Biometric Evidence Standard

Framework for Verifiable Biometric Governance

Issued by	Clavira Standards Program
Document Type	Evidence Standard
Version	1.0 · March 2026
Applies	Biometric Evidence Standard (BES-1)
Document ID	BES-2026-01

Executive Summary

In litigation, supervisory review, and consumer protection enforcement, biometric programs are increasingly evaluated not only on written policies, but on whether organizations can produce structured, time-ordered records demonstrating what occurred and when.

Policies describe what should happen. Evidence architectures document what did happen, when, and under which declared authority. Operational logs record system activity. BES-1 addresses a separate requirement: the ability to produce structured, time-ordered evidence demonstrating that governance actions occurred in the required sequence and under the declared authority.

BES-1 defines the minimum structural properties required for an evidence architecture to produce reviewable, time-ordered records of biometric governance activity. It defines the structural properties an evidence layer MUST and SHOULD provide to support demonstrability of biometric governance obligations. BES-1 is jurisdiction-agnostic — it does not interpret any specific statute or supervisory guidance, and it is not a product specification. It describes the structural properties that defensible biometric governance typically requires regardless of jurisdiction or sector.

Jurisdictional interpretation guides — including those addressing Illinois and Colorado biometric requirements — and sector interpretations such as financial services supervisory expectations apply BES-1 to specific legal and supervisory contexts. This document establishes the underlying standard those interpretations reference. BES-1 does not interpret any individual statute, regulation, or supervisory rule; companion documents perform that interpretive work for specific jurisdictions or sectors. BES-1 does not convert evidentiary strength, architectural completeness, or control maturity into a legal conclusion of compliance.

This document is provided for informational purposes only and does not constitute legal advice. Organizations should consult qualified legal counsel when designing biometric governance and compliance programs. BES-1 defines an evidence architecture framework; it does not ensure regulatory compliance or confer legal protection.

Normative Language

The key words MUST, MUST NOT, SHOULD, and MAY in this document are to be interpreted as follows:

- MUST / MUST NOT — An absolute requirement (or prohibition) for conformance with BES-1. A BES-aligned evidence architecture that does not satisfy a MUST or MUST NOT clause does not conform to this standard.

- SHOULD — A recommended practice. Deviation is permitted where documented justification exists, but the burden is on the implementing organization to demonstrate an equivalent or superior outcome.

- MAY — An optional mechanism. Implementation is at the discretion of the organization and does not affect conformance status.

This convention follows the usage established in IETF RFC 2119.

Part I: The Structural Problem

1.1 The Shift from Policy to Proof

Across the U.S. regulatory and litigation landscape, biometric governance obligations share a common structure. Across multiple litigation, regulatory, and audit contexts, programs may be expected to evidence:

- Notice before collection
- Consent before enrollment or use (as applicable)
- Purpose limitation throughout the lifecycle
- Retention within defined timeframes
- Deletion upon satisfaction of purpose or expiration of retention windows
- Vendor accountability for downstream processing and disclosure controls

Each of these obligations has a sequencing dimension. The governance question is not simply whether a policy exists. It is whether the right action occurred in the right order at the right time — and whether that chronology can be demonstrated.

In audits, investigations, and discovery, requests often focus on reconstructable chronology: what notice was presented, what was consented to, what occurred, and whether retention and deletion controls executed as represented. Where organizations cannot reconstruct these linkages, exposure increases.

Biometric compliance is increasingly evaluated through demonstrable execution. Organizations should be able to produce time-ordered records showing that required steps occurred in sequence. Written policies remain necessary but are rarely sufficient without evidence of operational implementation.

This is the evidentiary burden BES-1 is designed to address. Organizations that cannot produce structured, reviewable chronology of their biometric governance practices may face increased litigation, supervisory, or documentary risk depending on the applicable regime. In multiple statutory and enforcement contexts, the ability to demonstrate sequencing — rather than the existence of policy alone — can determine whether a violation is found. This shifts biometric governance from a policy problem to an evidentiary problem.

