KYVERGE

Teaser

A decentralized protocol for programmable identities, secure communication, transport, and verifiable interactions.

Communication is becoming infrastructure.

People, organizations, applications and AI agents increasingly need secure, independent and portable communication.
Not another platform chat. Not another inbox. Not another social media account.
KyVerge is a decentralized transport infrastructure for privacy-first communication, programmable identities, asynchronous retrieval, and verifiable digital interactions.

Programmable identities

Multiple identities for people, companies, apps, devices, and agents, structured as hierarchical trees, from root identities to scoped derived identities.

Decentralized and portable

No central platform, inbox, or social account: encrypted digital objects can move asynchronously across a decentralized transport layer and remain portable across clients, applications, and identity context.

Verifiable and auditable

Receipts, audits, and optional blockchain anchoring create evidence of interaction, with an architecture designed to support incentive-based infrastructure.

VERSION
v0.1.2
Alpha protocol foundation

AUTHOR
Filippo Recami
KyForge s.r.o.

DATE
June 2026
Prague, Czech Republic

Preliminary overview. Not a securities, investment or token-offering document. Technical, legal and commercial assumptions are subject to validation.

The opportunity: secure communication must become independent and verifiable

Digital communication is still mostly account-bound, platform-controlled, and hard to verify. End-to-end encryption protects content, but it does not solve portability, offline delivery, infrastructure dependency, or evidence. AI agents and programmable workflows make these limits increasingly visible.

Centralized Control and Security

Communication and digital transport still depend on operators that control identity, access, delivery, storage and recovery, creating concentrated security, censorship and trust chokepoints.

Flat Identities

People, companies, apps and agents are forced into rigid account models instead of scoped, portable, cryptographic identities.

Weak Portability

Communication, identity, encrypted objects, and recoverable interaction history are usually locked inside specific platforms, inboxes, clients, or service providers.

No Shared Ecosystem

There is no open, sustainable layer for encrypted object exchange, asynchronous retrieval and cross-application communication.

Missing Evidence Layer

Digital interactions rarely generate cryptographic evidence strong enough for audits, disputes, compliance or legal-grade verification.

Agent-era identity gap

Automated systems need limited authority, signatures, encrypted channels, rotation, revocation and evidence trails.

The chain of necessity

KyVerge is built on a simple premise: private communication cannot be solved by encryption alone. Once identities become independent and delivery becomes decentralized, each layer creates a new requirement for the next one.

- Private communication needs **independent identities and encrypted transport**.
- Offline delivery needs **decentralized storage**.
- Decentralized storage needs **nodes to contribute** to bandwidth, storage, availability and retrieval service.
- But nodes do not participate for free at scale: without **incentives**, the network cannot rely on stable voluntary contribution.
- Node incentives need **verifiable contribution**: receipts, audits and scoring.
- Economic security needs **penalties**, staking and slashing.
- **Blockchain** adds the public layer for incentives and settlement, while enabling **message registration, proof of transport, token transactions and economic value**.

