UniKey ID Security Architecture

The new trust layer for identity, payments, and access

Built on email. Hardened with cryptography. Ready for scale.

Gold-standard cryptography meets zero trust

- Externalized verification, not internal storage
- Distributed trust instead of local secrets
- No passwords, no app installs
- No user-side error paths

Designed to survive compromise —
and eliminate phishing by architecture.

The myths that won’t die

- Email accounts were once easy to hack
- Spoofing = impersonation, not intrusion
- Phishing preyed on human behavior

These issues gave email a bad reputation — but the infrastructure evolved.

Today’s email providers are secure by default

- Gmail, Outlook, Apple Mail use:
  - MFA
  - Biometric access
  - Anomaly detection
- Billions rely on them for password and Passkey recovery

These accounts are hardened — and trusted at scale.

Email is the fallback for the internet

- Used to recover:
  - Passwords
  - 2FA
  - Passkeys

If email accounts were insecure,
the entire internet would collapse —
but it hasn’t --- because they are

We use the email protocol — not the message

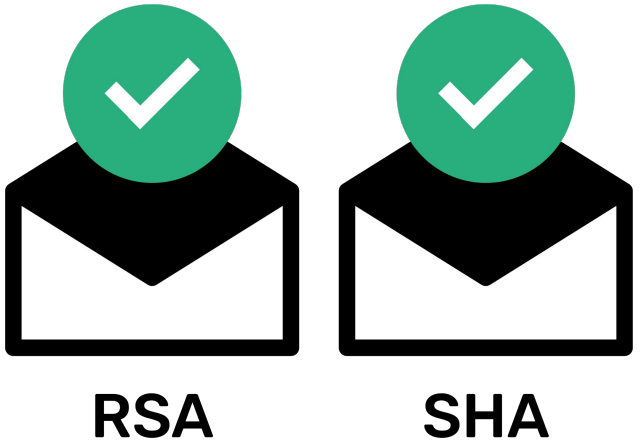
- UniKey ID doesn’t read email content
- We verify the DKIM cryptographic signature

Each login is a signed transaction —
not a message.

Verified by RSA and SHA

- Uses 2048–4096 bit RSA keys
- Hashed with SHA-256 or better
- Signed at send time, verified at login

A real cryptographic handshake —
not a password substitute.



We don’t just use crypto — we use validated crypto

- RSA + SHA are FIPS-validated cryptographic modules
- Approved by NIST and the U.S. Department of Defense

Not experimental.
Proven, standardized, and trusted globally.

Three layers of trust. One cryptographic signal.

- DKIM proves the sender
- SPF verifies the server
- DMARC enforces the policy

This trio doesn’t just detect spoofing — it blocks it.

Spoofing succeeds when systems are blind

- Lookalike domains fool humans
- Noncompliant servers bypass checks
- DNS errors let fakes through

Most systems rely on filters.
UniKeyID relies on cryptography.

No inbox. No interface. Nothing to fake.

- We don’t rely on visuals or headers
- We don’t trust the message, only the signature
- Machine-verified, not human-interpreted

No interface = no spoofing surface.

We don’t rely on DNS. We harden it.

- Multi-resolver DNS checks
- Historical key comparison
- Real-time anomaly detection

Poisoned records are caught —
before trust is granted.

Our public keys live in DNS, not a silo

- Globally auditable
- Redundant and distributed
- Not stored by any single provider

This is public key infrastructure at internet scale.

Infrastructure-grade resilience

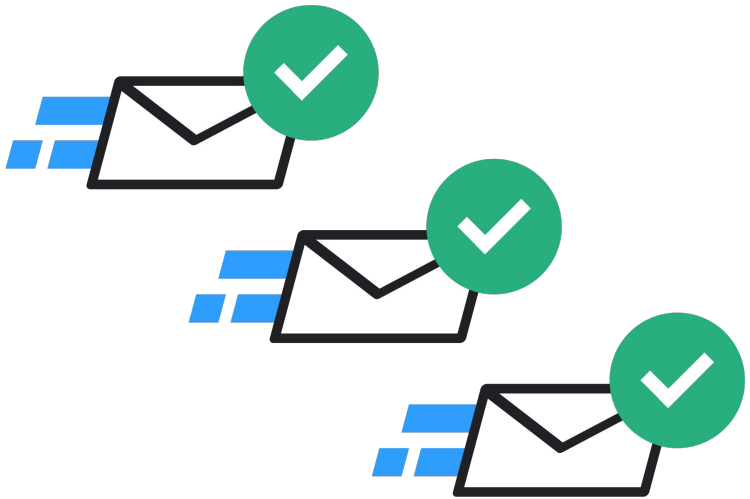
- Multi-source DNS resolution
- Change-detection algorithms
- National-lab-validated protections

We detect and deflect DNS manipulation — proactively.

We don’t store trust. We prove it.

- No key storage
- No shared secrets
- No persistent sessions

Each login proves itself — cryptographically, every time.



Distributed trust — not stored belief

- Public keys published
- Verifiable by anyone
- Resistant to tampering or revision

It’s like blockchain:
Transparent, auditable, and trustless by design.

Secure, even under interception

- SMTP uses a cryptographically signed message
- Signature is verified independently via DNS
- Session context validated over HTTPS

Even if the channel is intercepted,
the attacker can’t fake the signature or fingerprint.

One-way trust — nothing to click

- Email is sent, not received
- No spoofable interfaces
- No phishing vectors

Just a signed signal —
from your device to our server.

Your device proves it’s yours

- Browser, OS, hardware
- Network behavior and timing
- Geolocation consistency

You’re recognized — or challenged — in milliseconds.

Our stack stops spoofing, phishing, and MITM

- SMTP signature (DKIM)
- DNS trust validation
- HTTPS fingerprinting
- AI anomaly detection

No single point of failure.
No step can be bypassed.

We didn’t just harden email.

We turned it into a distributed, cryptographic trust layer.

- Infrastructure-grade identity
- Stateless by design
- Compatible with Passkey, passwords, and beyond

Secure enough for login.
Powerful enough for payments.