QVU: quantum-resilient email and files

Architecture, cryptography and standards · November 2026

QVU is one app for confidential work on Windows and macOS: protected email and files, an encrypted vault, Talk and signed evidence. It works on top of the email people already use, whether Microsoft 365, Google Workspace or any other provider. Keys are made and kept only on the user's device, so no email provider, cloud service or QuantumViva can open what QVU protects.

QVU is in build. This overview describes its design.

What QVU does

Protected mail and files

Sealed and signed on the sender's device, sent through their own email account and opened only in the recipient's QVU.

Encrypted vault

Files stay on the user's computer, each with its own key, with ransomware protection and earlier versions kept.

Talk

Short, direct conversations between two verified contacts.

Signed evidence

A signed audit log and evidence packages showing what was sent, to whom and when. The user keeps them.

Also included: security monitoring on the device and, on the Firm plan, a recovery key held by people the firm chooses.

Where keys live, and what our servers do

- Keys are created and held only on the user's device. There is no master key and no copy with QuantumViva.
- QuantumViva's servers register users, show who is available and pass on sealed packages they cannot open. They hold no session secrets.
- No phone number is needed.

What QuantumViva holds

Email address · account and billing details · the technical details needed to connect people

What QuantumViva never has

Keys · messages and attachments · files and vault · recovery phrases

Firm recovery key (Firm plan)

A firm creates its own recovery key, split between people it chooses. Any two of them can reopen a leaver's mailbox for a successor, or restore access for someone who has lost their recovery phrase. Every recovery is logged and shown to staff. QuantumViva never holds any part of the key, and firm recovery never touches signing keys.

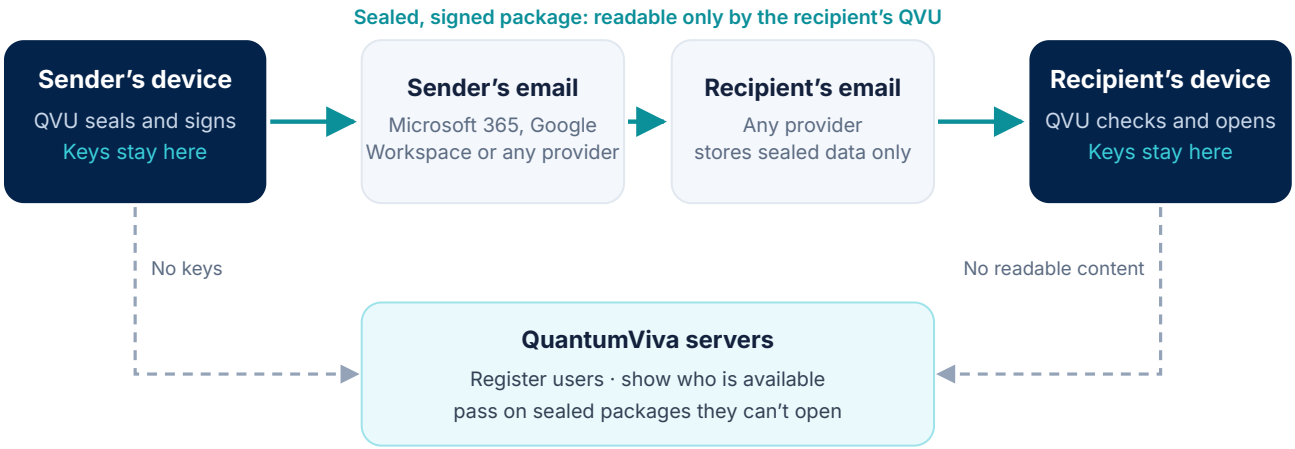
Cryptographic profile

Function	Primitive
Key establishment	ML-KEM-768 + X25519, hybrid
Signatures	ML-DSA-65 + Ed25519, hybrid, on every message
Bulk encryption	AES-256-GCM, authenticated, in transit and at rest
Hashing and key derivation	SHA3-384 · HKDF-SHA3-384 key combiner · Argon2id for passphrase-derived keys
Content keys	Every file and message has its own key. No shared content key.
Envelope format	ASiC-E (ETSI) containers, wrapped per recipient
Recovery	Recovery phrase plus local backup. No escrow.

