QVN private networking

A requirements-led pilot brief

Presented by FDI Advisory Group

Africa and international markets · Updated November 18, 2026

QVN is described in the supplied QVN presentation and Africa flyer as a controlled private network fabric connecting supported sites, users, devices, cloud environments, and applications. The materials describe central profiles, policy-controlled virtual networks, multiple-link paths, and hybrid post-quantum key establishment. These are source-described capabilities, not independently validated product findings.

FDI Advisory Group is the commercial inquiry contact for discovery, demonstration requests, pilot scoping, and integration discussions. Supplier identity and participation, written implementation or resale authority, supported release and configuration, availability, licensing, price, and responsibilities must be verified and agreed before any engagement is accepted. This brief does not establish those rights or confirm an available service.

What your team can evaluate

Alternative connection paths. Explore supported fixed/fibre, cellular, satellite, or radio links. Failover needs a working alternative connection, adequate power, and sufficient capacity. Session continuity is a design objective to test, not an uptime or uninterrupted-service guarantee.

Central access and virtual networks. Define approved users, devices, services, and policy-controlled virtual networks, or VNETs. Test permitted and denied access, segregation, policy changes, monitoring, and operating ownership.

Infrastructure interconnects. Discuss private paths between data centres, supported cloud environments, applications, and authorized remote devices. Networking alone does not establish data sovereignty, residency, endpoint security, application confidentiality, or regulatory compliance. Confirm the encryption boundary and supported platforms for the proposed configuration.

Hybrid key establishment. The supplied presentation describes P-384 plus ML-KEM-1024 key establishment and AEGIS-256 authenticated packet encryption. ML-KEM is standardized in NIST FIPS 203 1; that algorithm reference is not QVN product certification or cryptographic-module validation 2. Confirm the actual release, implementation evidence, key management, and relevant standard updates. No guaranteed quantum resistance is represented.

Choose an operating context

Banking and payment teams can evaluate branch connectivity, access separation, and application behavior during link changes. This is networking evaluation, not a banking, payment, settlement, or regulatory-approval service.

Data-centre, cloud, private-AI, telecom, and managed-service teams can evaluate interconnects, tenant boundaries, routes, capacity, and approved access. Supported integrations, service scope, licensing, and operational responsibilities need confirmation.

Utilities and remote-operation teams can evaluate authorized monitoring, mixed links, and operational-technology separation. A networking pilot is not an industrial safety certification or a substitute for safety systems.

Public-service teams can discuss connectivity among offices, service locations, and authorized field users. No government endorsement, procurement eligibility, national-security approval, or authorization to handle classified data is implied.

OEM and application-integration discussions require agreement on compatible apps/devices, licensing, redistribution, branding, implementation, and support. This brief is not an available SDK or an automatic white-label programme.

Assess → Pilot → Decide

Start with a nonconfidential description of the country, sector, locations, approximate site count, users, applications, available links, decision timeline, and operating priorities. Request pilot scoping, a demonstration, or an integration discussion; no inquiry confirms a booking or accepted engagement.

Agree a focused plan with the participating parties before testing. Define supported configuration, success criteria, responsibilities, costs, and dependencies. Connectivity, hardware, hosting, integration, and support may require separate arrangements. Do not infer availability or pricing from this brief.

Use measured results to decide whether to expand, change architecture, continue testing, or stop. No performance benchmark, commercial outcome, or rollout is guaranteed.

Pilot acceptance checklist

- Record application behavior and connectivity baselines before testing.
- Verify primary and alternative links, site power, and available capacity.
- Observe application/session behavior during link loss, recovery, and switching.

- Measure latency and throughput under agreed conditions rather than treating marketing benchmarks as promises.
- Test approved access, denied access, segmentation, and policy changes.
- Confirm supported devices, release, cryptographic configuration, and implementation evidence.
- Define monitoring, logging access, support, incident handling, and operating ownership.
- Record limitations, open issues, and the decision required before expansion.

Start a QVN conversation

Scope a pilot: https://fdiadvisorygroup.com/qvn/pilot
QVN overview: https://fdiadvisorygroup.com/qvn
Public brand contact: riste@fdiadvisorygroup.com

An inquiry is not an appointment, quote, contract, licensing right, pilot acceptance, or deployment authorization. Public forms are for general descriptions only. Do not submit confidential contracts, identification documents, banking information, classified information, secret network designs, or export-controlled technical data. Agree an appropriate sharing process if needed. Providing a phone number does not itself grant marketing or SMS consent.

Sources and limitations

Capability descriptions come from the supplied **FDI_QVN_Combined_Marketing_Presentation.pdf**, pages 3–4, 8–9, 11–12, and 15–19, and **FDI_QVN_Africa_Two_Page_Flyer.pdf**, pages 1–2. Both identify FDI as an inquiry contact; neither is evidence here of current supplier authority or availability. Historical deployment assertions and comparative internal benchmarks are not adopted as independently verified facts.

No government authorization, military/national deployment, customer endorsement, exclusive reseller status, uptime promise, regulatory certification, or guaranteed security is represented. Product-specific certifications and supporting evidence would need separate verification for the exact proposed implementation.

References

NIST FIPS 203 — ML-KEM algorithm standard. Official algorithm reference, not evidence of QVN validation.

NIST Cryptographic Module Validation Program. Separate module-validation programme; no QVN validation is asserted here.