Tab 1

QUIP

QUIC Identity Protocol

A Federated Identity and Interaction Layer for the Modern Internet

Institutional White Paper — Version 1.0
March 2026
By Junior Joseph Mututi

Executive Summary

QUIP — the QUIC Identity Protocol — is a proposed new layer of internet infrastructure. It defines a federated system for digital identity and structured interaction, built directly on QUIC, the modern encrypted transport protocol standardised by the IETF in 2021. QUIP runs in parallel with the existing web of documents. It does not replace HTTP, DNS, or any existing internet infrastructure. It adds something the internet has never had: a native, open, federated layer in which individuals and organisations own their identities, federate directly with each other, and interact across institutional and geographic boundaries without depending on any central platform.

The problem QUIP addresses is architectural. The internet was designed to distribute documents, not to represent persons. Every identity system built on top of it — passwords, social login, platform accounts — is a workaround that places control of identity in the hands of intermediaries. QUIP proposes to fix this at the infrastructure level, by defining identity as a first-class internet primitive rather than an application-layer convention.

This document is an institutional white paper. It describes the motivation, architecture, governance model, and standardisation pathway for QUIP at a strategic level. A companion technical specification document provides the detailed protocol design, wire format, and implementation requirements for engineers. References to that document appear throughout this paper where appropriate.

Contents

1. What QUIP Is — and Is Not

Before describing what QUIP proposes, it is worth stating clearly what it does not propose. Institutional readers will encounter new protocol proposals through a set of familiar pattern-matching heuristics, and QUIP does not fit the patterns most commonly associated with disruption to internet infrastructure. The following clarifications are offered to prevent misunderstanding from the outset.

1.1 What QUIP Is Not

- Not a social network. QUIP defines infrastructure, not applications. It specifies how identities are represented and how they interact across a federation. What users do with that infrastructure — messaging, publishing, commerce, collaboration — is determined by the applications built on top of it, not by the protocol itself.
- Not a blockchain platform. QUIP uses no distributed ledger, no consensus mechanism, and no cryptocurrency. Its trust model is based on cryptographic signatures and a distributed Certificate Authority network anchored in ISPs — institutions that already hold regulatory licences and legal accountability in their jurisdictions.
- Not a replacement for DNS. QUIP uses the Domain Name System for node discovery, exactly as email and the web do. It does not propose a new naming system. Domain names remain the namespace for QUIP addresses.
- Not a replacement for HTTP. QUIP runs on a different port, uses a different transport protocol (QUIC over UDP rather than TCP), and solves a different problem (identity and interaction rather than document retrieval). HTTP and QUIP coexist; a user visits a website over HTTP and maintains a QUIP identity session simultaneously.
- Not a closed ecosystem. QUIP is an open protocol designed for IETF standardisation. Any ISP, organisation, or developer can implement it. No single entity controls the federation.

1.2 What QUIP Is

QUIP is a new internet-native identity and federation layer. It is a protocol — a set of rules for how software components communicate — that enables independently operated nodes to form a global federation in which users own their identities, organisations federate directly, and interactions are carried over encrypted, authenticated connections without central brokers.

The simplest way to understand QUIP is by analogy to email. Email is a federated protocol: a user at gmail.com can send a message to a user at company.co.zw because both services implement the same open standard (SMTP). Neither Google nor the Zimbabwean company controls the other's infrastructure. The message travels directly between their servers. QUIP applies this same federation principle — which works well for email — to the broader problem of

identity, presence, and structured interaction, with modern cryptography and a modern transport protocol replacing email's decades-old foundations.

2. The Problem QUIP Solves

2.1 Identity Held Hostage

When a person creates an account on any major internet platform today, they do not acquire an identity. They acquire a tenancy. The platform owns the identifier. It can revoke it, monetise it, transfer it to a successor organisation, or surrender it under legal compulsion. The user cannot move it, cannot prove it cryptographically without invoking the platform, and cannot carry their social graph or interaction history if they leave.

This is not a policy failure. It is an architectural one. The web's foundational protocol, HTTP, was designed to transfer documents between servers and browsers. It has no native concept of a persistent user identity. Every login system, session cookie, and OAuth flow is a workaround layered on top of a protocol that was never designed to support it. Workarounds accumulate technical debt. They also accumulate power: the organisations that build the most widely adopted workarounds acquire structural control over digital identity at a global scale.

