

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.