1.2 Why Operational Logs Are Frequently Insufficient

Organizations deploying biometric systems typically maintain operational logs — outputs from SIEM platforms, vendor dashboards, IAM systems, and business applications. These systems were designed for security operations and monitoring. They are not designed to produce compliance-ready evidence.

Operational logs are frequently insufficient without additional integrity controls and lifecycle linkage because they are:

Fragmented. Biometric events, consent artifacts, retention configurations, and deletion actions often exist across separate systems without a unified lifecycle record linking them coherently.

Often mutable under typical administrative controls. Many logging environments permit alteration, deletion, or retention reconfiguration by privileged users without independent integrity controls, which can complicate integrity assertions during audit or discovery. Logging environments with architectural controls — such as message digests, WORM storage, or protected transport — can reduce this risk, but such controls are not present in default configurations across many deployments.

Purpose-agnostic. Logs record that an event occurred. They do not record why it was authorized, under what consent scope it was permitted, or whether it aligned with the purpose disclosed at the time of collection.

Context-light. Operational logs do not consistently encode jurisdictional context, consent model, or the retention rule in force at the time of capture.

Not structured for export as evidence. Logs produce raw records. In audits, investigations, and discovery, requests focus on reconstructable chronology — a need that raw logs alone frequently do not satisfy.

The gap between what operational logs produce and what evidentiary scrutiny demands is not primarily a technology failure. It is an evidence architecture gap. BES-1 defines the structural requirements for evidence that operational logs frequently cannot provide on their own. BES-1 addresses these gaps by producing purpose-bound, timestamped attestations linked across the biometric lifecycle and structured for export as reviewable evidence artifacts.

1.3 The Chronology Risk

A consequence of the evidence architecture gap is chronology risk: the inability to establish, after the fact, that required actions occurred in the required sequence.

Chronology risk is material because remedies and exposure can turn on sequencing and authorization. Illinois courts have treated retention-policy timing as central to the violation analysis: in *Mora v. J&M Plating, Inc.,* 2022 IL App (2d) 210692, the appellate court interpreted BIPA Section 15(a)'s duty as triggered by possession and held that a retention and destruction schedule must exist before or at the time biometric collection begins — later adoption may not cure earlier noncompliance.[1] Under BIPA's private right of action, an organization's failure to satisfy procedural prerequisites can create liability exposure even absent consequential harm to the individual.[2]

Where chronology cannot be demonstrated, organizations may face greater difficulty rebutting claims of improper collection, scope expansion, over-retention, or deficient deletion. Certain statutory frameworks treat failure to satisfy procedural prerequisites as a cognizable injury independent of downstream harm — meaning sequencing failures can create liability exposure without any showing of concrete damage to the individual. This risk is not limited to Illinois. Any regulatory or enforcement framework that imposes sequencing requirements — including consent timing, retention triggers, or deletion obligations — creates similar exposure where chronology cannot be demonstrated. In certain enforcement matters, regulators have required destruction of models or algorithms derived from unlawfully or improperly collected data, in addition to deletion of the underlying data itself.[3]

BES-1 is designed to preserve verifiable chronology throughout the biometric data lifecycle.

[1] *Mora v. J&M Plating, Inc., 2022 IL App (2d) 210692 (Ill. App. Ct. 2022).*

[2] *Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186 (Ill. 2019).*

[3] *See, e.g., In re Everalbum, Inc., FTC File No. 1923172 (2021) (requiring deletion of facial recognition models and algorithms developed using improperly collected biometric data; sometimes referred to in commentary as "algorithmic disgorgement").*

Part II: Core Principles

Principle 1 — Metadata-Only Evidence

A BES-aligned evidence system MUST NOT store biometric identifiers. It MUST NOT retain biometric templates, facial vectors, voiceprints, fingerprint images, or raw scan data within the evidence layer.

Evidence is produced from compliance-relevant metadata: who, what, when, where, and under what declared authority. This supports data minimization while enabling demonstrability.

Principle 2 — Chronological Integrity

Every compliance-relevant event MUST be timestamped at the moment it occurs and preserved in a form resistant to retroactive modification detectable and auditable. Evidence that cannot establish its own timeline is vulnerable to challenge.

