

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.