2.2 Federation Without Brokers

The same architectural gap affects organisations. Companies that wish to interact directly across institutional boundaries — to exchange structured events, verify each other's identity, or maintain persistent authenticated sessions — have no open standard for doing so. They must either adopt a shared proprietary platform (surrendering control to a third party) or build custom point-to-point integrations (expensive, brittle, and unscalable). Email is federated but provides no structured interaction vocabulary and no real-time capability. The result is a fragmented landscape of platform silos where direct institutional federation is the exception, not the norm.

2.3 The Surveillance Surface

Centralised identity creates a centralised surveillance surface. When identity is mediated by a small number of large platforms, those platforms become high-value targets for state surveillance, data breaches, and commercial exploitation. A federated identity layer in which ISPs — licensed, regulated, nationally accountable institutions — serve as trust anchors rather than identity owners produces a structurally different threat model. No single organisation can be compelled to hand over the identities of all users simultaneously. Compromise of one node does not compromise the federation.

3. Architectural Foundations

QUIP draws its design from three sources: the federation model of XMPP (the Extensible Messaging and Presence Protocol), the interaction vocabulary of ActivityStreams 2.0, and the transport capabilities of QUIC. Each contributes a distinct architectural principle.

3.1 Federation from XMPP

XMPP, the protocol underlying the original Jabber messaging network, demonstrated in the early 2000s that federated identity at internet scale is achievable. Its addressing scheme — user@domain — is simple, human-readable, and inherently decentralised: the domain component distributes authority across independently operated servers, exactly as domain names distribute authority for websites and email. No central registry of usernames is required. Each domain is authoritative for its own users.

QUIP inherits this addressing model directly. A QUIP identity takes the form user@domain. The domain maps to a federation node operated by the user's ISP or hosting provider. Two users at different domains can interact directly because their domains federate with each other, without any intermediary. The principle is the same as email; the implementation is modern.

3.2 Interaction Vocabulary from ActivityStreams

ActivityStreams 2.0, the W3C standard underlying the Fediverse (Mastodon, Pixelfed, and related platforms), defines a vocabulary for describing social interactions: Create, Follow, Like, Announce, and related types. This vocabulary has proven expressive enough to represent the full range of social and institutional interactions across millions of federated users.

QUIP adopts the ActivityStreams 2.0 vocabulary as its baseline interaction layer. This is a deliberate choice for two reasons: it ensures semantic compatibility with the existing Fediverse, enabling interoperability from day one of a QUIP deployment; and it avoids reinventing a vocabulary that the internet community has already invested significantly in defining and refining.

3.3 Transport from QUIC

QUIC (RFC 9000, 2021) is the modern transport protocol developed by Google and standardised by the IETF. It runs over UDP, integrates encryption natively, supports multiple simultaneous streams over a single connection, and eliminates the latency penalties that afflict TCP-based protocols. Every QUIC connection is encrypted from its first byte. There is no option for unencrypted communication.

QUIP is built exclusively on QUIC. This choice is not incidental. The properties of QUIC — native encryption, multiplexed streams, fast reconnection, connection migration across network changes — map directly onto the requirements of a federated identity and interaction layer. A mobile user who moves from Wi-Fi to cellular maintains their QUIP sessions without interruption. An ISP node that handles thousands of simultaneous federation relationships can multiplex them all over a small number of efficient connections.

3.4 The State Machine as Interaction Model

Rather than a simple message-passing model, QUIP represents every interaction as a typed state machine: a formally defined set of states and transitions that governs the lifecycle of that interaction from initiation to completion. A direct message, a presence subscription, a collaborative document session, a business-to-business data exchange — each is a different machine type, with its own defined states, valid events, and termination conditions.

This model provides structural properties that message-passing cannot: deterministic recovery from network interruption, cryptographic verification that two nodes' views of a shared interaction are consistent, and a natural unit for access control, auditing, and versioning. The state machine is what transforms QUIP from a transport mechanism into a platform for structured institutional interaction. The technical details of the state machine framework are defined in the companion specification document.

4. Identity Architecture

QUIP's identity model is built on three principles: self-sovereignty, domain addressing, and cryptographic verifiability. Together, they produce an identity layer that is owned by users, organised by institutions, and verifiable by anyone.

