifiable object.

> *The framework is a published specification. It is designed to operate within existing evidentiary doctrine — not to replace it. Existing law is capable of accommodating such a framework; the evidentiary doctrines are adequate to receive it. What remains is the empirical and institutional work of validation, pilot implementation, adversarial testing, and standards-body engagement. That work can now proceed on a defined and openly available foundation.*

References

ACPO. 2012. Good Practice Guide for Digital Evidence. Association of Chief Police Officers.

Brady v. Maryland, 373 U.S. 83 (1963).

Crawford v. Washington, 541 U.S. 36 (2004).

Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993).

Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 U.S.C. § 7001 et seq.

Federal Rules of Civil Procedure, Rules 26(a)(2), 26(e), 37(e).

Federal Rules of Evidence, Rules 702, 901, 1001–1008.

Gonzalez, V. 2026a. Modulign Standard v3.0. Zenodo. https://doi.org/10.5281/zenodo.19348703

Gonzalez, V. 2026b. The Formal Logic of Modulign. Zenodo. https://doi.org/10.5281/zenodo.19350847

ISO/IEC 27037:2012. Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. International Organization for Standardization.

Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007).

Melendez-Diaz v. Massachusetts, 557 U.S. 305 (2009).

NIST Special Publication 800-86. 2006. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology.

State v. Kandies, 467 S.E.2d 67 (N.C. 1996).

Uniform Electronic Transactions Act (UETA), adopted in 49 states.

United States v. Bansal, 663 F.3d 634 (3d Cir. 2011).

United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010).

Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y. 2003).