



QILAHK

SECURITY YOU CAN PROVE

ADVANCED RESEARCH WHITE PAPER

QTA-R04 / 04 OF 05

Federated Authority and Registry Consistency

Research into scoped delegation status freshness and accountable publication

Version 1.1 | October 12, 2026

QILAHK Trust Authority

LOCK / KEY / PROOF

qilahk.com | blog.qilahk.com

Table of contents

Federated Authority and Registry Consistency

Abstract	3
Authority as a scoped relationship	4
Recognition is a policy decision	4
A bounded delegation record	4
Relationship to access architecture	4
Registry events and current status	5
Publish decisions with version checks	5
Separate proof of history from proof of status	5
Partitions revocation and conflicting views	6
An illustrative withdrawal	6
Threat model	6
Make availability choices explicit	6
Federation evaluation protocol	7
Build a failure-oriented test federation	7
Research hypotheses	7
Governance gates and references	8
From prototype to a governed federation	8
Open research questions	8
References	8

Abstract

Federated Authority and Registry Consistency

A portable trust artifact creates a governance and distributed systems problem. A relying organization needs to know which authority may decide a particular claim, whether that authority remains valid, and whether the presented status reflects the latest applicable decision. A valid historical signature does not answer all three questions.

This paper proposes a QILAHK federation model with scoped authority delegation, versioned decision events, a current-status projection, and independently inspectable publication history. It distinguishes cryptographic issuer identity, institutional authority, and the relying party's permission to act. The proposed registry does not grant universal trust across organizations; each relying party applies its own recognition and reliance policy.

The research agenda tests whether this separation improves rejection of unauthorized or stale assertions while preserving bounded availability during failures. The design includes key rotation, delegation withdrawal, partitions, conflicting decisions, and delayed propagation. It is a proposed protocol architecture with evaluation criteria, not an assertion of a deployed federation or external accreditation.

Intended audience

Distributed systems architects, federation operators, and trust governance researchers

Research scope

This white paper presents proposed QILAHK research mechanisms, illustrative scenarios, and evaluation protocols. Its hypotheses are intended for prototype testing and independent review.

QTA-R04 | Version 1.1 | October 12, 2026

Authority as a scoped relationship

Recognition is a policy decision

An issuer can prove control of a key without being recognized to decide a claim. A federation participant must define which organizations and roles it accepts, for which subjects, properties, environments, and assurance contexts. Recognition should be versioned and reviewable. A certificate about a key is not automatically a grant of institutional authority.

The research model separates three checks: signature validation under a key policy, authority validation under a delegation policy, and reliance validation under the recipient's operational policy. A packet can pass the first check and fail the second or third. Keeping these checks visible prevents the presence of a signature from silently authorizing an action.

A bounded delegation record

A delegation identifies grantor, delegate, claim namespace, subject scope, permitted actions, effective interval, and restrictions on further delegation. The child scope must not exceed the parent scope. A delegation chain needs cycle detection, an explicit depth limit, and a rule for the status of downstream decisions when a parent grant is withdrawn.

The authority registry also preserves superseded grants and key histories. Historical review asks whether an actor was authorized when a decision became effective. Current reliance asks whether the decision may still be used now. These questions can have different answers after a withdrawal or policy revision.

Relationship to access architecture

NIST SP 800-207 describes zero trust without implicit trust based only on network location or ownership [1]. This proposal applies a related discipline to federated assertions: recognition is explicit and contextual. It does not replace a policy enforcement point or claim that a registry record alone authorizes access.

Registry events and current status

Publish decisions with version checks

A decision event names the subject, claim, authority grant, evidence commitment, criteria version, disposition, effective interval, and predecessor decision. The registry validates the event against the appropriate authority context. It uses expected-version checks and idempotency keys to detect concurrent or repeated submissions.

The current-status projection is derived from accepted events under a defined ordering and conflict policy. Do not rely on unsynchronized wall-clock timestamps alone to resolve conflicting authority actions. Explicit predecessor relationships and a controlled commit order make transitions auditable. Conflicts that cannot be resolved by policy should remain visible.

Separate proof of history from proof of status

A signed artifact and a publication inclusion proof can establish that a decision was recorded. They do not establish that it is still the current applicable decision. A status response must identify the relevant decision version, authority context, response time, and permitted cache lifetime. Its verifier needs a freshness rule.

An append-only publication log can make retrospective changes detectable to observers that compare authenticated checkpoints. RFC 9162 provides consistency-proof mechanisms for its certificate-log setting [2]. Applying similar mechanisms to trust decisions requires a separate protocol and monitoring design. A single isolated reader may fail to detect inconsistent views without checkpoint comparison.

Three independent relying-party checks

Check	Question	Example failure
Cryptographic	Did the accepted key sign these bytes	Invalid signature or disallowed algorithm
Authority	Could this actor decide this claim	Out-of-scope or withdrawn delegation
Current reliance	May this decision be used for this action now	Expired status cache or a superseding decision

TrustMark and certificate interfaces should direct relying parties to a scoped decision and a current-status path. The protocol should make the subject and assessed version visible so a valid representation cannot be casually reused for a replacement device or later software release.

