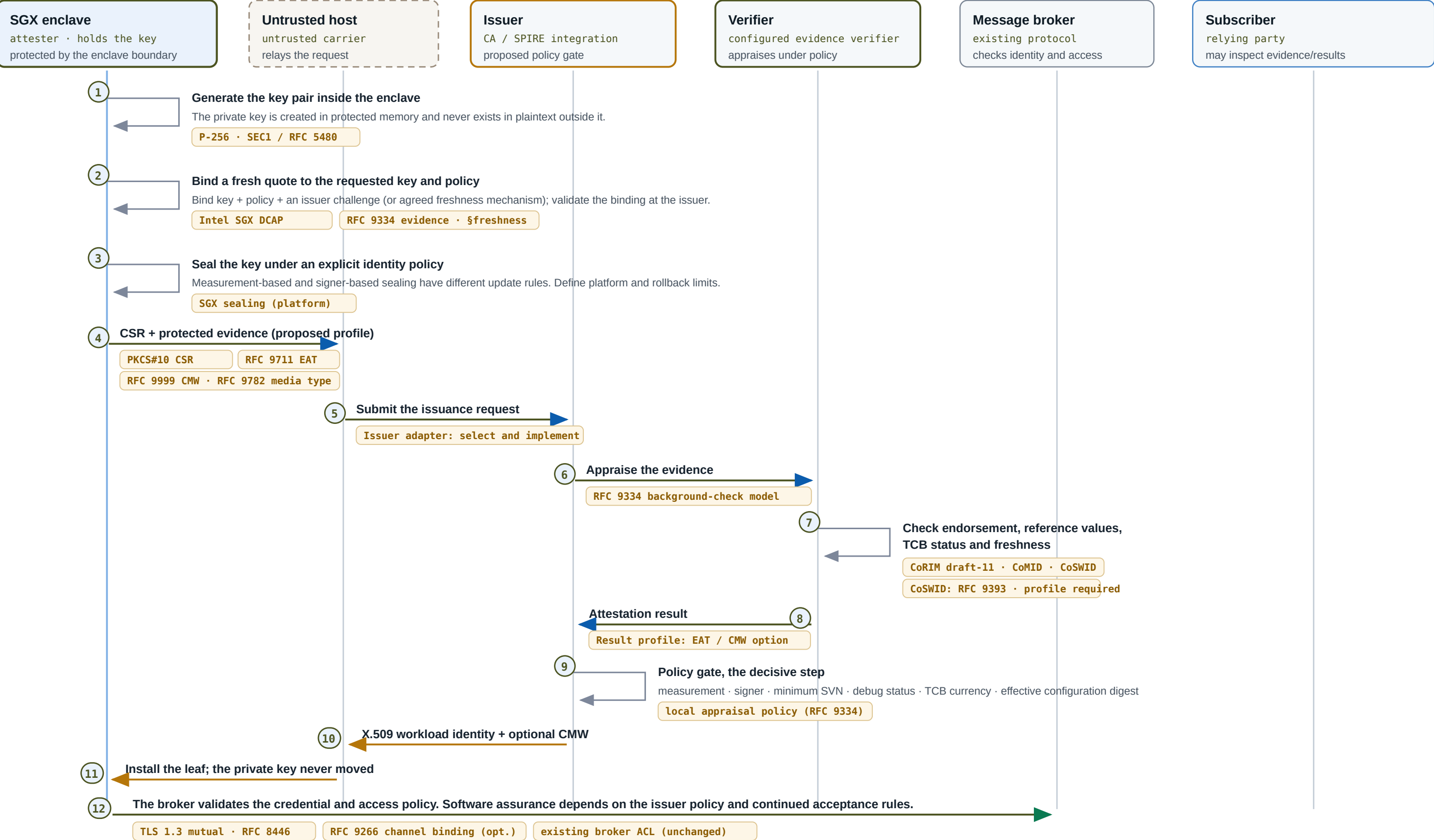


Proposed attestation-gated credential issuance

Design sequence: issue a workload identity only after accepted evidence. The full issuer path and its refusal case are not yet demonstrated.



What the proposed change would establish

The URI SAN remains a workload identity. Issuance would depend on accepted software evidence. An optional CMW extension can carry evidence/results; a broker that ignores it relies on the issuer. Exposure also depends on revocation, reappraisal, resumption and existing-session lifetime.

Refusal case to demonstrate — not yet evidence

Missing, stale or unapproved evidence should cause the new issuance request to be refused. Refused renewal does not invalidate a still-valid certificate or terminate an existing session. Immediate exclusion needs enforced withdrawal and session policy. Test those paths separately.