4.1 Self-Sovereign Identity

A QUIP identity is rooted in a cryptographic key pair generated by the user's device. The private key never leaves the user's control. The corresponding public key is the user's permanent identifier — their NodeId — which persists regardless of which ISP hosts their account, which address they use, or which devices they operate. If a user changes ISPs, their NodeId travels with them. Their interaction history, their social graph, and the trust relationships they have built are anchored to the key, not to any service provider.

This is the fundamental difference between QUIP identity and platform identity. A Gmail address belongs to Google. A QUIP address belongs to the user.

A single NodeId may carry more than one address simultaneously. A person might hold alice@home.isp as their primary personal identity and alice@corp.com as a secondary organisational identity, both resolving to the same cryptographic root. The primary address — always issued by the user's ISP — is the canonical identity returned when someone looks up the user by their key. Secondary addresses resolve inward to the same key, allowing messages sent to either address to reach the same person. If the user changes employer, they add or remove a secondary attestation without touching their primary identity.

4.2 Domain Addressing

The human-readable form of a QUIP identity is user@domain, where the domain identifies the ISP or organisation that hosts the user's federation node. This addressing scheme serves two functions simultaneously: it provides a memorable, shareable address for everyday use, and it provides a resolution path for the cryptographic identity underneath.

The domain component carries meaningful institutional context. Country-code top-level domains signal jurisdictional affiliation. Organisational domains signal the entity operating the node. This contextual richness is absent from purely cryptographic identifiers (public keys, wallet addresses, decentralised identifiers) and is one of the reasons QUIP's addressing model is designed for institutional adoption rather than purely technical use. The distinction between a

primary ISP-issued address and secondary organisational addresses is preserved in this namespace: a user's ISP address carries PERSONAL_ISP trust anchoring while their employer's address carries ORGANIZATIONAL trust anchoring, both verifiable through the same cryptographic root.

4.3 Cryptographic Verifiability

Every QUIP message is signed by the sender's private key. Any recipient can verify the signature using the sender's public key (NodeId). No third party needs to be consulted for this verification: it is a local cryptographic operation. This means that the authenticity of a QUIP message can be verified by any node in the federation, at any time, without depending on the availability of any central service.

The mapping from a human-readable address to the underlying cryptographic identity is performed through the ISP attestation mechanism described in Section 5. Once a node has obtained a user's attestation, it can verify all future messages from that user independently.

4.4 Key Portability and Rotation

Users can move their identity between ISPs by generating a new home node attestation and publishing a signed statement linking their persistent NodeId to their new address. Their contacts update their records; the social graph is preserved. This portability is technically guaranteed by the protocol and does not depend on the cooperation of the previous ISP.

When a private key is compromised or lost, users can initiate a key rotation: a formally defined protocol operation that links a new public key to the old identity with a cryptographic chain of custody. Revocation and rotation notices are published to a public transparency log, ensuring that the federation converges on the correct current state.

5. The ISP Trust Model

The trust architecture of QUIP is its most distinctive design choice, and the one most likely to require careful explanation to institutional audiences. QUIP does not use a blockchain for trust. It does not use a single global certificate authority. It uses Internet Service Providers — institutions that already exist, already hold telecommunications licences, and are already accountable to national regulators — as the distributed trust anchors for the federation.

5.1 Verifiers, Not Owners

The central principle of the ISP trust model is that ISPs verify user identities without owning them. An ISP's role in QUIP is analogous to a notary: it confirms, based on its existing subscriber relationship, that a given address corresponds to a given cryptographic key. The ISP issues the user's primary attestation — the canonical identity anchor. Organisations may independently issue secondary attestations for the same user under their own domain, without ISP involvement, as long as they operate a certified QUIP node. The hierarchy is clear: ISP-issued attestations are primary and Foundation-anchored; organisation-issued attestations are secondary and do not require ISP involvement. It does not hold the keys. It cannot sign messages on behalf of users. It cannot access message content, which is encrypted between sender and recipient. What it can do — and only this — is issue a signed attestation that a specific person holds a specific key.

This distinction has profound consequences. A government that compels an ISP to disclose subscriber records can obtain the mapping between a QUIP address and a subscriber identity. It cannot obtain message content. It cannot forge messages. It cannot silently impersonate a user. The protocol is designed so that the maximum damage achievable through ISP-level compromise is identity disclosure — not identity theft or surveillance of content.

