UNIKEY

A Distributed Authorization Network

The missing authority layer of the internet.

LAYER 01 **Identity & Agent Trust**	*Is this a known, trusted agent?*
LAYER 02 · UNIKEY **UniKey Authorization**	*Was this specific action explicitly authorized before it executed?*
LAYER 03 **Payment Execution**	*How do payments move securely?*

EXECUTIVE SUMMARY

The internet was built to move information. It was never built to prove authority.

> *Identity systems verify who is acting. UniKey verifies what they are doing. They verify the agent. UniKey verifies the action.*

UniKey is a distributed authorization network — device-bound, cryptographically provable, and pre-execution. It operates upstream of every settlement system in the world: card networks, bank transfers, blockchains, smart contracts, APIs. It does not move value; it strengthens the authorization signal those systems receive before value moves.

The contribution is structural. Every digital action carries a Trust Packet — a signed proof that this exact action was authorized by the rightful device holder. The proof is fresh, non-replayable, and deterministically verifiable by any participating system without shared state, proprietary integrations, or centralized authorization services. Authority precedes execution. Execution may precede settlement.

01 The internet's authorization model assumes that possession of a credential is equivalent to permission. In remote environments, that assumption breaks. Credentials scale abuse.

02 UniKey replaces credential-based authorization with cryptographic, action-bound authorization. A stolen credential cannot produce a Trust Packet. Scalable remote fraud structurally collapses.

03 The protocol leverages globally deployed DKIM and DNS infrastructure. UniKey introduces no new global certificate authority and no consensus network. The substrate is fifteen years operationally mature.

04 The asset comprises six published RFC-style specifications, 100+ patents granted and pending, reference libraries, and active engagement with the NIST National Cybersecurity Center of Excellence.

05 The business model is patterned on Visa: *UniKey does not authorize actions. UniKey licenses the protocol to those who do.* Authority is upstream from settlement. Sending Trust Packets is free. Verification is where value is exchanged.

SECTION 01 · THE STRUCTURAL GAP

Possession of a credential is not equivalent to authority. The internet is built as if it were.

Most digital systems verify transactions after submission. A payment request is sent to a processor. An API call reaches a server. A smart contract is broadcast to a chain. The receiving system checks credentials, tokens, or keys, and then decides whether to proceed.

This model assumes that possession of a credential is equivalent to authority. In remote environments, that assumption breaks down. Credentials are stolen. Sessions are hijacked. Tokens are replayed. Private keys are extracted. Once compromised, they can be reused at scale.

Settlement systems are not the weakness. Authorization is. As commerce becomes fully digital and increasingly autonomous, the gap becomes more consequential. Machines act at machine speed. Agents transact across domains. Systems execute commands without human visibility. The requirement is no longer identity alone. The requirement is verifiable authority prior to execution.

1.1 THE VISIBLE SYMPTOM: FRAUD AT SCALE

Online fraud scales because remote actors can execute actions without device-bound proof of authority. Credential-based remote abuse — card-not-present fraud, account takeover, push-payment fraud, automated bot attacks — accounts for the overwhelming majority of digital fraud losses globally. It scales because the underlying compromise (a stolen credential) is reusable.

$28B
Card-not-present fraud, projected 2026

$23B
Account takeover fraud, US 2023

$442B
Global fraud losses 2025 (INTERPOL)

80%+
Of data breaches originate from stolen credentials (Verizon DBIR 2024)

$9.4M
Average cost of a data breach, US 2024 (IBM)

97%
Of organizations saw AI-facilitated attacks rise in 2025

1.2 THE INVISIBLE SYMPTOM: THE AGENTIC BOTTLENECK

The fraud problem is the visible symptom of a deeper architectural gap. The same gap is now constraining the next wave of digital infrastructure: autonomous agents acting on behalf of users.

AI agents cannot be trusted to act freely across the internet because no infrastructure exists to verify that any specific action was authorized by the human or organization the agent purports to represent. Every agent transaction today is a leap of faith. The bottleneck is not compute. It is not models. It is authorization.

The economic stakes are commensurate. PwC projects $15.7T in AI economic impact by 2030. The infrastructure gap that gates that impact is verifiable, distributed, pre-execution authorization.

