

Four independent questions, and what answers each

Connectivity, identity, software evidence and observation accuracy need separate checks. Success in one does not establish the others.



QUESTION	MECHANISM THAT ANSWERS IT	GOVERNING STANDARDS	WHAT TO ESTABLISH
1 Can these two peers exchange packets at all? Reachability: which enrolled devices may route to each other. Sensors, effectors and laptops need an address before anything else. scope: network · nothing about who or what is at the far end	Network enrolment VPN or mesh membership Services are commonly reachable only from inside the network.	WireGuard · Noise-based protocol NIST SP 800-207 zero-trust framing Vendor-specific control plane; no single IETF standard governs it.	CHECK THE NETWORK Confirm which peers may connect and how access is controlled.
2 Which workload is at the other end? Workload identity: an issuer binds a name to a key. The assurance depends on how the issuer establishes that identity. scope: identity · assurance depends on issuance policy	X.509 leaf with URI SAN Lifetime and rotation are policy choices SPIFFE uses short-lived credentials with frequent automatic rotation.	X.509 · PKCS#10 · TLS 1.3 (mutual) SPIFFE X509-SVID / JWT-SVID Federation can extend trust across domains; policy still needs agreement.	CHECK THE ISSUER SPIRE can attest nodes and workloads. Review the configured attestors.
3 What code is running there, in what state? Hardware evidence identifies a defined software boundary. Its value depends on measurement scope, policy and fresh connection binding. A separate assurance decision. scope: measured workload · not the whole machine	Hardware remote attestation SGX quote · MRENCLAVE / MRSIGNER / SVN verifier appraisal · TCB status Proposed: require accepted evidence before issuing a workload credential.	RFC 9334 RATS architecture RFC 9711 EAT · RFC 9782 media types RFC 9999 CMW · X.509 extension CoRIM draft-11 · Intel SGX profile SEAT WG · attested (D)TLS, in progress	CHECK THE EVIDENCE A protected client call has hardware evidence. Issuer integration and wider admission remain separate deployment work.
4 Is the reported observation actually true? An attested sensor can report a drone that is not there: attestation authenticates a workload, not the world. scope: data accuracy · not established by attestation	Provenance, not proof source assertion · transformation chain Independent sources and provenance can support assessment of accuracy.	STANAG 4774 label · 4778 binding Transparency records: separate control Label and binding standards support handling; compliance is not claimed.	ASSESS THE DATA Correct software can still process inaccurate input. Check sources and context.

Identity and software assurance complement each other. What an attestation establishes depends on the measured boundary and the acceptance policy.
An independent client has checked hardware evidence and completed a protected call. Applying that check to backbone credential issuance remains proposed.

Threat scenarios and the controls they require

Endpoint compromise, replay and disrupted links require different controls. These design options have distinct assumptions and evidence limits.