5.2 The Foundation: A Distributed Certificate Authority

ISPs operate as intermediate certificate authorities under a root authority called the QUIP Foundation. The Foundation is a multi-stakeholder governance body — not a single server or corporation — whose root certificate is controlled by a threshold signature requiring cooperation from multiple geographically and jurisdictionally distributed members. No single Foundation member, and no single government, can unilaterally issue or revoke certificates.

This architecture mirrors the Certificate Transparency initiative used in TLS certificate management, and the DNSSEC root key signing ceremony used by ICANN. These are proven

models for distributing trust across competing institutional interests without requiring a single point of control.

5.3 Geographic and Regulatory Reality

QUIP is designed by people who are not naive about how internet infrastructure is governed. ISPs operate under national regulatory frameworks. They are subject to lawful interception requirements. They can be compelled to withdraw a subscriber's attestation. QUIP acknowledges these realities rather than attempting to engineer around them.

What the protocol can do — and does — is limit the consequences of regulatory compliance to the minimum technically necessary. An ISP that withdraws a user's attestation removes that user from the federation at their current address. It does not destroy the user's private key. The user retains their cryptographic identity and can seek re-attestation from a different ISP. The plurality of ISPs in any given territory is itself a structural defence against regulatory overreach: disabling a specific identity requires compelling every ISP in a jurisdiction simultaneously, a visible and legally complex action.

5.4 Surveillance Mitigation by Design

Because message content is encrypted between sender and recipient keys — not between sender and ISP node — the ISP federation layer cannot read what users are saying even for sessions it routes. This is not a configuration option. It is a structural property of the protocol. An ISP node that routes an event between two users sees the event's metadata (who sent it, to whom, when, of what type) but not its content.

Mass surveillance of QUIP communications would require compromise of individual endpoint devices, not infiltration of ISP infrastructure. This structurally changes the economics of surveillance: targeted surveillance of specific individuals remains possible through legal processes; untargeted bulk collection of communication content is not.

6. Federation and Interaction

Federation is what distinguishes QUIP from a centralised service with open-source software. Two ISP nodes that both implement the QUIP protocol can exchange interactions on behalf of their respective users without any prior commercial relationship, without any shared infrastructure, and without any central broker. They simply need to be able to reach each other over the internet and to verify each other's credentials through the Foundation's certificate chain.

6.1 How Federation Works

When a user at ISP-A sends a message to a user at ISP-B, the following sequence occurs. The sender's client submits the message to ISP-A's federation node. ISP-A verifies the sender's identity, locates ISP-B's node using DNS-based discovery, and establishes an authenticated QUIC connection to ISP-B. ISP-A delivers the message to ISP-B, which verifies ISP-A's credentials and delivers the message to the recipient's client. Neither ISP needs to have met before. Trust is established through the shared Foundation certificate chain, exactly as TLS certificates enable trust between web servers and browsers that have never interacted before.

6.2 Discovery and Peering

QUIP nodes find each other through two complementary mechanisms. For initial discovery between previously unconnected nodes, the QUIP Federation Registry — a Foundation-operated directory — provides a lookup service. For established relationships between ISPs with ongoing federation traffic, bilateral peering agreements (analogous to BGP peering in the routing layer) allow nodes to bypass the registry and connect directly through pre-configured paths.

This two-track model mirrors how real internet peering works: major carriers have direct peering relationships with each other, while smaller networks rely on transit and routing infrastructure for initial connectivity. QUIP's discovery architecture is designed to fit naturally into the operational culture of ISP network teams.

6.3 Interaction Types

The interactions that QUIP carries are defined by the ActivityStreams 2.0 vocabulary and QUIP's own extensions. From the perspective of an institutional audience, the relevant point is that QUIP is not limited to any single type of interaction. Direct messaging, presence subscriptions, activity publishing, document collaboration, notifications, and business-to-business event exchange are all representable within the same protocol framework.

The same federation infrastructure that carries a user's personal messages can carry institutional event streams and cross-organisational workflow triggers.

6.4 Real-Time and Asynchronous Modes

QUIP supports both asynchronous interactions (messages delivered whenever the recipient is next available, with store-and-forward reliability) and real-time interactions (audio, video, and live collaboration sessions with direct peer-to-peer paths established between end-user devices). The same identity and federation infrastructure handles both. A user's QUIP address works for a text message and for a video call. The protocol selects the appropriate routing mode based on the interaction type.