Chronological integrity requires attestations generated at the point of the event, not reconstructed later from other system data. This is the Contemporaneous Attestation Principle: evidence records generated before or at the moment of the governed event carry materially stronger evidentiary weight than post-hoc reconstructions. Courts and regulators routinely treat contemporaneous documentation as more reliable than reconstructed narratives, and enforcement scrutiny often focuses precisely on whether records existed at the time of the event rather than being assembled in response to a claim or inquiry.

Principle 3 — Purpose Binding at Point of Capture

Each biometric event MUST be linked, at the moment it occurs — prior to or at the time of collection, not afterwards — to the declared processing purpose, the applicable consent scope reference, and the legal basis category where tracked. A BES-aligned system MUST, prior to any biometric collection or biometric-enabled use event, capture an evidence record showing the applicable consent or authority basis for the use case (e.g., written release, opt-in consent, affirmative express consent, or another documented authority basis where tracked). Failure to bind purpose at the time of the event can create evidentiary gaps where organizations are unable to demonstrate that biometric use remained within the scope disclosed to the individual.

Principle 4 — Lifecycle Verifiability

A BES-aligned evidence architecture MUST produce verifiable records across the biometric lifecycle: notice (where applicable), consent capture, enrollment, operational use, retention clock, and deletion or destruction.

Deletion or destruction is not complete without a verifiable deletion certificate. Deletion or destruction is not complete for evidentiary purposes without a verifiable deletion certificate documenting when the destruction occurred and what trigger initiated it. Where processing involves vendors, the implementer MUST document and enforce contractual deletion obligations and MUST obtain written confirmation of

deletion covering source records and, where applicable, relevant derived work product within the vendor's control. Retention compliance is not demonstrable without a retention schedule that existed upon possession and a retention clock tied to the relevant subject and declared purpose. Lifecycle gaps are difficult to remediate after the fact and may not cure earlier noncompliance.

Principle 5 — Vendor Reconciliation

Biometric governance risk does not terminate at the institutional boundary. Vendors processing biometric data can create shared exposure. Statutory exemptions — including those available to financial institutions under the Gramm-Leach-Bliley Act — are fact-specific; applicability to third-party processors is fact-dependent and should be validated with counsel. Organizations MUST NOT assume that an institutional exemption automatically shields third-party processing.

A BES-aligned evidence architecture SHOULD include the capacity to reconcile vendor-side events against institutional consent scope and retention obligations. Contracts are necessary but do not, on their own, establish that downstream processing remained within authorized scope. Evidence of oversight and reconciliation strengthens defensibility.

Part III: The BES Architecture Model

3.1 Architectural Layers

A biometric evidence system operates across four layers:

Layer 1 — Biometric Systems

Capture devices, authentication engines, behavioral platforms, timekeeping terminals, and identity services. These systems generate the events that governance obligations apply to. They are not replaced or modified by the evidence layer.

Layer 2 — Operational Logs

SIEM records, IAM logs, vendor activity reports, and application logs. These records document system activity but frequently do not satisfy evidentiary requirements independently.

Layer 3 — Integrity Layer

The evidence engine. A metadata-only sidecar operating parallel to existing infrastructure. The integrity layer observes and attests; it neither initiates biometric collection nor determines access outcomes. It generates and preserves compliance-relevant attestations without storing biometric identifiers or replacing underlying systems. The integrity layer operates without modifying or interrupting underlying biometric system behavior, preserving separation between operational decision-making and evidentiary recording.

Layer 4 — Proof Artifacts

Structured, exportable evidence packages suitable for regulatory examination, internal audit, investigations, or legal discovery.

The integrity layer (Layer 3) does not replace Layers 1 or 2. It provides the evidence architecture that Layers 1 and 2 frequently cannot provide on their own.

3.2 The Four BES Integrity Primitives

BES-1 defines four integrity primitives that constitute the functional building blocks of a conformant evidence architecture. These terms are used consistently across all Clavira regulatory interpretations and operational guides. These primitives define how evidence is generated, preserved, and exported. Each primitive addresses a distinct evidentiary requirement: event capture, integrity assurance, exportability, and cross-system validation.