WHAT THE ADVERSARY DOES	WHAT THE ATTACK EXPLOITS	CONTROL TO CONSIDER	WHAT IT STILL WILL NOT DO
A trusted node is turned against you The node is genuinely yours, correctly issued, and sits exactly where it is supposed to sit.	Identity alone may not reveal altered software. A valid identity can remain usable after compromise unless additional controls intervene.	Proposed: evidence before issuance Require accepted hardware evidence before issuing a credential under an agreed policy. RFC 9334 · RFC 9711 · RFC 9999	Issuance checks a particular point in time. Exposure also depends on expiry, revocation, reappraisal and how existing sessions end. Refused renewal does not cancel a valid leaf.
A forward sensor is captured and returned It is recovered, its software replaced, and put back into service still wearing your badge.	A credential may survive a software change. A recovered device needs checks appropriate to its hardware and the suspected compromise.	Measure supported device software DICE and PSA support suitable embedded platforms; not every existing sensor qualifies. TCG DICE · RFC 9783 PSA token	Extracted keys can enable impersonation. Identity, key protection and software evidence must be considered together. Withdrawal cannot reach an isolated receiver immediately.
Reports arrive from a sensor that does not exist Traffic is injected that no real device produced, naming a call sign that exists only on paper.	An unverified source label is not identity. Bind the reporting principal to authenticated credentials; do not trust its label alone.	Bind source identity to authentication A verified channel identifies its endpoint. A gateway needs separate source bindings. keys per unit, never per batch	Per-device keys support individual attribution. A shared batch key weakens that distinction. Gateway attestation alone does not authenticate each physical sensor behind the gateway.
Yesterday's traffic is played back as today's Captured traffic is re-sent, or a session is diverted so the proof describes a different link.	A signature alone does not establish freshness. Reused evidence or reports need explicit replay protection and acceptance rules.	Bind evidence and enforce freshness Bind the evidence to the intended key/session. Use a challenge or defined time-based policy. RFC 9266 channel binding · nonce	Session binding is not observation time. Protected counters need persistent state and reset/rollback rules. They can support ordering, but cannot deliver reports without a link.
The equipment is subverted before it deploys The adversary reaches the kit, or the list of what the kit should look like, before it is ever issued.	Reference values are part of the trust boundary. A corrupted approval list can make unwanted software satisfy an otherwise correct check.	Protect the approved reference values Authenticate policy and software approvals; control updates and withdrawal of old values. CoRIM draft · CoSWID: RFC 9393	Review the authority behind the reference list. Check its integrity through a trusted route. Approval of a software image does not establish that it is free from exploitable defects.
The link is jammed instead of the equipment Disruption can prevent fresh evidence checks and delay delivery of operational information.	Online verification depends on connectivity. Define degraded operation in advance rather than silently dropping assurance requirements.	Design option: carry attestation results The passport model can reduce dependence on an online verifier at the point of use. RFC 9334 passport model	Validity periods and cached policy need limits. Disconnected withdrawal and later catch-up need separate design and testing. This is not a demonstrated anti-jamming capability.
The sensor itself is deceived GPS spoofing, decoys, or patterns built to make automatic recognition report the wrong object.	Untampered software can process false inputs. A valid measurement does not establish that the sensor interpreted the world correctly.	Attestation alone does not resolve this Independent sensing and checks may help. Protecting software supports those controls. this is question 4 · see sheet 2	Other sensing or security measures may detect particular deceptions. Software assurance does not make the observations accurate or guarantee that cross-checks find every error.

Recorded evidence and proposed controls
An independent client has appraised a protected workload and completed a call.
Issuer gating and disconnected attestation remain separate design work.
Per-sensor provenance needs evidence for the complete source-to-report path.

Limits of this evidence
It does not prove sensor accuracy, universal tamper resistance or operation under jamming. Each control must be tested on its intended deployment path.
The controls above are not a claim of a complete fielded defence.

Adding assurance to the existing backbone

Connectivity, information exchange and software assurance complement one another. Integration and policy work remain necessary.



HOW IT LAYERS

Proposed additions and integration choices

Evidence before credentials

Proposed: check hardware evidence against an agreed software policy before the issuer grants a credential. The issuer integration must be built.

Protect selected payloads

Endpoint encryption can keep content from intermediaries when deployed with suitable keys and participants. Broker TLS alone does not do this.

Publish clear interfaces

Common contracts support OpenAPI, AsyncAPI, Proto3 and MCP surfaces. Adapters, data meanings and topic registration still require integration.

 builds on existing services · requires agreed policy and integration

EFDI Data Backbone — documented integration

Netbird / WireGuard mesh

Decides which enrolled devices can reach each other at all.

answers question 1

Zenoh router and topic keys

Carries publish and subscribe traffic, with write authority by vendor prefix.

distribution, unchanged

BASELINE SERVICES

Issuer and service identity

Current records describe an offline CA. SPIFFE/SPIRE is an integration option.

answers question 2

TO BE UNAMBIGUOUS

What we are not proposing

- ✗ Replacing the selected network services
- ✗ A second, competing backbone
- ✗ Changing the router, the mesh or the topic scheme
- ✗ Asking other participants to adopt our tooling to interoperate with us

What we are proposing

- ✓ Require accepted evidence before issuing a workload credential
- ✓ Design endpoint payload protection where disclosure policy requires it
- ✓ Use published contracts to reduce bespoke integration work
- ✓ Agree deployment, compatibility and fallback behaviour in advance

RECOVERY PLANNING — A SEQUENCE TO ASSESS, NOT A DEMONSTRATED TIMETABLE

Step 1

Take stock

Identify surviving services, available state and the identities and permissions that remain valid.