7. Coexistence with the Existing Web

QUIP runs alongside the existing web, not in place of it. This is a foundational design commitment, not a transitional compromise, and it follows from a clear analysis of what the two layers are for.

The web of documents — HTTP, HTML, the browser — is the right infrastructure for distributing, rendering, and linking content. It is extraordinarily successful at this and will remain so. The web of identities — QUIP — is the infrastructure for representing, authenticating, and connecting persons and organisations. These are different problems. They benefit from different designs. Solving one does not require replacing the other.

7.1 Bridges Between the Layers

Three bridge components allow QUIP and the existing web to interact without friction.

The first is a web authentication bridge. A website that wishes to authenticate users via their QUIP identity can implement a simple flow in which the user approves the authentication request through their QUIP client. The website receives a cryptographically verified identity claim. No password, no OAuth dependency on a platform provider.

The second is a notification gateway. Web applications that generate notifications can deliver them to QUIP addresses through a simple translation service that converts an outgoing notification into a QUIP event. From the recipient's perspective, notifications from web services and messages from other QUIP users arrive through the same identity-native channel.

The third is a Fediverse bridge. Because QUIP adopts the ActivityStreams 2.0 vocabulary, QUIP nodes can exchange activities with Mastodon, Pixelfed, and other ActivityPub-based Fediverse platforms without those platforms implementing the QUIP protocol. This gives QUIP users immediate access to a federated social graph of millions of existing users from day one of their account.

7.2 Migration, Not Cutover

Organisations that operate existing identity infrastructure — enterprise directories, university authentication systems, government identity platforms — can participate in QUIP by deploying a federation node alongside their existing systems. Internal users' identities are mapped to QUIP addresses attested by the organisation's own node. External federation uses QUIP; internal systems continue to operate as before. The migration is additive and incremental, not a forced replacement.

8. Technical Specification (Separate Document)

This white paper describes QUIP at the architectural and strategic level. The detailed engineering specification — intended for protocol implementers, cryptographers, and IETF working group participants — is maintained as a companion document titled:

> QUIP: QUIC Identity Protocol — Technical Specification, Draft v1.0

The technical specification defines, in full detail, the following components that are intentionally omitted from this white paper:

- Wire protocol: frame structure, binary encoding, field definitions, and byte-level format
- Serialisation format: Protocol Buffers schema for all message types, canonical serialisation requirements, and schema governance
- State machine framework: formal definition of the machine type model, transition function semantics, lifecycle phases, and resource quotas
- Transport binding: QUIC stream mapping, connection establishment, 0-RTT session resumption, flow control, and ALPN configuration
- Security model: Ed25519 signature scheme, key derivation, anti-replay mechanisms, and mutual authentication protocol
- Federation discovery: registry protocol, peering agreement format, capability advertisement, and routing loop prevention
- Consistency and synchronisation: snapshot transfer algorithms, delta encoding, Merkle tree construction and verification, vector clock ordering, and CRDT conflict resolution
- Operational requirements: monitoring metrics, capacity targets, load testing suite specification, and cluster architecture

> *Readers seeking implementation guidance, interoperability test specifications, or the formal open questions list for IETF working group discussion should consult the technical specification document directly.*

9. Institutional Engagement

QUIP is designed to work within the existing ecosystem of internet governance institutions rather than around it. The following describes the role each institution plays in QUIP's development and deployment, and the nature of the engagement sought with each.

9.1 Internet Engineering Task Force (IETF)

The IETF is the primary standardisation body for internet protocols. QUIP's goal is to become an RFC — a published IETF standard — through the IETF's open working group process. The engagement strategy with the IETF proceeds in three stages.

The first stage is an Internet-Draft submission to the IETF's dispatch working group, which evaluates new protocol proposals and routes them to the appropriate existing working group or recommends the formation of a new one. The dispatch submission is based on the protocol overview sections of this white paper and the companion technical specification.

The second stage is engagement with the QUIC Working Group — which maintains the QUIC transport specifications on which QUIP depends — and the Crypto Forum Research Group, which oversees the cryptographic algorithms QUIP employs. Early technical review from these groups reduces the risk of design conflicts that would require costly revision later.