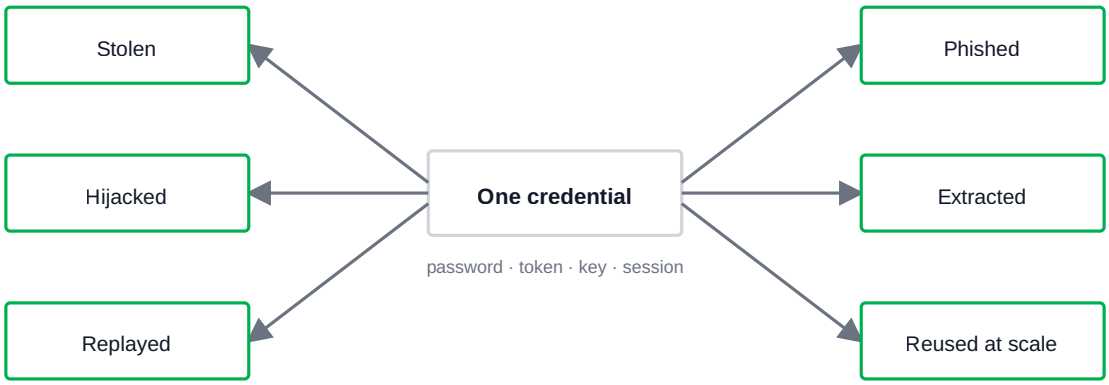

Figure 1 · A single compromised credential becomes scalable abuse across multiple attack surfaces. Possession is treated as authority.

UniKey closes the gap by requiring cryptographically verifiable authority before execution. A stolen credential cannot produce a Trust Packet. A replayed token cannot produce a Trust Packet. The compromise boundary shifts from remote credential theft — which scales — to physical device or key compromise, which does not.

> *Fraud reduction is one application of this architectural shift. Secure autonomous execution is another. The broader category is distributed authority itself.*

SECTION 02 · THE UNIKEY ARCHITECTURE

Four primitives. One authority layer. No central control.

UniKey is built on four cryptographic primitives. Together they constitute a distributed, pre-execution authorization layer that operates without consensus overhead, without a global ledger, and without a central certificate authority.

2.1 AUTHORITY ANCHORS

Who holds the authority to act? Any person, device, or enterprise system that establishes cryptographic authority through domain-based keys. Authority is expressed through public keys distributed via DNS — the same global infrastructure that has supported DKIM-signed email for over fifteen years. No new certificate authority is introduced. Authority is independently verifiable by any counterparty. The architecture is peer-to-peer rather than hierarchical: every domain, every device, every agent holds its own anchor.

*Specified in **UniKey RFC-1300** — Device Authority & OS Integration.*

2.2 TRUST PACKETS

Was this action authorized before execution? A Trust Packet is a self-contained, cryptographically signed data structure asserting identity, authority, and intent for a specific action. Each packet is non-replayable, deterministically verifiable, and transport-agnostic. It can travel via HTTPS, SMTP, message queues, or QR/NFC handoff with cryptographic integrity preserved. Verification is stateless and does not require shared session state or prior bilateral integration.

Verification targets sub-five-millisecond latency on commodity hardware (RFC-2001 §7). Any ambiguity in canonicalization, signature, temporal validity, or replay state results in immediate rejection. The architecture fails closed by design.

*Specified in **UniKey RFC-2001** — Trust Packet Format & Canonicalization.*

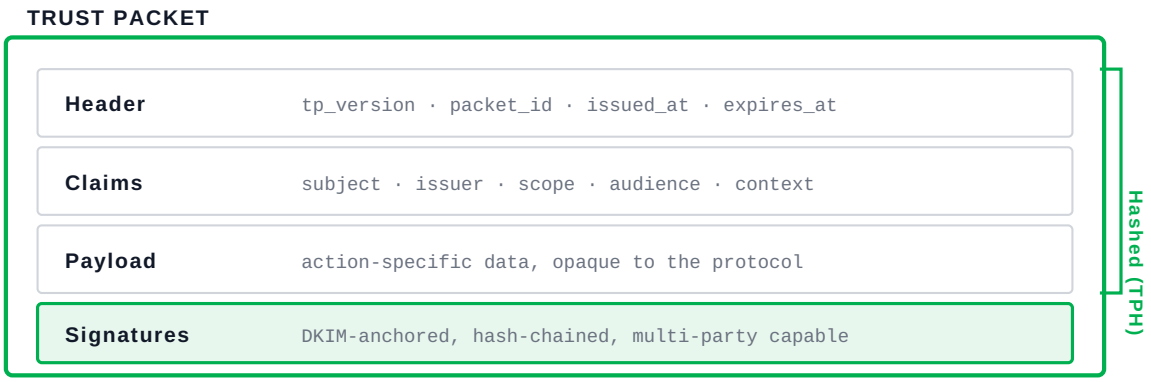

Figure 2 · Trust Packet anatomy. Header, claims, and payload are canonicalized and hashed (the TPH). Signatures attest to the TPH and travel with the packet.