Step 2

Review the contracts

Check published interfaces, data meanings and dependencies with each participating team.

Step 3

Integrate and test

Adapt incompatible interfaces and verify schemas, routing, access policy and failure behaviour.

Step 4

Exercise recovery

Test restored services and data continuity under realistic disruption. Record time and limitations from that exercise.

Separate the three integration decisions

The network governs reachability; the issuer and application establish identity and authority.
Hardware evidence adds assurance about a defined software boundary under an acceptance policy.
Existing identity mechanisms may already inspect workload properties; review their actual policy.

Issuer gating, protected sessions and carried evidence are distinct designs with different costs.
They do not automatically make an arbitrary partner system interoperable.

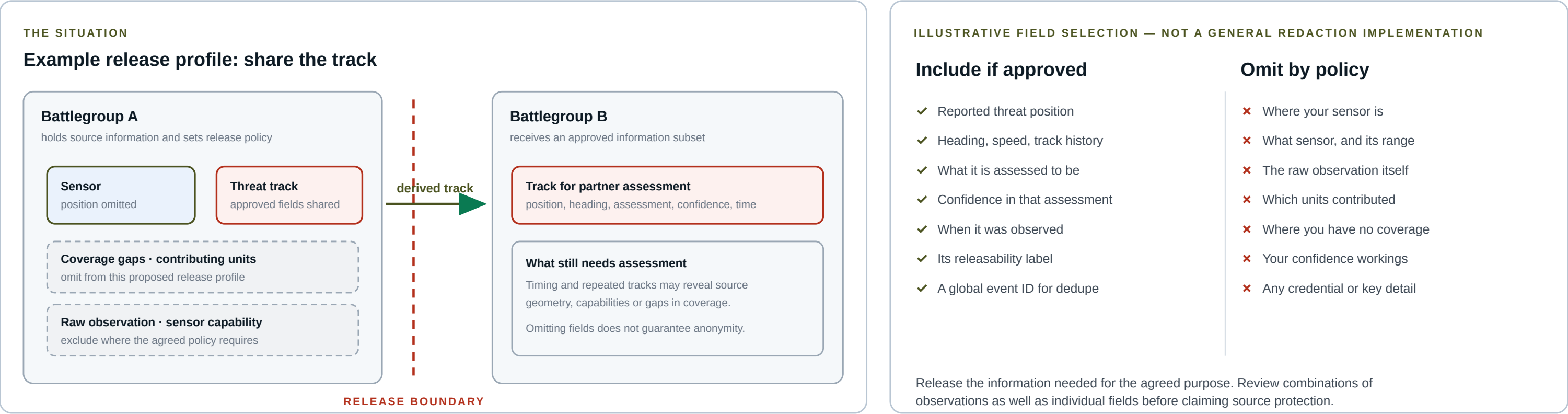
Recorded integration and remaining work

The records show outbound synthetic telemetry reaching the backbone through a publication bridge.
That is a specific delivery path, not proof of endpoint-encrypted backbone payloads or complete inbound and replay integration. Those paths need their own implementation and acceptance evidence.

An independent client has appraised the enclave and completed a protected call. Credential issuance based on that evidence remains proposed; the direct client path does not establish the issuer path.

Sharing useful information with controlled disclosure

Limit unnecessary source detail while providing a partner with useful warning. Assess both released fields and what can be inferred.