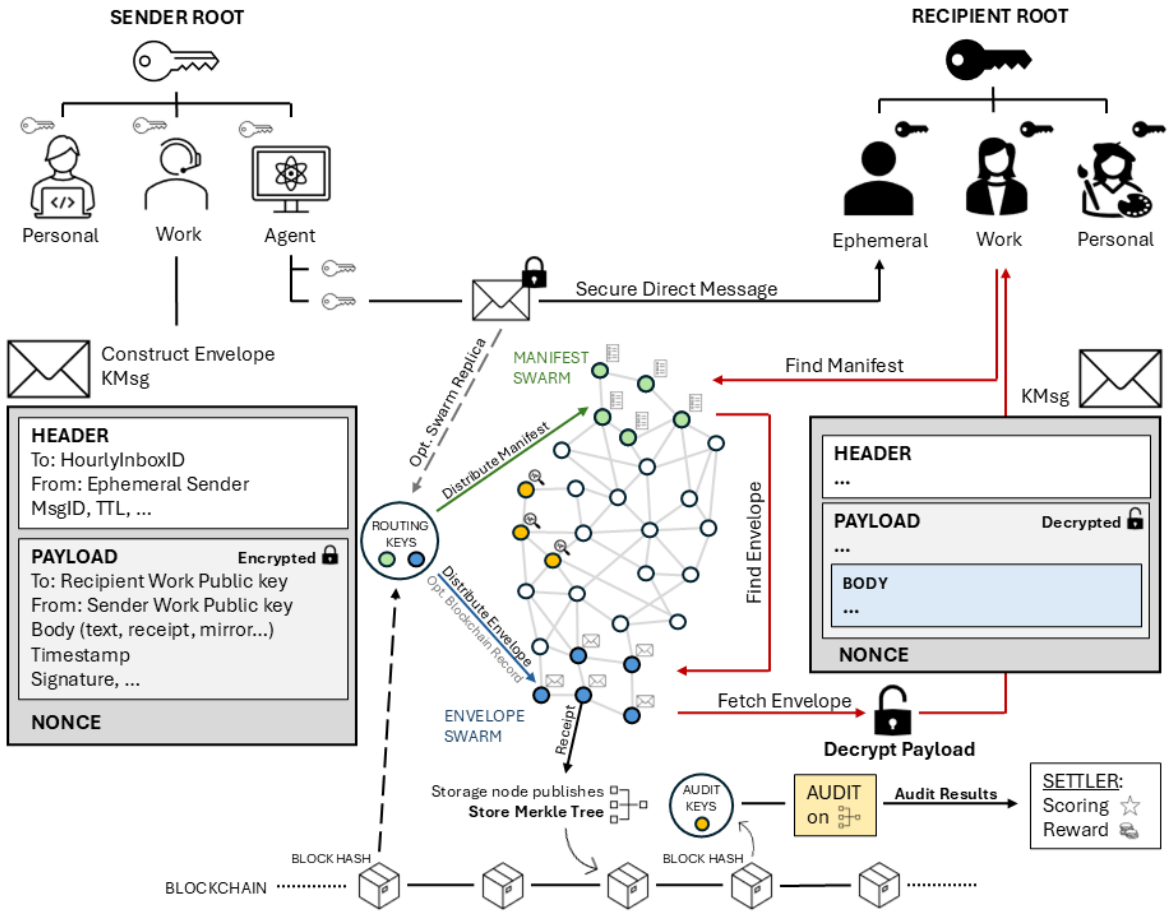
KyVerge composes these layers into one protocol model: private communication, resilient delivery and self-sustaining decentralized infrastructure.

The KyVerge solution

A protocol substrate where programmable identities exchange encrypted digital objects, retrieve them asynchronously through decentralized swarms, and attach evidence to infrastructure work.

1	2	3	4	5
IDENTITIES	**ENVELOPE**	**SWARM**	**EVIDENCE**	**AUDIT**
Root and derived keys for programmable users, devices, organizations and agents.	Signed and encrypted objects for messages, files and proofs, organized through rotating time windows	Asynchronous retrieval through recipient-oriented decentralized swarms.	Receipts, notary bundles and optional blockchain records for transport, storage and retrieval.	Scoring, reputation and future settlement for infrastructure work.

System view



High-level protocol flow: programmable identities, encrypted envelopes, manifest and envelope swarms, receipts, audits, settlement and optional blockchain registration

Messages	Files	Proof	Agents
Private human and organizational communication.	Encrypted blobs referenced through content-addressed storage.	Receipts, certificates, identity proofs and evidence bundle.	Scoped communication for automated clients and AI systems.

03 KYVERGE TEASER

From one open protocol to multiple product surfaces

KyVerge is an open-source protocol designed to let third parties build applications on top of encrypted, identity-bound transport. Messaging is the first tangible surface, but the larger opportunity is a reusable infrastructure where people, organizations, applications and AI agents exchange digital objects with verifiable delivery, selective disclosure and evidence.

Programmable identities

Root and derived identities allow users, companies, departments, devices and agents to operate through separate keys. Future ZKP-based disclosure can prove authority, delegation or linkage only when needed, enabling privacy-preserving permission systems.

Secure messaging & files

Private messaging and encrypted document exchange are the first product surfaces. Premium clients can add larger storage, longer retention, structured groups, advanced key wallets, passkey-style access and enterprise-grade recovery.

Verifiable delivery

Receipts, notary bundles, timestamps and optional blockchain anchoring can prove transport, delivery, disclosure and integrity without exposing private content. This creates a foundation for contractual, commercial, institutional and regulated communication.