Primitive 1: Event Attestation

Event Attestation is the atomic unit of evidence within a BES-aligned system. A cryptographically bound metadata record generated at the moment of a biometric-related governance event — prior to or at the time of the governed event, not reconstructed afterwards. Each attestation captures (at minimum):

- Subject identifier (non-biometric reference)
- Provider or device identifier
- Event type (e.g., notice presented, written release or affirmative express consent captured, enrollment, operational use, deletion or destruction)
- Exact timestamp
- Regulatory context identifier (if tracked internally)
- Consent or authority reference (e.g., written release, opt-in consent, affirmative express consent, opt-out pathway where legally relevant, or another documented authority basis as applicable)
- Declared processing purpose
- Retention period (time-to-live), expressed as a concrete window tied to a defined trigger
- Policy, retention schedule, and notice version identifier in effect at the time of the event

Event Attestation is the foundational evidence primitive. All other primitives depend on the integrity and completeness of attested events. Evidence records generated before or at the moment of the governed event carry materially stronger evidentiary weight than post-hoc reconstructions.

Primitive 2: Anchor to Ledger (ledger anchoring)

The strength of tamper-evidence depends on the ledger model, anchoring cadence, and key management practices, and should not be treated as uniform across implementations. An optional tamper-evidence mechanism. A cryptographic hash of one or more attested events is recorded on an append-only ledger — internal, private, or public — creating an externally verifiable timestamp checkpoint.

Ledger anchoring MAY strengthen integrity claims by making retroactive modification of those records externally detectable, depending on the threat model, ledger type, and anchoring process. See Part X (Threat Model) for scope of tamper-evidence claims.

Important qualification: Ledger anchoring is not a compliance mechanism and does not independently establish legal admissibility. For use in legal proceedings, ledger evidence typically requires authentication and a hearsay pathway where applicable. Foundation may be provided through qualified witness testimony explaining system architecture, hash generation, and ledger properties, or through certification mechanisms for electronic records where applicable. Without proper foundation, ledger records may face admissibility challenges.

Primitive 3: Proof Bundle

Proof Bundles represent the primary format in which evidence is presented during audits, regulatory inquiries, or legal discovery. A structured, exportable evidentiary artifact consolidating, for a defined and limited scope (such as subject, event type, or time period), the chain of compliance-relevant attestations — retaining records necessary to demonstrate how sequencing, retention, and deletion provisions were operationally implemented for the scope in question. A Proof Bundle includes:

- Notice artifact reference (where applicable)
- Consent receipt (timestamped written release or affirmative express consent record linked to notice and policy version)
- Enrollment record linked to consent, generated prior to or at the moment of collection
- Operational use events linked to declared purpose and consent scope
- Retention schedule version and retention clock context in effect at the time of collection
- Deletion certificate (verifiable deletion or destruction event record, including written confirmation of deletion where vendors are involved)
- Derived work product deletion confirmation (where applicable)
- Vendor disclosure log references (where applicable)
- Ledger verification references (where ledger anchoring was used)

Proof Bundles SHOULD be available in human-readable PDF for auditors and legal discovery, and in structured CSV/JSON where technical analysis or SIEM ingestion is required.

Proof Bundles MUST NOT contain biometric identifiers, templates, raw scans, or reversible biometric representations.

Proof Bundle exports MUST default to least-privilege scopes — exporting only the records necessary to satisfy the specific request.

Primitive 4: SIEM Reconciliation

SIEM Reconciliation functions as a drift-detection mechanism, identifying discrepancies between recorded governance events and observed system activity. Ongoing cross-verification between operational logs (Layer 2) and the attested event record (Layer 3), retaining records necessary to demonstrate full compliance with sequencing, retention, and deletion provisions. Designed to detect:

- Operational biometric events without a prior or contemporaneous attestation of notice and consent (potential pre-collection gate failure)
- Consent records with no subsequent biometric events (where relevant)

- Retention schedule violations — data remaining beyond the documented retention window without a documented exception
- Deletion or destruction failures, including missing written confirmation from vendors
- Derived work product not accounted for in deletion records
- Vendor disclosures not reflected in governed disclosure records

SIEM Reconciliation SHOULD be configured to surface discrepancies in near-real-time rather than only at examination. Alert thresholds and resolution workflows SHOULD be documented and reviewed periodically.

