

Q-Kavach

Modernising identity trust.



Q-Kavach applies cryptographic choices across selected credentials, assertions, tokens, sessions and audit evidence. Its engineering focus is the identity lifecycle: how trust is established, delegated, checked and recorded as organisations examine post-quantum migration.

THE DECISION

Changing a transport algorithm does not resolve classical assumptions in credentials, delegated authority or long-lived evidence. An evaluation must connect cryptographic migration with the people and systems responsible for issuing, verifying and retiring identity.

ARCHITECTURE / SELECTED BOUNDARIES

01	Establish	ML-KEM establishes shared secrets on supported key-exchange and envelope-protection paths. Algorithm roles remain explicit.
02	Assert	ML-DSA signs and verifies selected identity tokens, federated assertions and verifiable credentials. Selected agent paths use signed client assertions.
03	Govern	Provisioning, scope, policy and lifecycle checks govern selected paths. Protected resources must enforce their own verified boundary.
04	Prove	Linked records and signed checkpoints support change detection when correctly provisioned and verified. These are distinct layers; not every request traverses every capability.

WHO SHOULD READ THIS

For identity architects, security leaders, public institutions and programme owners evaluating a bounded identity trust path.

A focused evaluation brief, not a certification or production-readiness statement.

EVIDENCE & EVALUATION

What can be examined today.

Evidence reviewed 28 September 2026 / P11.1. Publication does not represent new testing. States are not a maturity score.

Implemented	Selected development paths represent agents as distinct identities and use signed client assertions.
Tested	Selected tests exercise delegation narrowing, parent binding, depth, lifetime, audience, replay, lifecycle state and linked evidence with signed checkpoints.
Deployment-dependent	Resource enforcement depends on verification of the exact identity, scope, audience, lifetime and available lifecycle state in the target environment.
Design proposal	Disconnected identity, queued evidence and later reconciliation remain an evaluation model, not product-wide operational behaviour.
Out of scope	Universal agent governance, agent-behaviour correctness, vendor integration and standards certification are not claimed.

BOUNDARY TO RETAIN

Pre-certification and pre-scale. Engineering tests do not establish independent assurance or production-scale deployment. The Q-Kavach module is not FIPS 140-3 validated. SLH-DSA is not implemented. Evidence is tamper-evident, not immutable; selected checks do not imply immediate revocation across disconnected systems.

A BOUNDED FIRST EVALUATION

- 01 Who issues the identity, owns its lifecycle and remains accountable for delegated authority?
- 02 Can one evaluated chain demonstrate narrower child scope, bounded lifetime and refusal of an invalid grant?
- 03 What must the protected resource verify, and which dated evidence supports that exact path?

Discuss one bounded trust path. Agree the issuer, verifier, resource boundary and evidence required before considering a conditional pilot.

Public dossier: astrasutra.in/work#q-kavach

Read: Delegated agent identity

Read: Tamper-evident is not immutable