The third stage, contingent on positive reception at dispatch, is the formation of a dedicated QUIP Working Group to develop the protocol to RFC status. This stage requires demonstrating two or more independent interoperable implementations, which is the milestone that formally validates the specification.

9.2 Internet Assigned Numbers Authority (IANA)

IANA manages the registries of protocol parameters that allow internet protocols to interoperate: port numbers, protocol identifiers, URI schemes, and similar namespace allocations. QUIP requires several IANA registrations that will be requested through the IETF standards process as part of RFC publication. These include a dedicated UDP port assignment, an Application-Layer Protocol Negotiation (ALPN) identifier, a URI scheme, a DNS service label, and two new IANA-managed registries for QUIP machine types and error codes.

QUIP's engagement with IANA is procedural rather than political: the registrations follow established processes and do not require policy decisions beyond the scope of normal IANA operations. IANA engagement is noted here because registry allocations are on the critical path to protocol deployment and should be initiated early in the standardisation process.

9.3 Internet Corporation for Assigned Names and Numbers (ICANN)

QUIP's addressing model uses domain names as the namespace for federation nodes. This creates an interface with ICANN's governance of the DNS root and the broader domain name ecosystem. QUIP's relationship with ICANN involves two areas of engagement.

The first is policy compatibility. QUIP's use of DNS for node discovery follows established conventions (DNS SRV records) and does not propose changes to DNS governance or the root zone. ICANN engagement on this dimension is a matter of transparency and coordination, not of seeking permission.

The second is the jurisdictional semantics of country-code TLDs in QUIP addresses. QUIP's addressing model assigns implicit jurisdictional meaning to ccTLDs, which intersects with ICANN's policies on ccTLD delegation and the expectations of national governments. ICANN's Government Advisory Committee (GAC) is the appropriate body for discussion of these implications.

9.4 Regional Internet Registries

The five Regional Internet Registries — AfriNIC, ARIN, APNIC, LACNIC, and RIPE NCC — are the operational bodies that connect QUIP's standardisation work to the ISP communities that will deploy it. Each RIR convenes the network operators and ISPs in its region through policy development processes and annual meetings. QUIP's engagement with the RIRs has a different character from its engagement with IETF and IANA: it is less about formal process and more about building the community of operators who will become early adopters and the interoperability testing partners the standardisation process requires.

AfriNIC (Africa)

AfriNIC is QUIP's highest-priority RIR engagement target. Africa's internet infrastructure presents characteristics that make QUIP's value proposition especially compelling: a rapidly growing ISP ecosystem with strong incentives to assert sovereignty over national identity infrastructure, high mobile connectivity that benefits from QUIC's resilience to network transitions, and a regulatory environment in which national data sovereignty is a genuine policy priority. QUIP's Africa-first deployment strategy is not marketing positioning — it reflects a genuine architectural fit between the protocol's design and the region's needs. The immediate action is a presentation to AfriNIC's technical community, followed by engagement with ZISPA (Zimbabwe Internet Service Providers Association) and POTRAZ (Zimbabwe's telecommunications regulator) to identify a pilot deployment partner.

RIPE NCC (Europe and Middle East) and ARIN (North America)

RIPE NCC and ARIN serve the regions with the highest concentrations of technically sophisticated ISPs and the deepest participation in IETF standardisation. Many IETF working

group participants are also RIPE and ARIN community members. Presenting QUIP at RIPE Meetings and ARIN Public Policy Meetings builds credibility in the community from which IETF working group contributors are drawn. RIPE Labs, RIPE NCC's technical publication platform, is a valuable venue for documenting QUIP's design and early deployment experience.

APNIC and LACNIC

APNIC (Asia-Pacific) and LACNIC (Latin America and the Caribbean) represent regions with large and growing internet user populations underserved by protocols designed primarily for North American and European market conditions. Engagement with these RIRs should begin once a demonstrable reference implementation exists, targeting their annual technical meetings and capacity-building programmes.

10. Governance

QUIP requires a governance body — the QUIP Foundation — to operate the trust infrastructure that the protocol depends on. The Foundation is not a commercial entity and does not control the protocol. It is a custodian of shared infrastructure: the certificate authority, the schema registry, the federation registry, and the transparency logs. The protocol itself is governed through the IETF's open standards process, not by the Foundation.

