Email is the nervous system of modern business, but its security is failing.

For decades, email has been the bedrock of communication—an open, interoperable standard. Yet this very openness now exposes us to unprecedented risks. AI-powered phishing, sophisticated impersonation, and nation-state attacks target email's inherent weaknesses.

We face a fundamental tension: how to protect our most sensitive communications without breaking the protocol that connects the world.

We've tried to fix email security. The results have been inadequate.

Current approaches are a patchwork of compromises, each with critical limitations that have prevented widespread adoption.

S/MIME

Plagued by complex certificate management, poor mobile support, and high costs. Adoption remains minimal outside specific enterprise silos.

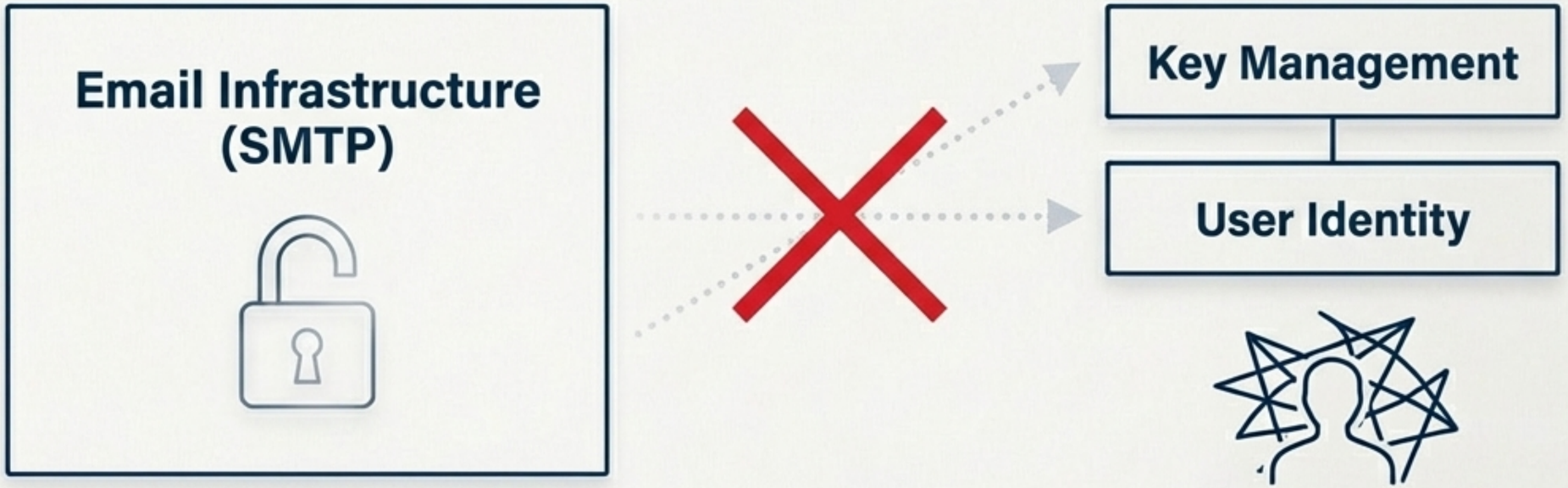
PGP/GPG

The steep learning curve, burdensome key management, and the fragility of the “web-of-trust” model have relegated it it to a niche, technical audience.

Proprietary Apps

These create fragmented ecosystems that sacrifice interoperability. They lead to vendor lock-in and fail to solve the problem for the open email standard.

The core failure is clear: We've been trying to secure an untrusted system with tools that burden the user.



True email security requires delegating the complexity of identity and key management to trusted, specialized providers, leaving email infrastructure to do what it does best: deliver messages.

Introducing the Tiered Security Email Protocol (TSEP).

A backward-compatible extension to SMTP that provides end-to-end encryption by delegating identity to trusted providers.

