ICS | Institute of Contaminant Standards

HEAVY METALS SPECIAL REPORT / LABORATORIES

Verifiable laboratory evidence with TECRID

Authority, scoped disclosure and correction history in an ICS proposed adoption method

Version 1.0.1 | Published 9 November 2026 | Evidence cutoff 2026-11-09

A practical evidence review and adoption guide for decision-makers. Public sources, explicit limitations, and tools that can be put to work.

Institute of Contaminant Standards is the institutional publisher and is affiliated with the ecosystem discussed in this report. See the disclosure and methods sections.

Free HTML edition and current PDF: https://contaminantstandards.com/articles/tecrid-verifiable-laboratory-evidence

Publication package SHA-256: dc91757dbf2a4f2c52cc8f22e2ec21e23dc33f526cba451e083f7a1f899213e8

Contents

Executive summary 3

01 Make the laboratory claim checkable at its source 3

02 Authentication, conformance and public disclosure are separate 4

03 What is available, and what was not tested 5

04 Laboratory onboarding: authority precedes production issuance 6

05 Brand and supplier onboarding: private intake is not issuance 7

06 Recipient onboarding: request a defined package 7

07 Permissions and correction history require explicit choices 8

08 Worked hypothetical: a corrected supplier report 9

09 Measure the workflow and its failure paths 9

10 Choose the entry route and keep the scope visible 10

References 11

Read the executive summary first. Use the operational sections as working templates. The references resolve the evidence behind the report; the methods state the limits of the search.

Executive summary

A laboratory result becomes more useful when recipients can check its issuer, exact record and current status without losing control of confidential findings. TECRID describes a signed, versioned evidence registry with recipient-specific disclosure. Authentication remains separate from sampling quality, safety and compliance. This companion sets out the published role and technical boundaries, current production limitations, and an ICS proposed method for a narrow authorized pilot. It includes laboratory, controller and recipient checklists, a fictional correction example and measures for testing operational value. No production issuance, independent security result or measured benefit is asserted. [1],[2],[3]

01 Make the laboratory claim checkable at its source

A laboratory report can become difficult to evaluate after it moves through several organizations. A recipient needs to know who issued it, whether the values and context are intact, whether a correction exists and whether the recipient is entitled to the findings. Those are evidence-management questions before they are safety questions. A plausible-looking document or a familiar laboratory logo does not by itself resolve them.

TECRID means Test Evidence Credential Record Identifier. The public service describes a persistent identifier for a laboratory-issued evidence record, with issuer provenance, status and preserved versions. Its technical materials document Ed25519 signatures and SHA-256 fingerprints. That is the supported cryptographic model: a laboratory signs a defined record and the registry verifies it against reviewed authority. No blockchain claim is needed to explain the design. [1],[2]

The intended practical benefit is governed reuse of the same source evidence across authorized recipients. A laboratory should not have to reconstruct every verification by email, and a recipient should not have to infer provenance from a detached screenshot. Those are reasonable operational aims, not measured outcomes established by this report. The proposed adoption method below tests them against a limited workflow and keeps the organizations' technical decisions separate from authentication.

A result becomes useful through a complete control chain



ICS proposed operational workflow; authentication alone does not establish safety.

Conceptual TECRID evidence chain: laboratory authority and sample context, signed record, persistent identifier and version history, authorized recipient package, and a separate recipient decision. Authentication does not establish sample representativeness, safety, legal compliance or certification. [1],[4]

02 Authentication, conformance and public disclosure are separate

A signature answers a defined integrity and origin question about a signed record. It cannot establish that a submitted sample represented a commercial lot, that a method was appropriate for every intended use or that the measured result meets a particular legal or certification rule. TECRID's public materials make those limits explicit. The recipient still needs a suitable decision rule, sufficient context and the authority to make the decision. [1],[4]

ICS proposed review map. Different questions require different evidence and accountable decision-makers.