10.1 Foundation Structure

The Foundation should be incorporated as a nonprofit organisation under a jurisdiction with a strong rule of law and a well-developed nonprofit legal framework. Its governance must include explicit provisions preventing any single member from holding a controlling interest, and must require supermajority votes for changes to the Foundation's core mandate.

The Foundation operates three membership tiers. Founding Members are the initial set of ISPs and technical organisations that contribute to the protocol's development; they hold seats on the Foundation's board and participate in the certificate authority signing ceremonies. Operational Members are ISPs and organisations that operate certified QUIP nodes; they can vote on policy matters but do not hold CA signing roles. Associate Members are technology companies, academic institutions, civil society organisations, and individual contributors who support QUIP's development without operating federation infrastructure.

10.2 Certificate Authority Governance

The Foundation's root certificate is controlled through a threshold signature scheme: no single Foundation member holds the complete root key. Multiple geographically and jurisdictionally distributed members must cooperate to perform any root-level certificate operation. This signing ceremony procedure will be modelled on ICANN's DNSSEC root key signing ceremony and published as a public document, auditable by any interested party.

All certificate issuances, revocations, and key operations are logged to a public transparency log. Any party can monitor this log to detect unexpected certificate operations — the same model used by Certificate Transparency in the web PKI.

10.3 Interoperability and Certification

The Foundation maintains the QUIP Interoperability Test Suite: a collection of test cases that define the mandatory behaviours of the base protocol and each standardised interaction type.

An implementation that passes the relevant test suite levels is certified as interoperable and may be admitted to the production federation registry as an Operational Member.

Interoperability hackathons — structured events where teams from different organisations test their implementations against each other — are held in conjunction with IETF meetings and RIR annual conferences. The first successful interoperability test between two independent implementations is the milestone that formally validates the protocol specification.

> **Milestone: The first successful interoperability test between two independent QUIP implementations — even in a controlled test environment — is the single most important event in QUIP's standardisation journey. It transforms QUIP from a specification into a protocol.**

11. Regulatory Considerations

QUIP is operated by Internet Service Providers, among the most heavily regulated entities in the technology sector. The protocol has been designed with regulatory realities in mind. This section addresses the three regulatory frameworks most relevant to QUIP deployments.

11.1 Data Protection

QUIP's design minimises the personal data that passes through ISP infrastructure. ISP nodes hold session metadata — who communicated with whom, when, and in what type of session — but not message content for sessions using end-to-end encryption. This minimisation limits ISPs' exposure under data protection regulations such as the GDPR, Zimbabwe's Data Protection Act, South Africa's POPIA, and Kenya's Data Protection Act.

The protocol supports the right to data portability (users can move their identity and interaction history between ISPs using the key rotation and session transfer mechanisms) and the right to erasure (a tombstone mechanism for the event log, specified in the technical document, allows content to be removed while preserving cryptographic audit continuity).

11.2 Lawful Interception

QUIP's ISP node can respond to a lawful interception order with identity information (the mapping from QUIP address to subscriber records, held in the ISP's subscriber database), session metadata (which identities communicated, when, and in what session types), and attestation withdrawal (disabling a specific identity under court order). For sessions using end-to-end payload encryption, the ISP node cannot provide message content, as it does not hold the decryption keys. This position is consistent with that of widely deployed end-to-end encrypted communication services and is legally well-established in most jurisdictions.

ISP operators should obtain legal advice on the lawful interception obligations applicable in their specific jurisdiction before enabling end-to-end payload encryption for subscriber sessions. The Foundation will publish guidance on this question for Operational Members.

11.3 Telecommunications Licensing

The Foundation's Operational Membership criteria require that ISP node operators hold valid telecommunications licences in the jurisdictions in which they operate. This ensures that QUIP's federation fabric is operated exclusively by licensed, accountable entities. It also ensures that QUIP deployment is compatible with existing licensing frameworks: deploying a QUIP node is an extension of a licensed ISP's service offering, not a new regulated activity.

Jurisdictional engagement should begin with a regulatory assessment confirming that the planned service falls within the scope of the operator's existing licence. In Zimbabwe, this assessment would engage POTRAZ under the Postal and Telecommunications Act. In Kenya, the Communications Authority. In South Africa, ICASA. The Foundation will maintain jurisdiction-specific guidance for Operational Members.