Hybrid by design. Classical and post-quantum algorithms are combined, so both halves must be broken: protection is never weaker than today's best practice. Algorithms can move up (for example to ML-KEM-1024 or ML-DSA-87) without changing the architecture.

ML-KEM and ML-DSA are NIST's post-quantum standards FIPS 203 and FIPS 204, published 13 August 2024 (NIST). The EU's post-quantum roadmap recommends hybrid schemes wherever feasible (EU Coordinated Implementation Roadmap, June 2025).

How protected email travels



1. **Connect once.** Each contact is verified with a short code before a connection opens. QVU only delivers to people the user has connected with; anyone else gets an invitation instead.
2. **Seal and sign.** The message and attachments are encrypted for that recipient and signed with the sender's hybrid signature, on the sender's device.
3. **Send.** The sealed package goes through the sender's own email account. Providers and servers along the way only ever hold sealed data.
4. **Check and open.** The recipient's QVU checks the signature, then opens the package. AI can imitate a writing style, but not a valid signature.

Vault protection

Windows Controlled Folder Access and a protected macOS container stop unknown programs changing vault files. Canary files with a write-rate lock catch ransomware-like behaviour, and versioned backups to storage the user or firm already has keep earlier versions. Security monitoring on the device warns the user about anything suspicious.

Architecture: security lives on the device

Layer	Role
App interface	Windows and macOS screens. Presentation only, and treated as untrusted: the core validates every command, so a new interface cannot change the threat model.
Platform adapters	Connect the core to the operating system, email accounts and storage. No protocol logic and no key material.
Core engine	One native engine holds every key and secret and does all cryptography, protocol state, policy and envelope handling, behind a narrow, stable interface.
Encrypted local storage	Vault, logs and settings, encrypted at rest on the device.

The engine can be re-implemented behind the same interface without changing protocols, data formats or screens.

Your email provider and QVU

	Most Microsoft 365 and Gmail plans	QVU
Who holds the keys	The provider	You, on your own devices
Can the provider open your mail?	Yes, and so can its AI tools	No. It only ever holds sealed data
A US CLOUD Act demand	The provider can be required to hand over data it controls, wherever it is stored	Nothing readable to hand over
Keys held by the customer	Top-tier plans only: Microsoft 365 E5 (Double Key Encryption) or Google Workspace Enterprise Plus (client-side encryption)	Every plan
Post-quantum encryption	Microsoft: transition complete by 2033	Built in

As of November 2026. Sources: Microsoft, August 2025 · Microsoft Learn, Double Key Encryption · Google Workspace, client-side encryption · DOJ CLOUD Act white paper, summarised by Hunton Andrews Kurth, April 2019.

Standards and assurance

- **Standards.** Built on NIST's post-quantum standards FIPS 203 (ML-KEM) and FIPS 204 (ML-DSA), in hybrid with X25519 and Ed25519, and on ETSI ASiC-E for signed containers.
- **Readiness path.** Designed for FIPS 140-3 validation. GDPR-aligned. Maps to the EU Cyber Resilience Act.
- **Verification.** QVU's protocol designs are being formally verified, and QVU gets an independent cryptography review and penetration test before anyone uses it.
- **Engineering basis.** Specified before it is built: 1,005 numbered requirements, 12 protocol specifications and 101 engineering documents, with a full data model, threat model and design system, checked against each other automatically.
- **Responsible disclosure.** Security researchers can report issues through the Responsible Disclosure page at quantumviva.com.

> **Find out more.** Plain-English answers, the risks QVU protects against and the waitlist are at quantumviva.com. For technical questions, contact info@quantumviva.com.