2.3 AUTHORIZATION CERTIFICATES

What is the tamper-evident record? An Authorization Certificate is a hash-chained record of a complete multi-party transaction sequence. Each Trust Packet in the chain incorporates a cryptographic hash of all preceding packets. Modify any step, and the entire chain breaks. All public keys necessary for verification are embedded, enabling self-contained validation by any party — without external lookups, without shared databases.

The certificate is the artifact that makes complex transactions cryptographically resolvable. Disputes that today are operationally adjudicated — friendly fraud, repudiated approvals, contested fulfillment — become questions of signature verification rather than testimony.

*Specified in **UniKey RFC-2001**.*

2.4 AUTHORIZATION LEDGERS

Where is the permanent record? An Authorization Ledger is a distributed, append-only record of Authorization Certificates. Each party in a transaction can maintain an independently verifiable record of every action they participated in — without relying on UniKey-operated central infrastructure or shared consensus systems. The ledger is permanent audit infrastructure by default. It is generated as a byproduct of normal operation, not as a separate data-collection exercise.

*Specified in **UniKey RFC-5003** — Authorization Flow & Verification Architecture.*

SECTION 03 · VERIFICATION FLOW

Six packets. Six signatures. Every party authenticated. No shared secrets.

UniKey's authorization flow separates authority verification from action execution. Authority is verified first. Execution follows only after verification succeeds. The flow scales from single API calls to complex multi-party payments without changing the underlying primitive.

3.1 THE SINGLE-ACTION FLOW

For a simple authorized action — an API call, an agent invocation, a service request — the flow has three principal participants: the caller, the verifier, and the destination. The caller's library constructs a Trust Packet describing the specific action and DKIM-signs it with the caller's domain key. The packet travels point-to-point to the verifier as a single-hop signed delivery. The verifier validates the signature against DNS-published public keys and forwards a standard HTTPS request to the destination API. The destination does not need to know UniKey exists.

Three deployment models are supported, depending on the integration constraints of the destination system. The verifier may relay the authorized HTTPS call (verifier-as-relay). The destination may receive the Trust Packet alongside an HTTPS request and correlate them (target-receives-authorization). Or the destination may run an embedded verifier and accept Trust Packets directly (embedded-verifier). The protocol is the same in all three. The deployment choice depends on latency, integration cost, and trust topology.

3.2 THE MULTI-PARTY PAYMENT FLOW

Payments are the hardest case. A payment is not a single authorization; it is a sequence of authorizations across six or more parties, with cryptographic integrity required at every hop. The architecture handles it as a chain of Trust Packets, each signed by its originator and hash-chained to the prior packet.