Part IV: Regulatory Expectation to Evidence Mapping Model

The following table maps regulatory expectations to evidence requirements and BES-1 mechanisms. This table is referenced in jurisdictional interpretation guides to connect specific governance obligations to the evidence architecture that addresses them.

This table serves as the canonical mapping model linking regulatory expectations to evidence artifacts and BES-1 primitives.

Regulatory Expectation	Evidence Typically Required	BES-1 Primitive	Output Artifact
Consent obtained before collection	Timestamped consent record linked to enrollment event	Event Attestation	Consent receipt / manifest
Notice provided before consent	Versioned notice identifier preserved at time of presentation	Event Attestation	Notice artifact
Purpose limitation throughout lifecycle	Purpose declaration linked to each use event at time of occurrence	Event Attestation	Purpose-bound event log
Retention within statutory limits	Documented TTL and deletion execution	Lifecycle tracking + SIEM Reconciliation	Deletion certificate (verifiable deletion event record)
Vendor accountability	Evidence of permitted disclosures; reconciled vendor logs	SIEM Reconciliation	Disclosure log
Tamper-evident record integrity	Immutable chronological timeline	Anchor to Ledger (optional)	Verifiable event timeline
Audit and discovery response	Structured, exportable evidentiary record	Proof Bundle	Human-readable PDF; structured CSV/JSON

Part V: Applicability Scope

BES-1 abstracts structural evidentiary expectations from multiple legal, regulatory, and supervisory contexts, but it does not itself determine the applicability or meaning of any specific authority. It is jurisdiction-agnostic and may be applied to biometric governance programs operating under, among others:

- **Illinois Biometric Information Privacy Act (BIPA)**, 740 ILCS 14, particularly with respect to the notice-consent-collection sequencing requirements of Section 15(b) and the deletion obligations of Section 15(a)
- **Colorado House Bill 24-1130** (Colo. Rev. Stat. § 6-1-1314), effective July 1, 2025,[4] particularly with respect to written retention policy requirements, opt-in consent obligations, annual review obligations, and deletion controls
- **Federal Financial Institutions Examination Council (FFIEC)** authentication guidance, as it relates to audit logging, monitoring, and vendor oversight expectations for biometric authentication systems in financial institutions
- **Federal Trade Commission** enforcement authority under Section 5 of the FTC Act, particularly as applied to biometric data practices involving consent, retention, and misrepresentation. Enforcement orders have required destruction of algorithms and models derived from unlawfully collected data, in addition to deletion of the underlying data
- **Consumer Financial Protection Bureau** UDAAP authority, as potentially relevant to the security and transparency of consumer data in financial services contexts. This is an inference from broader CFPB consumer-finance and data-security posture rather than a biometric-specific CFPB rule, and it should be treated as requiring verification. This interpretation requires verification against primary-source guidance.
- **Emerging or existing biometric privacy** requirements in Texas, Washington, and other jurisdictions with biometric-specific or biometric-relevant privacy frameworks. Applicability of specific provisions requires primary-source verification.

Each companion document explicitly applies BES-1 to its jurisdiction or use case and should be read as an interpretation or implementation guide, not as an alternative standard.

[4] Colorado General Assembly, HB24-1130 (enacted 2024), codified at Colo. Rev. Stat. § 6-1-1314, effective July 1, 2025.

Part VI: Implementation Scope and Constraints

A biometric evidence system implementing BES-1 MUST operate within the following structural constraints. These constraints ensure that the evidence layer operates as a non-decisional, metadata-only system that does not alter biometric system behavior:

Sidecar architecture. The integrity layer MUST operate parallel to existing biometric systems without modifying capture devices, authentication engines, or operational log infrastructure. The integrity layer observes and attests; it neither initiates biometric collection nor determines access outcomes. Inline modification of existing systems is outside BES-1 scope.