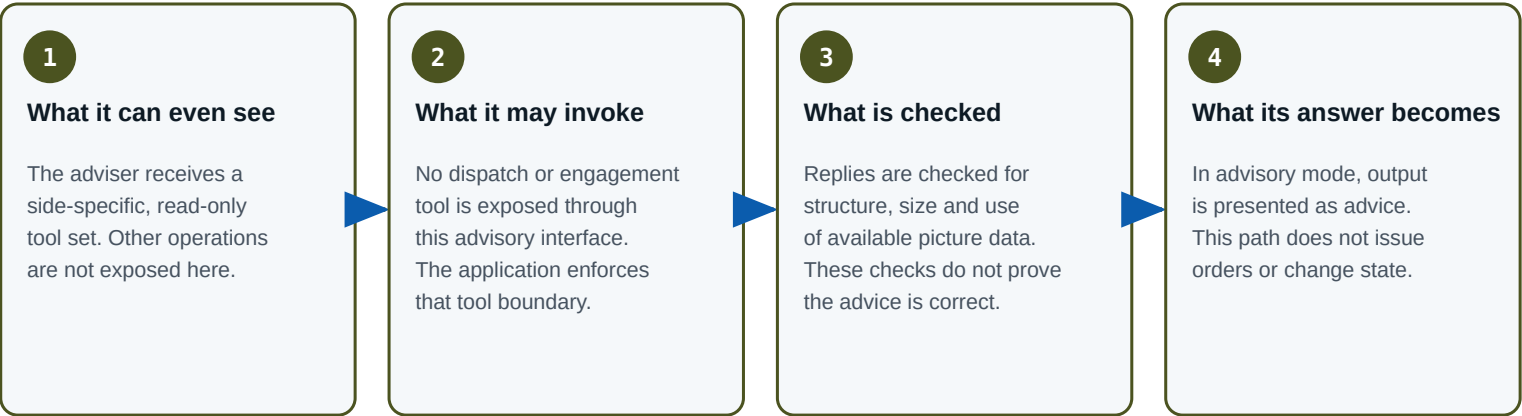
Limiting what an AI adviser is permitted to do

Application controls define available tools and validate responses. Software assurance can help establish which controls are running.



BOUNDED AUTHORITY, IN FOUR GATES

The advisory interface has defined limits



Operations excluded from the published advisory tool interfaces

× publish a proposal	× authorise anything	× task or dispatch	× engage	× write a civilian alert
× replicate to a peer	× touch the audit record	× see a credential	× see attestation evidence	× control media

SCOPE OF THE DEMONSTRATION



Two distinct modes

The advisory tools let a model inspect a bounded picture. They do not give it direct command or effect operations. The external model is not inside the attested application boundary.

A separate synthetic wargame controller can use validated model outputs to take actions after an operator authorises that invocation. This is distinct from the advisory-only path.

Authorise the mode and constrain its actions

An authorised exercise is not per-action approval. The scope must be clear to the operator.

ASSURANCE AROUND THE APPLICATION

Check the software enforcing the limits

Confidential computing can protect a defined application boundary from its host. It supplements organisational and application controls; it does not remove the need to trust the hardware, verifier policy, approved code or deliberate data recipients.

- The hardware demonstration places application logic and tool execution inside an enclave. The external model and its provider remain outside that boundary; data sent to them is not hidden from those recipients.
- An independent client has appraised hardware evidence and completed a protected call. The in-page verifier is served from unsealed assets, so its panel alone is not an independently trusted browser bootstrap.
- Software evidence can identify the measured controls; it does not certify their correctness or the safety of every model response.

What the evidence establishes

The recorded application and tool boundary is distinct from the external, unattested model. Two advisers completed structured tool-call cycles in the recorded demonstration. This is not evidence that every model response is safe.

Read-only tools limit direct action through that interface. The separate synthetic controller has a different, explicitly authorised scope.