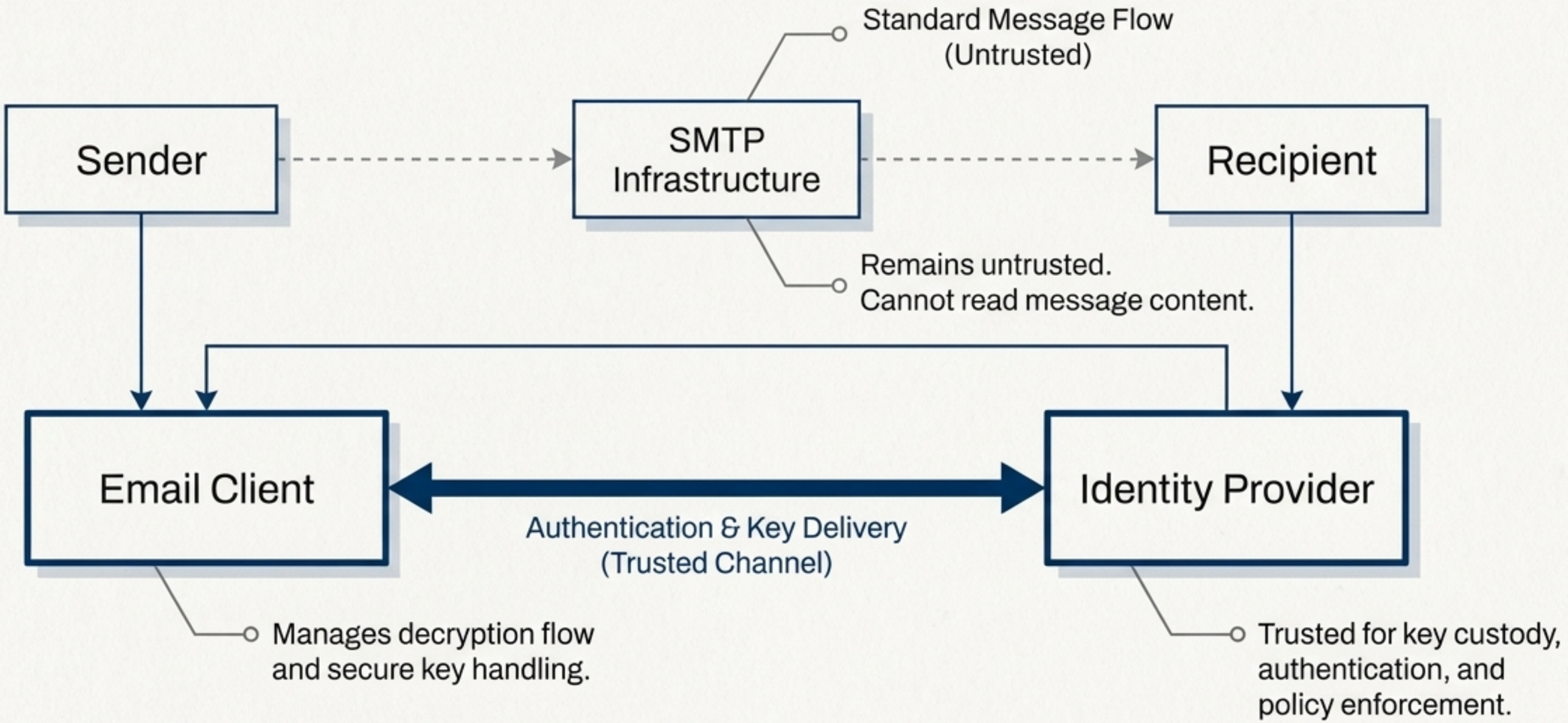
A Multi-Tier Security Model

Balances user convenience and robust protection by offering graduated security levels optimized for different use cases—from routine messages to high-stakes transactions.

Identity Provider-Mediated Key Management

Decouples identity from email. Banks, enterprise identity systems, and authenticators handle key custody, user verification, and policy enforcement, dramatically simplifying the user experience.

TSEP’s architecture separates message transport from trust verification



Three security levels provide the right protection for every message.

Level 1: Cached Key

- **Key Delivery:** One-time sync with Identity Provider.
- **Authentication:** Initial setup only.
- **Use Case:** Routine communications, statements, notifications. Works offline.

Level 2: Online Verification

- **Key Delivery:** Per-message, via real-time auth.
- **Authentication:** Real-time 2FA (e.g., biometric/PIN).
- **Use Case:** Sensitive actions, password resets, financial confirmations.

Level 3: Time-Bound

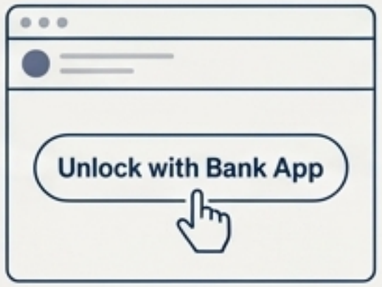
- **Key Delivery:** Per-message with strict constraints.
- **Authentication:** Real-time 2FA + policy checks.
- **Use Case:** High-stakes transactions, legal documents, trade secrets.

Level 2 brings real-time authentication to email without the friction.

Step 1:
Message Arrives

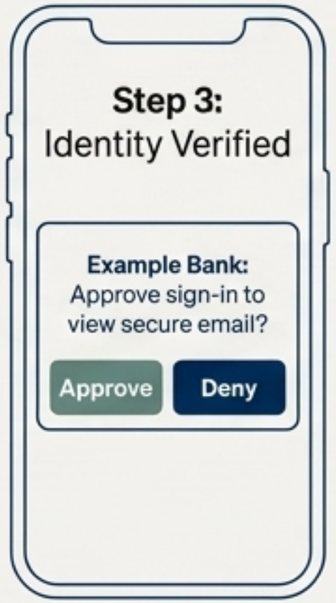
Encrypted message from `noreply@bank.com` received.