Metadata-only footprint. The integrity layer MUST NOT retain biometric identifiers, templates, facial vectors, voiceprints, or raw scan data. All evidence is derived from compliance-relevant metadata exclusively.

Non-decisional. The integrity layer MUST NOT make authentication decisions, access control decisions, or identity verification decisions. Those functions remain within existing biometric systems.

Export integrity. All Proof Bundle exports MUST be logged, including the identity of the requester, the time of export, and the scope of data exported. Exports MUST be restricted to authorized roles.

Export minimization. Proof Bundle exports MUST default to least-privilege scopes. Exports SHOULD include only the records necessary to satisfy the specific request, not full population data.

Role-based access. Access to the evidence layer, attested records, and export functionality MUST be controlled and audited.

Corrective-action handling. Where material evidence gaps, reconciliation failures, or export-control failures are identified, the implementation SHOULD maintain a documented corrective-action path covering triage, owner assignment, remediation, retest, and closure.

Part VII: Limitations of the Standard

BES-1 defines an evidence architecture framework. It does not represent a legal compliance guarantee. The following limitations apply and must be understood by organizations implementing or evaluating a BES-1-aligned system:

BES-1 does not ensure regulatory compliance. Evidence architecture supports demonstrability. It does not substitute for implementing the underlying obligations — valid consent, lawful purpose, compliant retention, and timely deletion. If an organization fails to obtain consent, an attested record of that absence does not create compliance.

BES-1 does not replace legal counsel. Jurisdictional interpretation requires qualified legal analysis. Organizations must consult counsel when designing biometric governance programs.

BES-1 does not validate biometric accuracy or bias. The standard addresses governance evidence, not biometric system performance. Accuracy testing, bias assessment, and model validation are outside BES-1 scope.

BES-1 does not itself prevent misuse of biometric systems. It documents whether required governance actions were taken. It cannot prevent unauthorized use that is not surfaced through SIEM Reconciliation.

Ledger anchoring does not independently establish legal admissibility. Authentication and a hearsay pathway are required for ledger records to be used in legal proceedings. Anchoring enhances tamper-evidence; it does not satisfy evidentiary foundation requirements.

BES-1 records what occurred; it does not certify that what occurred was lawful. That determination rests with counsel, regulators, and courts.

BES-1 compatibility with a standards framework or control model does not, by itself, create legal obligation or establish compliance with that framework.

Part VIII: Governance and Verification

These governance practices support ongoing verification that the evidence architecture remains complete, accurate, and reviewable over time. Organizations operating biometric programs aligned with BES-1 SHOULD incorporate the following governance practices:

Control owner assignment. Legal, Privacy, and Security/IT functions SHOULD each have defined ownership and escalation paths for biometric evidence architecture oversight. Responsibility for maintaining integrity of attested records, responding to audit inquiries, and managing export requests SHOULD be explicitly assigned.

Annual attestation. Legal, compliance, and technical leadership SHOULD jointly attest, on at least an annual basis, that biometric evidence architecture practices align with documented policies, applicable legal requirements, and BES-1 integrity primitives. Attestation records SHOULD be retained.

Quarterly Proof Bundle testing. A representative sample of Proof Bundles SHOULD be exported and reviewed quarterly to verify completeness, accuracy, and format suitability for regulatory examination.

Export-scope review. Periodic review SHOULD confirm that exported Proof Bundles remain limited to the records necessary for the specific request, inquiry, or test case.

Ledger verification testing (where applicable). Where Anchor to Ledger is implemented, cryptographic hash validation and timestamp accuracy SHOULD be verified on a quarterly basis. Test results SHOULD be documented.

Retention clock audit. Periodic review SHOULD confirm that retention configurations reflect documented retention schedules and that deletion jobs are executing within required timeframes.

SIEM Reconciliation review. Alert thresholds, drift detection rules, and reconciliation logs SHOULD be reviewed and validated periodically to confirm the evidence layer remains synchronized with operational systems.

Corrective-action review. Where discrepancies or control failures are identified, remediation steps, retest results, and closure records SHOULD be documented and retained.