Question	Relevant evidence	Remaining decision
Who issued this record?	Reviewed issuer identity, key and signature	Does the issuer's approved scope fit the requested work?
Has this record changed?	Fingerprint, version and current status	Does a correction affect the decision already made?
Which findings may this recipient receive?	Controller's recipient-specific grant and scope	Is this access sufficient and appropriate for the stated purpose?
Does this material meet a requirement?	Sample identity, method, result and applicable criterion	An authorized technical or program reviewer determines conformance.

Question	Relevant evidence	Remaining decision
Is the underlying report public?	Separate publication authority and disclosure state	Knowing an identifier does not create public disclosure rights.

This distinction also matters when TECRID is discussed with HMTc or VLE. A laboratory credential is not a product certificate or a qualified-lot claim. HMTc's current public verification page shows a pending lookup and a specimen rather than an issued certificate. VLE's current workflow says production TECRID authentication and laboratory ordering are not connected. A future integration should name each achieved step instead of allowing the presence of an identifier to imply the entire chain is operating. [5],[6]

The same discipline applies to public communications. A brand may accurately say that an authorized laboratory record can be checked, where that is true, without claiming universal product safety. A recipient may say it reviewed a specified evidence package without claiming that the laboratory approved the recipient's final interpretation. A short, scoped statement is more useful than a broad assurance that the record itself cannot support.

03 What is available, and what was not tested

The public TECRID site offers role-specific entry pages, API documentation, private-report intake information, an explained sample workflow and workspace setup. It describes the documented API routes as implemented. This report inspected those public descriptions and matching local source boundaries, but did not enroll a laboratory, approve authority, issue a production credential, upload a private report or create a recipient grant. Implemented documentation is not independent proof that a particular organization's production integration has completed. [2],[7],[8]

The commercial entry is unusually clear: the core registry is offered without a subscription to laboratories, brands, suppliers, certifiers, retailers and government programs. Optional paid implementation support helps configure a workflow; it cannot purchase issuer approval, a different verification result or a stronger evidence record. An adoption team should choose its support level separately from its evidence acceptance rules. [9],[10]

A responsible first objective is therefore a bounded authorized pilot, not an announcement of institution-wide transformation. Name one report stream and one receiving use. Establish the relevant parties, their roles and their disclosure authority. Review the public contracts, then test what the specific implementation actually does. Record the environment clearly so a fictional credential or a successful sandbox exercise is never presented as production evidence.

Success should be defined in terms the organization can verify: the correct issuer and record resolve, the intended recipient receives only the authorized scope, the reviewed version can be recovered and a correction produces the expected review action. These conditions are proposals for acceptance testing. They are not a representation that every organization can achieve production issuance on the day it creates an account.

04 Laboratory onboarding: authority precedes production issuance

TECRID describes five separately reviewed production gates: legal identity and authority, competence evidence, approved scope, key control and signing conformance. A laboratory workspace does not itself confer production issuance authority. The published laboratory workflow reserves an identifier, renders it in the final report, fingerprints that completed document, prepares and signs the canonical record, and finalizes issuance. Accreditation evidence and method scope remain distinct from the registry's own authentication function. The current FAQ describes ISO/IEC 17025 accreditation with relevant scope and commercial approval before production, while the developer page also refers to comparable competence evidence. A laboratory should confirm its applicable admission conditions with the registry before planning production issuance. [2],[7],[10]

ICS proposes that a laboratory begin with one released-report template and a named laboratory owner. The owner should decide when the result becomes final, which source system supplies identifiers and which staff can authorize a correction. The technical implementer should identify where signing occurs without moving private key material into an ordinary project ticket or a recipient's system. A sandbox can rehearse the sequence while the laboratory prepares its actual authority evidence.

• Choose one matrix and report workflow whose identity fields are well understood. Document the intended scope before attempting to generalize to other sites, methods or customer programs.

• List the fields the laboratory will sign, including report reference, sample identity, dates, methods, units, qualifiers and document reference. Mark missing context as missing rather than inventing a value for a required-looking field.