12. Strategic Positioning

QUIP is a long-term infrastructure evolution, not a short-term product launch. The internet's identity layer has been broken for thirty years. Fixing it requires building infrastructure that will outlast any single organisation, any single technology cycle, and any single regulatory environment. The design choices in QUIP — open standards, ISP-anchored trust, coexistence with the existing web, IETF standardisation — are all made with this long horizon in mind.

12.1 Compatibility with the Existing Internet

QUIP does not require the internet to be rebuilt. It does not require DNS to be replaced, HTTP to be modified, or browsers to be rewritten. It requires only that new software — QUIP clients and ISP federation nodes — be added to devices and servers that already exist, communicating over network infrastructure that already operates. This additive deployment model is the same model that has successfully introduced every major internet layer upgrade of the past two decades, from DNSSEC to IPv6 to TLS 1.3 to QUIC itself.

12.2 Designed for Global Interoperability

QUIP's federation model is structurally opposed to fragmentation. The same protocol that allows a user in Zimbabwe to communicate with a counterpart in Japan operates identically regardless of the national infrastructure those users connect through. The ISP trust model accommodates jurisdictional diversity: different countries' ISPs operate under different regulatory frameworks, and QUIP's architecture allows these differences to coexist within a single global federation rather than requiring regulatory harmonisation as a precondition for interoperability.

12.3 Identity Ownership as Infrastructure

The deepest ambition of QUIP is to establish identity ownership as a property of internet infrastructure rather than a policy preference of application providers. When identity is a protocol primitive — when a user's digital identity is as portable and self-sovereign as their email address, as verifiable as a TLS certificate, and as interoperable as a domain name — the structural conditions for a more equitable and resilient internet exist. Applications built on that infrastructure inherit these properties without having to reimplement them. The internet community benefits from a shared foundation rather than a collection of competing silos.

This is the promise of QUIP: not a better product, but better infrastructure. Infrastructure that returns to users and institutions the control over digital identity that the current architecture has, by accident and accumulation, placed in the hands of a small number of platform intermediaries.

13. Next Steps

The following actions are proposed as the immediate priorities for advancing QUIP from white paper to deployed protocol. They are listed in sequence, as each depends on the completion of the previous.

13.1 Immediate Actions (0–3 months)

- Submit a presentation proposal to the next AfriNIC technical meeting, targeting the engineering track with a 30-minute overview of QUIP's architecture and a demonstration of the reference implementation prototype.
- Initiate contact with ZISPA and POTRAZ to identify one or two Zimbabwean ISPs willing to participate in a pilot deployment under a POTRAZ regulatory sandbox arrangement.
- File Internet-Draft 00 at the IETF datatracker, targeting the dispatch working group, based on the architectural sections of this white paper and the companion technical specification.
- Publish the companion technical specification document and the reference implementation source code under an open-source licence, establishing the public record of the protocol design.

13.2 Near-Term Actions (3–12 months)

- Identify a co-author with academic affiliation to strengthen the protocol's research credibility and open doors to IRTF engagement and conference publication.
- Achieve the first Level 1 interoperability test between two independent implementations. This is the milestone that transforms QUIP from a specification into a protocol.
- Present at RIPE Meeting and begin engagement with RIPE Labs for technical publication, building credibility in the European network operator community.
- Incorporate the QUIP Foundation as a nonprofit entity, draft the founding membership criteria and certificate authority ceremony procedure, and recruit Founding Members from at least three RIR regions.

13.3 Medium-Term Actions (1–3 years)

- Achieve IETF working group adoption of the QUIP base protocol specification, enabling the formal RFC development process to begin.
- Complete the pilot deployment with one or more Zimbabwean ISPs and publish results as a public case study for the benefit of the RIR and IETF communities.
- Extend engagement to APNIC and LACNIC communities, targeting deployment partnerships in Asia-Pacific and Latin American markets.
- Develop the mobile client profile and associated interoperability tests, addressing the largest single end-user deployment context for QUIP in developing markets.

> **The long arc of this work is measured in years, not months. Each step in this sequence builds the institutional legitimacy, technical credibility, and operational evidence that a protocol needs to achieve the level of adoption where it becomes infrastructure. The work begins now.**

QUIP — QUIC Identity Protocol

Institutional White Paper v1.0 — March 2026

Companion document: QUIP Technical Specification, Draft v1.0