Part IX: Conformance

An implementation conforms to BES-1 if it satisfies all MUST and MUST NOT statements in this document.

Implementations that satisfy a subset of MUST/MUST NOT statements MAY represent their status as **“BES-1 Informed”** but MUST NOT represent their status as **“BES-1 Conformant.”** Organizations claiming BES-1 conformance SHOULD be prepared to document how each MUST and MUST NOT clause is satisfied.

Conformance is assessed against the version of BES-1 current at the time of implementation. Organizations SHOULD document which version they have assessed against. Documents or implementations that describe themselves as “BES-1 Informed” or “BES-1 Conformant” MUST NOT imply that BES-1 itself determines legal compliance.

Part X: Threat Model

BES-1's tamper-evidence mechanisms — particularly Anchor to Ledger — are designed to address a specific, bounded set of threats. Understanding this scope is necessary for accurate representation of what the evidence architecture provides.

Threats within scope:

- Retroactive modification of attested event records by internal administrators or privileged users
- Post-hoc reconstruction of consent or purpose records to cure earlier compliance gaps
- Disputes over whether a specific event occurred or when it occurred
- Vendor disagreements over whether disclosed processing occurred within contracted scope

Threats outside scope:

- Fraud at the point of capture (e.g., false consent inputs, fabricated subject identifiers at enrollment time)
- Compromise, loss, or misuse of cryptographic keys used to generate attestation records
- Errors or misrepresentations introduced into the evidence layer before attestation occurs
- Systemic failures in the underlying biometric system that the integrity layer is not positioned to detect

The tamper-evidence value of Anchor to Ledger depends on the threat model, ledger type (public vs. private), anchoring cadence, and key management practices. Implementations using private ledgers carry different trust assumptions than those using public ledgers and SHOULD document those assumptions explicitly.

BES-1 does not claim to solve fraud at capture time. It claims to preserve integrity of what was recorded after capture occurred.

Implementations that rely on cryptographic attestation SHOULD document key-custody, rotation, and recovery assumptions in supporting implementation materials.

Part XI: Definitions

The following terms are used with specific meanings throughout this document.

Append-only ledger. A data structure or system in which records can be added but not modified or deleted after creation, used to provide tamper-evidence for attested events.

Attestation. A cryptographically bound metadata record generated at the time of a biometric-related governance event, documenting who, what, when, where, and under what declared authority the event occurred. Attestations do not contain biometric identifiers.

Biometric data. One or more biometric identifiers used for identification purposes. Definition varies by jurisdiction; organizations should verify applicable statutory definitions.

Biometric identifier. A measurable biological or behavioral characteristic used for automated recognition, including but not limited to fingerprint, facial geometry, iris, voiceprint, and hand geometry. Definition varies by jurisdiction; organizations should verify applicable statutory definitions.

Contemporaneous Attestation Principle. The evidentiary principle that records generated before or at the moment of a governed event carry materially stronger weight than records reconstructed after the fact. BES-1 requires attestations to be generated at the point of the event in application of this principle. Post-hoc reconstruction of consent records, retention policies, or deletion evidence is treated as lower assurance throughout this standard.

Deletion certificate. A verifiable deletion event record attesting that a biometric identifier or associated record was deleted or destroyed within the required timeframe and in accordance with a documented retention schedule and destruction guidelines. Where processing involves vendors, a deletion certificate SHOULD include or reference written confirmation of deletion from the vendor covering both source records and derived work product. In high-risk contexts, implementations MAY support sworn written statement formats — this is an optional mechanism for situations where heightened proof of destruction is warranted, and does not reflect a universal BES-1 requirement for sworn attestations.

Derived work product. Data, models, or algorithms derived in whole or in part from biometric identifiers or biometric-enabled system inputs. In some legal or enforcement contexts, deletion or remediation obligations may extend to derived work product within the implementer's control. Where that risk is relevant, implementations should preserve records sufficient to document whether derived work product was addressed.

Destruction guidelines. Documented procedures specifying the method and timing for permanently destroying biometric identifiers and associated records. Destruction guidelines MUST exist upon possession of governed biometric data and MUST be versioned and auditable. Later adoption of destruction guidelines is not equivalent to guidelines that existed at the time of collection.