• Assign custody of the reviewed signing key and a separate process for staff authorization. A person allowed to edit a customer contact list should not automatically gain authority to release a laboratory credential.

• Rehearse a correction and a revocation before the first production issuance. Confirm who approves the reason, how the new version is identified and how affected customer decisions are located.

• Keep the production authorization decision visible. Passing a software test, paying for implementation and completing an account form are separate events from issuer review.

The laboratory can then assess a concrete operational proposition: whether a recipient can independently resolve the issued record and reduce repetitive source-verification requests. Measure those requests before and after the pilot. A lower number of calls may be useful, but it should be reported with report volume and customer mix; otherwise a quiet period could be mistaken for an effect of the system.

05 Brand and supplier onboarding: private intake is not issuance

The brand/supplier entry describes a portfolio organized by product and lot, private historical-report intake and laboratory confirmation. Uploading a PDF does not create a laboratory-issued TECRID. The named laboratory must claim or confirm the report through the appropriate authority process before it is represented as laboratory-issued evidence. That distinction is essential when an organization starts with a large archive of forwarded or renamed documents. [8]

An ICS proposed first step is to inventory one product line's reports without publishing them. Retain the original filenames and report references, but add a separate internal mapping to product, SKU and lot. Record the source of that mapping and any ambiguity. Do not rewrite the laboratory's sample description simply to make it match an internal product catalog. A catalog association can be corrected without pretending that the laboratory originally issued different words.

For each report, decide who can authorize disclosure and what the intended recipient actually needs. A retailer reviewing one product may need a narrow scope rather than the brand's complete analytical portfolio. A certifier may need a frozen evidence package for a program decision. A public QR disclosure is another separate choice. Record the purpose and expiration alongside the recipient, and review the grant when the commercial or program relationship changes.

The pilot should preserve a distinction between the underlying laboratory record and the organization's derived analysis. A brand can create a trend view or a sourcing summary, but a reviewer should be able to return to the exact contributing records. The summary should identify inconsistent methods, bases or units as a review issue instead of presenting every number as directly comparable. The proposal is a traceability control, not an automatic scientific interpretation engine.

Begin with an exception ledger: unconfirmed issuer, ambiguous product mapping, missing original, unresolved basis, obsolete version, denied permission or insufficient scope. Give each exception an owner and next action. Completion means a documented disposition, which may be that evidence remains unavailable. It does not require turning every historical report into a credential or making every private result public.

06 Recipient onboarding: request a defined package

TECRID's recipient entry describes requests with a defined SKU and result scope, validation of authority and preservation of the version relied on. The brand or supplier controls each grant, and the recipient applies its own program criteria. The documented API also describes frozen packages and receipts. These mechanisms can support evidence intake; they do not make an approval decision for a retailer, certifier or government program. [2],[4]

An ICS proposed recipient intake specification should state the program, product identity, required evidence scope, allowable formats, purpose and review owner. Specify what happens when the incoming record does not match the request. For example, an authentic report with a missing lot identifier may be retained as

background while remaining unacceptable for a lot-specific release. A transparent exception is preferable to acceptance based only on the fact that the signature passed.

Create a decision reference that records which package was reviewed, which criteria were applied and who approved the outcome. Keep the evidence receipt separate from the approval record. The receipt establishes an exchange event; it does not show that a person understood the result or that an automated rule was appropriate. If review is automated, retain the rule version and a route for an authorized exception decision.

The recipient should test access boundaries with the controller before relying on the workflow. A request for narrower evidence must not return a broader private payload. A recipient should not gain access because another organization used the same identifier. If the grant expires or is withdrawn, the organization should know what future requests will fail and which previously received records it must retain under its own policies. Review those expectations in advance rather than at the first dispute.