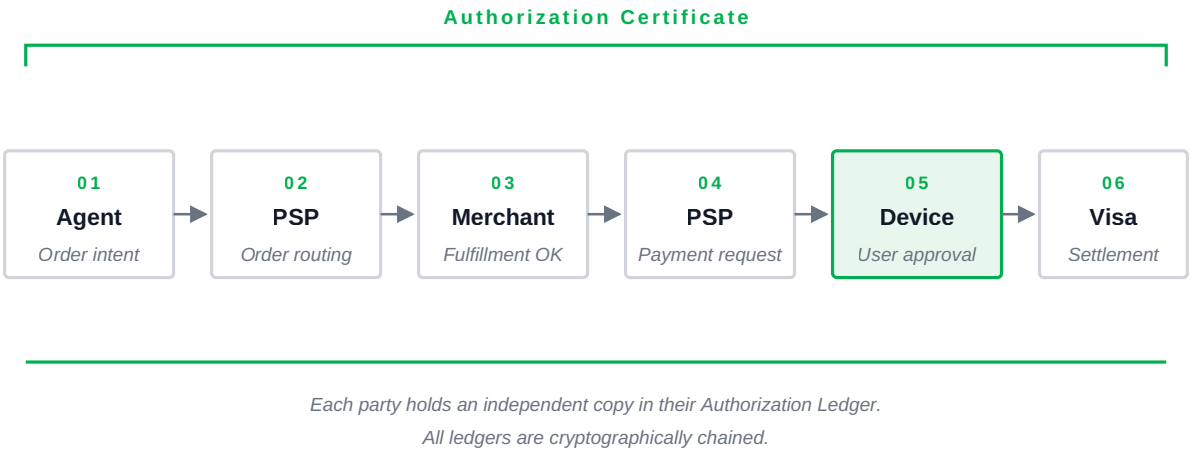

Figure 3 · The multi-party payment flow. Six Trust Packets, each DKIM-signed by its originator. Each packet incorporates the hash of all preceding packets. The full chain is the Authorization Certificate.

Several architectural properties follow from this structure:

- **The merchant never sees payment credentials.** The credential lives in the device's Secure Enclave and is invoked only at step 5. The merchant approves *fulfillment*, not *payment*. PCI-DSS scope drops to zero for participating transactions.
- **Network-level adoption propagates without integration.** If Visa adopts UniKey at the network layer, the protocol propagates through existing PSP relationships to roughly 80 million merchants worldwide. Merchants do not change their POS, their integrations, or their workflow. They simply stop touching credentials.
- **Disputes become resolvable, not adjudicated.** The Authorization Certificate is unambiguous, signed evidence at every party. Friendly fraud, repudiated approvals, and contested actions become cryptographically resolvable rather than operationally arbitrated.
- **Card-on-file storage becomes obsolete.** No party except the device holds the credential. The data-breach risk that flows from card storage at merchants and processors disappears for participating transactions.

*Specified in **UniKey RFC-5003** — Authorization Flow & Verification Architecture.*

SECTION 04 · DISTRIBUTED AUTHORITY

Blockchain decentralized settlement. UniKey decentralizes authority.

Two architectural ambitions in modern computing have aimed to remove centralized choke points from the digital economy. They address different layers and produce different properties.

Blockchain technology decentralized settlement by distributing ledger state across many nodes and enforcing consensus on what was recorded. Once a transaction is committed, it cannot be altered without consensus. Blockchain answers the question: *what happened?*

UniKey decentralizes authority by distributing cryptographic verification across DNS, devices, and verifiers. It does not require global ledger replication or consensus overhead. It performs stateless verification of device-bound cryptographic authority prior to execution. UniKey answers the question: *who was permitted to make it happen?*

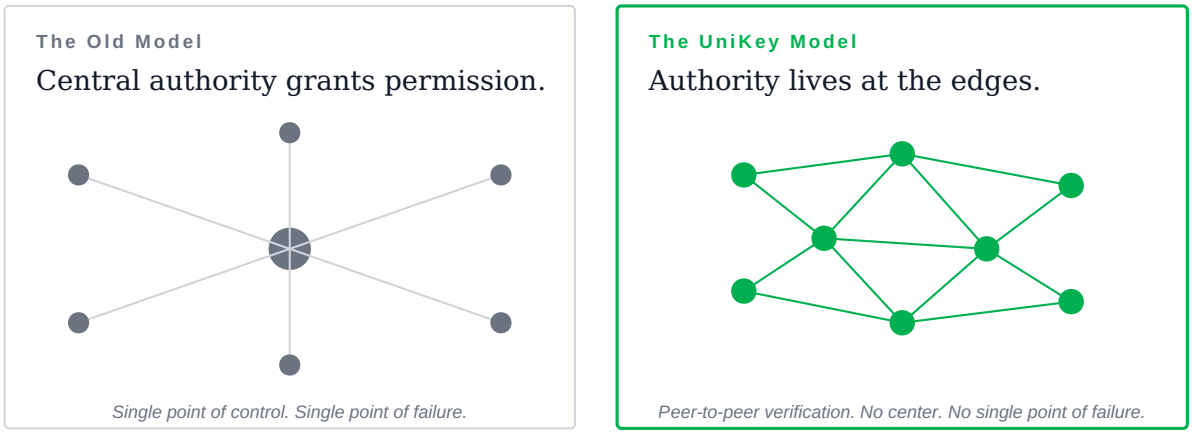

Figure 4 · Centralized authorization (left) versus distributed authorization (right). UniKey eliminates the single point of compromise.