Partitions revocation and conflicting views

An illustrative withdrawal

Authority A delegates a bounded endpoint claim to reviewer B. B records a decision for device D17. A later withdraws B's grant. The federation policy must state whether that withdrawal affects only future decisions or also reliance on existing decisions. The protocol cannot infer this governance choice from a key-status change alone.

A relying party holding a cached status may miss the withdrawal until its cache expires or it receives an authenticated update. Bound that exposure through a declared cache and outage policy. Shorter cache lifetimes can reduce stale reliance but increase dependency on the status service. The research must measure both effects.

Threat model

Attackers may replay old status responses, publish out-of-scope decisions, steal a delegate key, exploit ambiguous subject names, or attempt to present different histories to different readers. The model also includes honest service failures and network partitions. It assumes some recognized authorities and verifier trust anchors remain uncompromised.

Audit records and commitments help investigate equivocation but do not make a malicious authority honest. Independent observers, authenticated checkpoint exchange, and dispute procedures are proposed components. Their own recognition, availability, and key management need assessment.

Make availability choices explicit

For a high-consequence action, a relying policy may require fresh status and refuse to proceed during a partition. A lower-consequence action may permit bounded cached reliance. Record the selected rule and the actual freshness observed at the action. Do not represent degraded operation as fully current verification.

When two authorized decisions conflict, preserve both events and apply a declared reconciliation process. An automatic last-write-wins rule can erase the significance of a disagreement. A registry designed for accountability needs to expose the dispute and the authority action that resolves it.

Federation evaluation protocol

Build a failure-oriented test federation

Create multiple test authorities, delegates, registry replicas, and relying clients. Generate scoped grants and decisions with known valid and invalid chains. Inject withdrawal, key rotation, status replay, version conflict, partitions, delayed events, and inconsistent checkpoint presentation.

Compare signature-only artifact validation, centralized live-status lookup, and the proposed federation with bounded caching and publication observation. Document the differences in metadata and availability. A centralized baseline may provide stronger immediate consistency while incurring a different failure boundary; comparisons should preserve those tradeoffs.

Research hypotheses

H1 proposes that explicit delegation validation reduces acceptance of cryptographically valid but unauthorized assertions. H2 proposes that checkpoint observation detects inconsistent publication histories under a defined observer-connectivity model. H3 proposes that bounded caching makes stale-reliance exposure measurable and enforceable under the chosen fault model.

The hypotheses fail if out-of-scope assertions are accepted, if inconsistent views remain undetected beyond the declared observer condition, or if clients exceed cache limits without exposing degraded status. Report results separately for key compromise, authority withdrawal, and ordinary service outage.

Proposed federation measures

Measure	Definition
Unauthorized acceptance	Accepted out-of-scope assertions divided by all out-of-scope assertions
Stale reliance window	Elapsed time from effective withdrawal to the last action relying on affected cached status
Conflict visibility	Conflicting event pairs exposed to review divided by injected conflicting pairs
Equivocation detection	Detection delay under the declared checkpoint-exchange topology
Availability	Permitted requests completed within policy divided by all permitted test requests

Use adversarial workloads alongside benign workloads and report the recognition policy used by every client. A protocol-level result does not establish external accreditation, business legitimacy, or legal authority. Those remain governance inputs that the federation must maintain.

Governance gates and references

From prototype to a governed federation

Specify claim namespaces, delegation semantics, withdrawal effects, status freshness, conflict resolution, and dispute ownership before building broad interoperability. Implement independently testable verifiers and publish conformance vectors for valid and invalid authority chains.

A deployment gate should require explicit authority recognition, rejection of stale and out-of-scope assertions, visible partition behavior, and an accountable publication recovery process. Key rotation must be tested without losing historical verification or unintentionally extending a delegate's scope.

Open research questions

How should organizations express partial recognition of another authority? What observation topology is sufficient to detect inconsistent histories within a desired interval? How can a federation protect sensitive subject information while preserving status verification? Which governance events should trigger reassessment of existing decisions?

The intended contribution is a protocol that makes authority and freshness inspectable. Its success depends as much on maintained recognition policy and clear withdrawal semantics as on the cryptographic validity of the artifacts it transports.

References

[1] NIST SP 800 207 Zero Trust Architecture

Contextual authentication and authorization foundation.

<https://csrc.nist.gov/pubs/sp/800/207/final>

[2] IETF RFC 9162 Certificate Transparency Version 2

Append-only log and consistency-proof design reference.

<https://www.rfc-editor.org/rfc/rfc9162>

[3] QILAHK Journal Trust Registry Current State and Decision History

Registry scope and history framing.

<https://blog.qilahk.com/trust-registry-current-state-and-history.html>

Reference editions and source pages checked October 12, 2026. The proposed mechanisms and evaluation plans in this paper are research designs, not reported experimental findings.