07 Permissions and correction history require explicit choices

TECRID's privacy policy distinguishes private intake, controlled credentials and intentional public release. Knowing the identifier, requesting evidence or paying the operator does not allow a requester to make a private record public. Publication and recipient grants are separate authorized choices. Lawful confidential disclosure is also distinct from public publication. These are the published governance rules; this report is not an independent security audit. [3]

For practical adoption, use a permission register that identifies the controller, recipient, purpose, fields, product/lot scope, expiry and withdrawal route. Record who approved the grant and where that authority came from. If a buyer forwards a private package internally, its own access policy should govern that onward use. The registry cannot replace every recipient's information-management responsibilities.

Correction and revocation are two different lifecycle events to rehearse. A correction can preserve an earlier version while supplying the amended record. A credential revocation can change its current status. Grant withdrawal can stop future delivery to a recipient. None of these can erase a PDF, screenshot or package already downloaded and relied upon. TECRID's public recipient materials state that limitation explicitly. [4],[7]

An ICS proposed correction plan should therefore name both a technical action and a decision action. The technical action identifies the changed status or version. The decision action finds the affected purchases, reviews or claims, assigns an owner and records whether a new decision is needed. Receiving an update without acting on it is not the same as maintaining a current decision. Conversely, an update should not silently rewrite the evidence basis recorded for a past decision.

The organization should also decide how it handles an unavailable status service. Record the time of the last successful check and route the case for review under its own policy. Do not invent current status from an old favorable screenshot. This is a proposed operational fallback, not a promise of a particular service uptime or an instruction that every outage requires the same purchasing action.

08 Worked hypothetical: a corrected supplier report

Hypothetical example

This fictional ICS exercise uses invented organizations and events to show the decision trail. It reports no real laboratory issuance, sample result, certification or buyer outcome.

A supplier, Cedar Ingredients, has an existing laboratory report for ingredient Lot C-17. A retailer, Harbor Retail, needs evidence for a defined product application. The supplier first places its report in private intake. The ledger records that it is awaiting laboratory confirmation, so Harbor does not treat an uploaded file as an authenticated credential. The supplier identifies its authorized evidence controller and agrees on a narrow recipient scope.

After the fictional laboratory completes the required authority process, it issues the appropriate record. The supplier grants Harbor access for the stated product and purpose. Harbor receives a package, records its version and fingerprint, and performs its own review against its program criteria. The exercise does not assume that authentic evidence must pass. If the report lacks information necessary for the program, Harbor records an exception and asks for the missing context.

Later, the laboratory discovers that a sample description needs correction. It issues a signed new version with an explanation. The earlier reference remains part of the historical trail. Harbor's monitoring owner identifies the decision that used the earlier package and asks whether the change affects that decision. Procurement sees the resulting disposition rather than merely seeing that a new document exists.

Suppose Cedar then withdraws Harbor's future grant at the end of the relationship. Harbor can no longer use that grant to obtain new deliveries, while its previously received evidence remains subject to its retention and use obligations. The withdrawal does not make the old decision disappear or turn the private evidence into public material. The fictional scenario is successful when all parties can explain those boundaries, including what they can no longer access.

The useful pilot output is a complete trail: intake state, issuer authority, authorized grant, received version, recipient decision, correction response and grant withdrawal. Each event answers a different question. A project that demonstrates only initial issuance has not yet demonstrated correction monitoring, recipient isolation or the handling of already received records. These should be separate acceptance items in the implementation brief.

09 Measure the workflow and its failure paths

ICS proposes a small comparison using a clearly defined report stream and a comparable historical or parallel process. Record the baseline workload before announcing a benefit. Candidate measures include time spent verifying issuer provenance, manual transcription steps, unresolved identity exceptions, number of repeated document requests and time needed to identify decisions affected by a correction. These are proposed measures; no measured improvement is reported here.

ICS proposed pilot acceptance matrix. Test cases should be authorized and clearly separated from production claims.