UniKey is rail-neutral and execution-agnostic. It does not move funds. It does not clear transactions. It does not store value. It verifies authority. Because it operates at the authorization layer, it integrates with existing card networks, bank transfer systems, real-time payment rails, stablecoins, and smart contract platforms without displacing them.

> *DKIM is not the product. It is the foundation. UniKey is the authorization architecture built on top of it.*

For more than fifteen years, DKIM has enabled domains to publish cryptographic public keys that can be globally validated in a distributed and stateless manner. UniKey extends this model beyond message integrity to authorization integrity. Because the substrate is already deployed and operationally hardened, UniKey introduces no consensus overhead and no centralized control.

SECTION 05 · FRAUD AND THE AI ECONOMY

Scalable, credential-based fraud structurally collapses under pre-execution authorization.

Fraud reduction is not the category UniKey defines. But it is the most measurable application of distributed authority, and it is the application most directly visible to operators evaluating the architecture commercially.

5.1 WHY FRAUD SCALES TODAY

Online fraud scales because remote actors can execute actions without device-bound proof of authority. Card-not-present fraud, account takeover execution abuse, push-payment fraud, and bot-driven automation attacks are all consequences of weak upstream authorization. When authority is reduced to credentials, those credentials can be reused at scale. Fraud becomes industrialized.

By requiring cryptographically verifiable authority before execution, UniKey materially compresses the scalable portion of remote fraud. A stolen card number is insufficient. A compromised password is insufficient. A replayed token is insufficient. Fraud shifts from credential-based remote abuse to non-scalable physical compromise.

5.2 THE ADDRESSABLE SURFACE

The fraud categories most directly addressed by pre-execution authorization are precisely the categories that scale through credential reuse.

- **Card-not-present fraud.** A stolen card number cannot produce a Trust Packet. The credential lives only in the device's Secure Enclave; remote possession of card data does not authorize anything.
- **Account takeover execution.** An attacker holding a stolen password or hijacked session cannot complete an authorized action. The action requires a fresh, device-bound signature that the attacker cannot produce.
- **Synthetic identity fraud.** Fabricated identities cannot establish Authority Anchors that are verifiable by counterparties. The identity-anchor structure is rooted in real domain control.
- **Push-payment fraud.** The user-approval step on the device is per-action and per-recipient. Authorization cannot be redirected after the fact.
- **Friendly fraud and repudiation.** The Authorization Certificate is an unambiguous signed record of user approval. Disputes become resolvable rather than adjudicated.

- **Bot-driven automation attacks.** Automated abuse cannot generate valid Trust Packets at scale; each action requires a fresh device-anchored signature.

Fraud categories that *remain* are categories that do not scale through credential reuse: physical device theft, social engineering attacks where the user is deceived into approving a malicious action, and supply-chain compromise of trusted code paths. These are bounded, non-scalable, and addressed by other layers of the security stack. UniKey does not eliminate all fraud. It eliminates the kind that scales.

5.3 THE AGENTIC-ECONOMY BOTTLENECK

The same architectural property that compresses scalable fraud also resolves the constraint preventing AI agents from acting freely across the internet. The agentic economy has not stalled for lack of capable models. It has stalled for lack of authorization infrastructure.

Without verifiable per-action authorization, no operator can responsibly allow an agent to act autonomously across organizational boundaries. The default has become severe restriction: agents act only within tightly scoped sandboxes, only with extensive review, only at machine-supervised throughputs. The economic cost of that default is substantial — projections of AI-driven economic impact (PwC: $15.7T by 2030) implicitly assume that agents can transact at scale, which today they cannot.

UniKey is the missing infrastructure. Every agent action carries a Trust Packet asserting that this specific action was authorized by the principal it represents, signed by the device that holds the principal's authority anchor, verifiable by every counterparty. Agents become first-class digital actors. The bottleneck dissolves.

> *Fraud is the visible application. The agentic economy is the larger one. Both reduce to the same architectural property:* **distributed, cryptographically verifiable, pre-execution authorization.**

SECTION 06 · THE BUSINESS MODEL

Visa does not move money. UniKey does not authorize actions. Both license the network.

> *The economic model is patterned directly on Visa. Visa verifies transactions and licenses the network to the institutions that move money. UniKey verifies authority and licenses the protocol to the institutions that authorize actions.*

6.1 THE ECONOMIC STRUCTURE

Sending Trust Packets is free. Any participant — any agent, any service, any device — can construct and send a Trust Packet at no cost. Universal participation at zero marginal cost is the precondition for the network to scale.