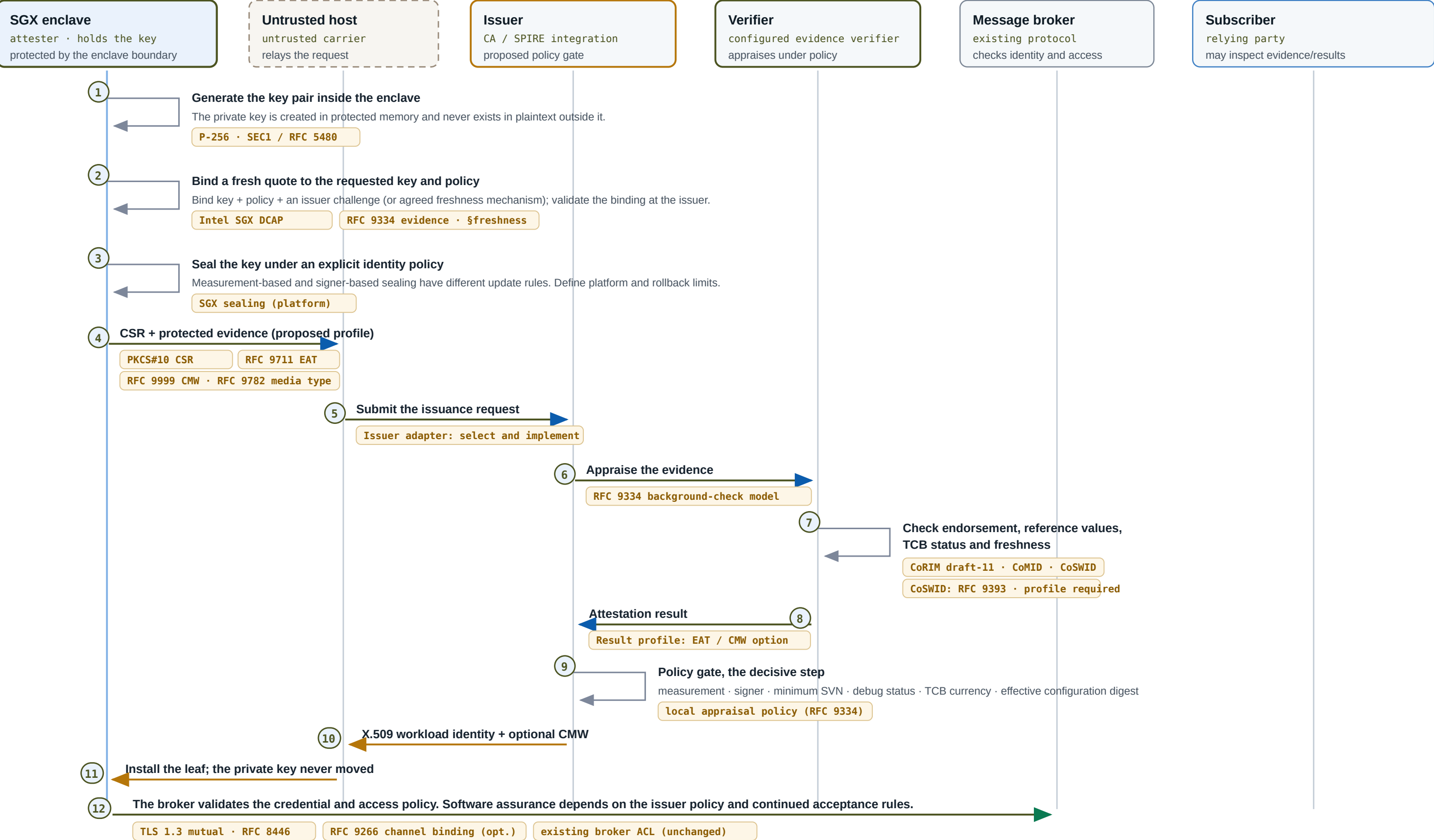
Neither mode is a guarantee against rogue AI.

The assurance argument

Restrict the operations available to the adviser, validate its output and check the software enforcing the boundary. State separately who authorises any controller that turns advice into actions. Hardware checking does not make advice correct.

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.