Pilot test	Expected evidence	What success does not prove
Correct issuer and record	Reviewed authority plus matching signed evidence and identifier	Sampling quality or conformance to every recipient rule.
Scoped delivery	Named recipient receives only approved fields and record scope	Permission for unrelated recipients or public release.
Current-version review	Reviewer can identify current status and preserve historical reliance	That every prior decision automatically updates correctly.
Correction rehearsal	Affected package and decision owner can be located	A fixed turnaround for every real laboratory or recipient.
Withdrawal rehearsal	Future access changes as intended and retention limits remain explicit	Erasure of downloaded copies.

Report both successful and failed cases, the number of records in scope and time spent waiting for other organizations. A reduction in data-entry time may coexist with a slower first-time issuer review. A rise in exceptions may indicate that the new process is finding problems the old one missed. Interpret each measure on its own terms before making an overall efficiency claim.

At pilot closeout, retain a short implementation report with the workflow boundary, environments, roles, acceptance evidence, unresolved dependencies and named operational owner. Specify what can now be used in production and what remains a demonstration. This report should support a concrete go/no-go decision; it should not turn an incomplete experiment into a marketing claim about fraud elimination, safety, universal compliance or legal protection.

10 Choose the entry route and keep the scope visible

Laboratories should start with the issuer role page and its linked setup pack, then complete authority review before production issuance. Brands and suppliers should start with one product line and a private report inventory. Certifiers, retailers and government programs should first define the receiving criteria and review owner. Technical teams should read the API contract alongside the permission and correction plan. The free core is the common starting point; paid implementation is an optional support choice.

Laboratories: review the issuer workflow

Brands and suppliers: start a governed evidence portfolio

Certifiers, retailers and government programs: define recipient intake

Technical teams: inspect the API contracts

Choose a free role-specific workspace entry

Review privacy, grants and disclosure rules

Evidence cutoff is November 9, 2026. Sources are operator-published role pages, technical documentation, governance and public availability surfaces. No private findings were used. No external account mutation or production transaction was performed. Public descriptions support a defined design and entry path; they do not establish adoption volume, independent security certification, availability guarantees or measured operational benefit.

ICS publishes this companion and operates TECRID and related resources under disclosed institutional relationships. It is therefore affiliated institutional guidance, not independent third-party endorsement. HMI's public literature role remains outside the private evidence path. The checklists, hypothetical scenario and pilot measures are original ICS proposals for accountable implementation. Their effectiveness should be evaluated through authorized use, with each organization retaining responsibility for sampling, analytical interpretation, legal requirements and its own final decisions. [11],[12]

References

[1] Institute of Contaminant Standards. (2026, August 29). *What is a TECRID?* https://tecrid.com/what-is-a-tecrid

[2] Institute of Contaminant Standards. (n.d.). *TEC Registry API: Canonicalize, sign, issue, resolve*. https://tecrid.com/developers

[3] Institute of Contaminant Standards. (2026, August 29). *TECRID privacy and data governance*. https://tecrid.com/privacy

[4] Institute of Contaminant Standards. (n.d.). *TECRID for certifiers, retailers and regulators: Structured laboratory evidence*. https://tecrid.com/for-certifiers-retailers

[5] Heavy Metal Tested & Certified. (n.d.). *Verify a certificate*. https://heavymetalcertified.com/verify

[6] Verified Lot Exchange. (n.d.). *How does this work?* https://vle.exchange/how-it-works

[7] Institute of Contaminant Standards. (n.d.). *TECRID for laboratories: Issue verifiable laboratory reports*. https://tecrid.com/for-laboratories

[8] Institute of Contaminant Standards. (n.d.). *TECRID for brands and ingredient suppliers: Verifiable COA portfolios*. https://tecrid.com/for-brands

[9] Institute of Contaminant Standards. (n.d.). *Join TECRID*. https://tecrid.com/join

[10] Institute of Contaminant Standards. (n.d.). *TECRID frequently asked questions*. https://tecrid.com/faq

[11] Institute of Contaminant Standards. (n.d.). *Governance*. https://contaminantstandards.com/governance

[12] Pendergrass, K. (2026, April 24). *About*. https://heavymetalindex.com/about