Verification is where value is exchanged. The institutions that operate verification endpoints — payment networks, telecommunications carriers, SASE platforms, enterprise gateways, certificate authorities — collect fees for each Trust Packet they verify. The economics are metered: per action, with no natural ceiling at agentic-commerce scale.

The protocol itself is an open standard. Licensees pay for the right to operate verification endpoints, deploy the architecture inside their products, and use the IP foundation. The model is ARM-style: open standard, licensed ecosystem, no proprietary lock-in.

6.2 THREE REVENUE STREAMS

Figure 5 · Three revenue streams. Verification and licensing are the primary commercial layers; authorization intelligence is generated as a byproduct of the network's normal operation.

Verification fees are the primary metered revenue stream. Every Trust Packet verified by a network operator generates a per-action fee. At agentic-commerce scale — billions of agent actions daily as autonomous systems become routine — this is metered infrastructure revenue with no natural ceiling.

Licensing fees are paid by the institutions that operate verification endpoints or deploy the protocol inside their products. Payment networks license to enable network-level adoption. Telecommunications carriers license to operate verification using their existing trust relationships with billions of devices. Device manufacturers license to integrate the architecture into Secure Enclaves and OS-level workflows. Enterprise security platforms license to embed verification in their edge and cloud products.

Authorization intelligence emerges as a byproduct of the network's normal operation. Every transaction produces an Authorization Certificate. Aggregated across billions of transactions, the resulting Authorization Ledger is a real-time map of what was authorized, by whom, through which authority chain. It is sold as fraud detection, compliance reporting, threat intelligence, and risk-scoring services — generated automatically, not collected separately.

6.3 WHY THIS MODEL SCALES

The economics compound at three levels. Every additional verifier increases the network's reach. Every additional licensee increases verification volume. Every additional transaction enriches the authorization-intelligence corpus. Each layer reinforces the others.

Founding partners — institutions that commit early to the standard and operate verification at scale — receive preferential terms on the commercial layer. The objective is to seed the network with the institutions that have the deepest existing trust relationships with the largest number of digital actors.

SECTION 07 · ADOPTION PATHWAYS

Five categories of organization. Five commercial paths. One protocol.

The architecture composes naturally with five categories of organization. Each represents a distinct commercial path with a distinct business model. The asset is structured to license to all of them.

7.1 AI AGENT PLATFORMS

The infrastructure that lets agents act autonomously across domains. UniKey is the verification layer their actions must pass through. Without distributed pre-execution authorization, no operator can responsibly allow an agent to transact at scale. The agentic-platform category — encompassing model providers, agent frameworks, and orchestration platforms — is the most direct beneficiary of the architecture and the most natural early founding partner.

7.2 PAYMENT NETWORKS

Visa, Mastercard, American Express, and Discover are the natural licensees in this category. Network-level adoption propagates through existing PSP relationships to roughly 80 million merchants worldwide without merchant-side integration. The structural outcomes — card-not-present fraud eliminated, card-on-file storage obsoleted, merchant PCI scope dropped — accrue to the entire network at once.

The license model is flat-fee annual at scale, comparable to architectural licensing in other infrastructure categories. The economic logic is straightforward: license fees are a fraction of the eliminated cost categories. CNP fraud alone, projected at $28 billion in 2026, dwarfs any plausible licensing fee.

7.3 TELECOMMUNICATIONS CARRIERS

Carriers operate trust relationships with billions of devices through SIM provisioning, network authentication, and OS-level integrations. They are natural verification operators, particularly for actions that involve the device's network identity. The carrier category — encompassing AT&T, T-Mobile, Vodafone, and the broader GSMA membership — operates verification at network scale and licenses the protocol to extend it.

7.4 DEVICE MANUFACTURERS

Apple, Samsung, and Google are the direct licensees in this category. UniKey integrates with the Secure Enclave and OS-level credential workflows that these manufacturers already operate.

> *Every device becomes a magic wand — the cryptographic origin point for authorized actions across every connected service the user touches. The biggest leap in what a phone can do for the user since the App Store.*

The licensing model is a per-device royalty, comparable to ARM's IP licensing rates ($0.30–$1.00 per device historically), with credential provisioning integrated into existing Secure Enclave workflows. At full smartphone-fleet scale, the device-licensing stream alone is structurally significant.