Evidence artifact. A structured record or document — such as a consent receipt, notice artifact, or deletion certificate — that can be produced to demonstrate that a governance action occurred.

Ledger. An append-only record store used to anchor cryptographic hashes of attested events for tamper-evidence purposes. May be implemented as a public blockchain, private distributed ledger, or governed append-only database.Implementations should document the trust assumptions associated with the chosen ledger model.

Notice artifact. A record attesting that required pre-collection disclosures were presented to the subject, including the version of the notice presented and the timestamp of presentation.

Policy version identifier. A unique reference to the version of a written policy or notice in effect at the time of a given biometric event, enabling reconstruction of what governance framework applied at that moment.

Proof Bundle. A structured, exportable evidentiary artifact consolidating attestations, consent records, retention lifecycle events, and deletion confirmations for a defined subject, event type, or time period. Proof Bundles do not contain biometric identifiers.

Regulatory context identifier. An internal metadata tag identifying the jurisdictional or regulatory context applicable to a given biometric event (e.g., Illinois resident / BIPA, Colorado resident / HB 24-1130). Used for routing retention and deletion rules; not a legal interpretation.

Retention clock. A time-to-live counter associated with a biometric event or subject record, tracking the elapsed time since collection or last interaction and triggering deletion workflows upon expiration.

Subject identifier (non-biometric). A reference identifier for the individual associated with a biometric event that does not itself constitute or encode a biometric characteristic. Used to link governance records without retaining biometric data.

WORM (Write Once Read Many). A storage configuration in which data, once written, cannot be modified or deleted, used to enforce immutability in logging and evidence systems.

Part XII: Relationship to Clavira's Evidence Infrastructure

Clavira is a reference implementation of the BES-1 framework: a metadata-only sidecar integrity layer designed to operate alongside existing biometric systems and vendors, IAM platforms, and SIEM infrastructure.

Clavira's implementation produces the four BES-1 integrity primitives — Event Attestation, Anchor to Ledger, Proof Bundle, and SIEM Reconciliation — as operational outputs within one implementation model. Proof Bundles are exportable in human-readable PDF for auditors and legal discovery, and structured CSV/JSON for technical analysis and SIEM ingestion.

Clavira does not collect biometric identifiers, store biometric data, make authentication decisions, or guarantee regulatory compliance. It provides the evidence infrastructure that supports organizations in demonstrating how their biometric programs operated when questions arise.

Clavira is a reference implementation of BES-1. The standard is designed to be implementable by any evidence architecture that satisfies the primitives and constraints defined herein.

Conclusion

Biometric governance is increasingly evaluated through an evidentiary lens. Courts, regulators, and auditors increasingly focus not only on what an organization intended to do, but on whether it can demonstrate what occurred — with specificity, chronological integrity, and artifacts that survive scrutiny. Operational logs, vendor dashboards, and policy documents are not structured for that purpose. They describe system activity. They do not produce compliance evidence.

The Biometric Evidence Standard defines the architecture that bridges that gap: a metadata-only integrity layer that generates Event Attestations, optionally anchors them to tamper-evident ledgers, produces exportable Proof Bundles, and maintains ongoing SIEM Reconciliation between the evidence record and operational reality. The evidentiary question is not whether systems were designed correctly, but whether their operation can be demonstrated under scrutiny. A proof layer does not replace controls. It can make controls more reviewable and more defensible.

Companion Documents

Each companion document explicitly applies BES-1 to its jurisdiction or use case and should be read as an interpretation or implementation guide, not as an alternative standard.

- Illinois BIPA — Evidence Interpretation Guide (2026)
- Colorado HB 24-1130 — Evidence Interpretation Guide (2026)
- Biometric Authentication in Financial Services — Federal Regulatory Interpretation (2026)
- Biometric Audit Trail Documentation — Operational Guide (2026)
- BIPA Evidence Readiness Checklist (2026)
- Colorado HB 24-1130 Evidence Readiness Checklist (2026)