Legal-grade communication

KyVerge can evolve toward eIDAS-aligned ERDS / QERDS models for electronic registered delivery, combining secure client-side keys, verifiable transport and optional semi-centralized service layers for legal, corporate and public-sector use cases.

Enterprise workflows

Role-based communication between companies, departments, tools, devices and AI agents can be built on portable identities rather than platform accounts. This enables auditable delegation, secure document flows and machine-to-machine communication.

Blockchain services

Blockchain can be used as a public verification layer for commitments, message registration, naming, entropy and settlement. Private communication stays encrypted and off-chain, while public chains provide trust anchors where verifiability matters.

Decentralized social apps

Portable identities, encrypted transport, verifiable interactions and optional blockchain anchoring can support decentralized or semi-decentralized social networks and applications where users keep stronger control over identity, data and reputation.

Infrastructure network

Storage, retrieval and audit participants create the operational layer of the protocol. Receipts, scoring, audits and staking turn decentralized infrastructure into an accountable service network.

Token economy

The token can become the economic rail of the network: rewarding measurable infrastructure work, while enabling microtransactions, premium services, naming rights and settlement across the ecosystem.

Why this can become valuable

Near-term revenue surfaces

Proprietary clients, hosted infrastructure, secure file exchange, advanced key wallets, enterprise integrations, verifiable and notarized communication services, developer tooling and premium storage or retention services.

Long-term network effects

Identity portability, reusable evidence, decentralized or semi-decentralized social applications, naming markets, protocol-native payments, storage and audit incentives, public trust anchors and third-party clients built on the protocol.

The strategic point: KyVerge is not a generic crypto wrapper. It is an open protocol for encrypted, identity-bound transport where blockchain, tokens and anchoring are used only when they support real infrastructure work, legal-grade evidence, public commitments, naming or settlement.

Current alpha and next steps

The current v0.1.2 alpha already implements the core protocol baseline. The next stage is focused on external testing, security hardening, legal structuring and commercial validation.

Implemented in v0.1.2

- Hierarchical Ed25519 identity derivation via Rust/WASM
- End-to-end encrypted typed envelopes
- Direct messaging, receipts, attachments and mirror flows
- RID/WRID recipient-oriented storage
- Manifest and envelope swarms
- libp2p / DHT-based peer discovery and storage RPC
- Badger-backed envelope, manifest and audit storage
- Storage receipts and notary bundles
- Repair scheduling and replica checks
- Merkle commitments and possession challenges
- Receipt-backed targeted audits
- Storage-target and auditor scoring
- Anti-abuse primitives: rate limits and adaptive PoW
- Work-accounting hooks, settlement interfaces and demos

Next layers

- External testing and network validation
- Security review and protocol hardening
- Production deployment, bootstraps and relay operations
- Forward-secrecy and metadata protections
- Zero-knowledge identity lineage
- Blockchain anchoring runtime and naming
- Token settlement, staking and slashing policy
- Conflict resolution and formal dispute logic
- Legal review for evidence-oriented products
- Developer SDK and go-to-market validation

Project status and release strategy

KyVerge is moving from protocol alpha to product and network validation. The current stack is already designed around a dual model: an open protocol layer and proprietary product surfaces built on top.

The protocol is already supported by two working applications:

- **KyLocker** is a key-management client for generating, storing and managing identity trees, derived keys and passkey-style access.
- **KyTalks** is a functional secure messaging client built on top of the protocol, demonstrating encrypted communication, identity-based transport and the first user-facing experience of the KyVerge stack.

The intended model is open protocol, proprietary product surfaces. The KyVerge protocol should become open source because trust, interoperability, security review and third-party adoption require transparency and auditability. At the same time, commercial clients such as KyTalks, KyLocker and future enterprise products can remain closed source, allowing KyForge to build revenue-generating applications, hosted services, premium features and integrations on top of the shared protocol layer.

The release strategy is progressive. The KyVerge protocol repository is expected to be opened in coordination with the first public application releases and the broader network/token launch. In the initial phase, the network may rely more heavily on official KyVerge-operated infrastructure to guarantee reliability, onboarding and user experience. As participation grows, storage, audit, retrieval and settlement functions can progressively move toward broader decentralization and independent network operators.

Current phase

The current phase is focused on protocol hardening, external testing, security review, legal structuring, product design and go-to-market validation with selected strategic partners. A technical whitepaper and alpha documentation are available for selected reviewers, partners and early-stage investors.