Step 2:
User Unlocks



User taps unlock button within the email.

Step 3:
Identity Verified



Identity verified via secure push notification.

Step 4:
Message Decrypted

Message decrypted and content is visible.

Key Security Properties

- Per-message user authentication
- Audit trail of all decryption events
- Instant revocation capability
- Enforces device and location policies

Level 3 delivers cryptographic non-repudiation for high-stakes communication.

Level 3 extends the real-time verification of Level 2 with a rich, enforceable security policy embedded directly into the message envelope.

```
"security_policy": {
  "expires_at": "2025-11-13T10:45:00Z",
  "max_decrypt_count": 1,
  "read_receipt_required": true,
  "geofence": {
    "allowed_countries": ["US", "CA"]
  }
}
```

Time-Limited Access
Messages can be set to expire.

Single-View Enforcement
Ensure information is seen only once.

Geographic Restrictions
Limit decryption to specific locations.

Device Attestation
Require minimum device trust scores.

Cryptographic Proof of Reading
Generates a signed, non-repudiable read receipt, satisfying eSignature and compliance requirements (e.g., ESIGN, eIDAS).

TSEP is built on a foundation of modern, agile cryptography.

RECOMMENDED ALGORITHMS

- Encryption: **X25519 + ChaCha20-Poly1305**
- Signing: **Ed25519**
- Hashing: **SHA-256**

KEY STORAGE

- Level 1: Private keys are encrypted at rest in the client's hardware-backed keystore (iOS Keychain, Android Keystore).
- Levels 2 & 3: Private keys are held in the Identity Provider's Hardware Security Modules (HSMs). They are never transmitted.

KEY DISCOVERY

- A simple DNS-based protocol (`_tsep._tcp.example.com`) allows for federated and secure public key discovery.

POST-QUANTUM READY

- A defined migration path to hybrid cryptography (**X25519 + Kyber768, Ed25519 + Dilithium3**) to address future threats.

A governed ecosystem ensures trust and interoperability.

Email Client Responsibilities

- MUST support TSEP envelope parsing and validation.
- MUST integrate with platform secure keychains.
- MUST use deep linking to Identity Provider apps for authentication flows.

Identity Provider Certification Requirements

Providers must undergo rigorous certification to participate. Key requirements include:

- **Security:** SOC 2 Type II compliance, annual penetration testing.
- **Technical:** HSMs or secure enclaves for all key storage, <2s P95 authentication latency.
- **Audit:** Immutable audit logs with 5-year retention, transparent incident reporting.

A phased roadmap makes adoption practical and achievable.

Phase 1: Pilot
(Months 1-6)

2-3 IdPs, reference implementations, 10k users

Phase 2: Early Adoption
(Months 7-18)

Email client integrations (Gmail, Outlook), certification program established, 1M+ users

Phase 3: Mainstream
(Months 19-36)

Default encryption for institutions, consumer authenticator support, 10M+ users

Phase 4: Universal
(Years 4+)

IETF standardization, regulatory recognition, 100M+ users

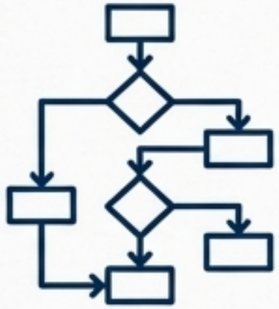
Graceful Degradation for Non-TSEP Clients

Non-TSEP clients receive a standard email containing a plaintext notice and a secure link to view the message, ensuring no communication is lost during the transition period.

TSEP is a platform for the future of trusted digital interaction

Decentralized Identity (SSI)

Future versions will integrate with W3C DID standards, allowing users to control their own keys without a provider, using Verifiable Credentials for attestation.



Advanced Policy Language

Evolve to a ‘policy-as-code’ model, enabling complex rules like multi-party approval workflows based on transaction value or user context.

AI-Powered Security

Identity Providers can leverage AI for real-time risk scoring based on behavioral biometrics, device trust, and location anomalies to prevent coerced authentication and fraud.

TSEP provides the path to a secure and interoperable email ecosystem. It’s time to build it.

TSEP is not just a specification; it is a plan for collective action. We invite you to participate.

For Identity Providers

Join the pilot program. Shape the standard and establish your role as a trusted authenticator for the next generation of email.

For Email Client Vendors

Integrate TSEP. Differentiate your product with best-in-class, user-friendly security that meets growing enterprise and consumer demands.

For Standards Bodies

Support the TSEP IETF working group. Help create the RFC that will define the de facto standard for authenticated, end-to-end encrypted email.

For Enterprises & Regulated Industries

Advocate for TSEP. Demand support from your email and identity vendors to finally solve the challenge of secure digital communication.