7.5 ENTERPRISE SECURITY PLATFORMS

Cisco, Cloudflare, Amazon, and Google Cloud each operate global edge or cloud infrastructure where verification at scale composes naturally with their existing services. Several are building agentic-security products that UniKey would extend or replace at the architectural layer. The licensing path here is operator-led: the platform licenses the protocol, embeds verification in their edge or cloud product, and offers it to their enterprise customer base.

7.6 ACQUISITION PATHWAY

For an acquirer in any of the categories above, the natural path is to acquire the IP foundation, the protocol specifications, and the reference libraries — and then to operate verification at scale using existing infrastructure. The acquirer becomes both the operator of the verification network and the licensor of the protocol to other parties. The asset is structured for this outcome: ARM-style, IP-heavy, with the operational scale to be supplied by the acquirer rather than the asset.

SECTION 08 · OPEN STANDARDS AND INTELLECTUAL PROPERTY

Governed by published specifications. Protected by an international patent portfolio.

UniKey is not a proprietary product. It is a published standard with a licensed ecosystem. Specifications are open and publicly available. Reference implementations are documented. The objective is the establishment of a verifiable, standardized authorization layer that can operate at internet scale — supported by an IP foundation that protects the architectural primitives and ensures the standard is operated rather than copied.

8.1 THE RFC SERIES

The protocol is defined in six published RFC-style specifications, all publicly available on GitHub. Each specification is referenced in the others, and conformance is testable against the published normative requirements.

RFC	TITLE	SCOPE
RFC-1000	**Master Index**	Index of the UniKey RFC series, conformance levels, and normative cross-references.
RFC-1200	**Delegation Profile**	How authority can be delegated and how delegation chains are verified without scope expansion.
RFC-1300	**Device & OS Integration**	Device authority model, Secure Enclave integration, OS-level credential workflows.
RFC-2001	**Trust Packet Format**	Canonical packet structure, canonicalization rules, hashing, signatures, verification procedure.
RFC-3001	**DNS Hardening Algorithm**	Multi-resolver consensus, key validation, anti-poisoning logic for verifiers.
RFC-5003	**Authorization Flow**	Verification architecture, multi-party flow, role definitions, conformance requirements.

All specifications: **github.com/Swoop-Now/unikey-spec**

8.2 PATENT PORTFOLIO

UniKey is protected by an international portfolio of over 100 granted and pending patents across multiple jurisdictions. The portfolio covers:

- Distributed cryptographic authorization architectures
- Replay-resistance mechanisms for cryptographic action proofs
- DNS-based key distribution and validation, including multi-resolver consensus methods
- Trust Packet construction, canonicalization, and chaining
- Cross-domain authority verification without bilateral integration
- Device-bound authorization workflows integrated with Secure Enclave architectures

The portfolio is the structural moat for the licensing model. It ensures that the standard, once published, is operated under license rather than reimplemented and operated outside the licensing framework. Strategic acquisition or licensing of the portfolio is the natural path for partners scaling the architecture to global deployment.

8.3 STANDARDS-BODY ENGAGEMENT

UniKey has been submitted to the U.S. National Cybersecurity Center of Excellence (NIST NCCoE) as a recommended solution within their AI Agent Identity and Authorization framework. Independent threat-model review has been completed by Black Duck Software, with findings incorporated into the architecture. Engagement with additional standards bodies and recognized security researchers is ongoing.

> *The objective is not proprietary lock-in. It is the establishment of a verifiable, standardized authorization layer that can operate at internet scale — protected by the IP foundation that ensures the standard is operated rather than copied.*

CLOSING

Every digital action should carry proof of authority.

> *UniKey ensures that proof exists before systems act.*

Digital systems have matured in their ability to move value. They have not matured equally in their ability to verify authority before action. As commerce becomes autonomous and cross-domain, the distinction between identity and authority becomes critical.

UniKey defines a new infrastructure layer: distributed, device-bound, pre-execution authorization. Fraud reduction is one application. Secure autonomous execution is another. The broader category is distributed authority itself.

The asset is built. The specifications are published. The IP foundation is in place. The architecture is ready for the institutions that will operate it at internet scale.

ACQUISITION · LICENSING · FOUNDING PARTNER DISCUSSIONS

john@swoopnow.com

TECHNICAL SPECIFICATIONS

github.com/Swoop-Now/unikey-spec

ADDITIONAL RESOURCES

unikeyid.com

OPERATOR

Swoop In Technologies LLC