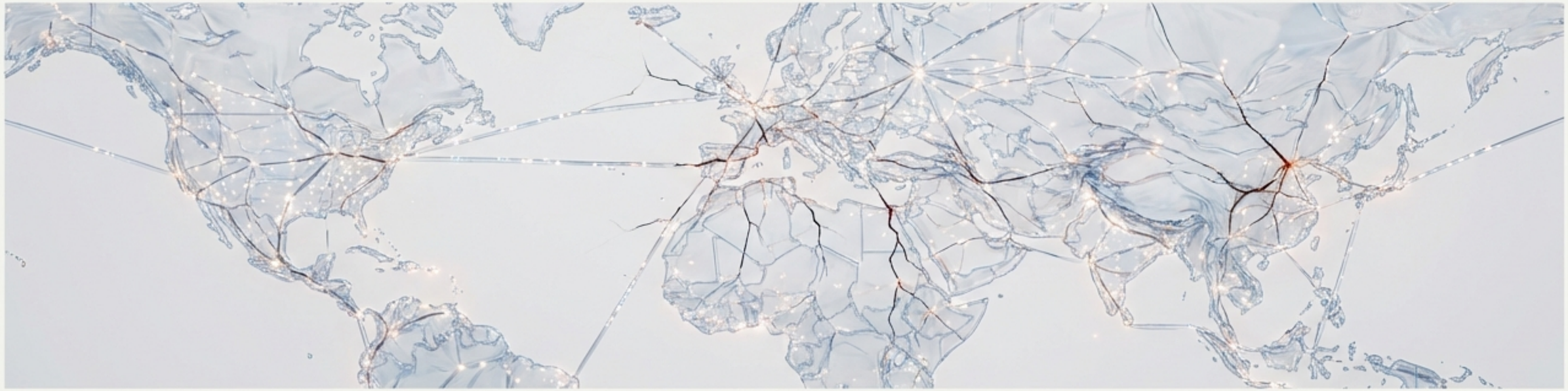
Email is the most critical communication protocol, but it remains fundamentally insecure.

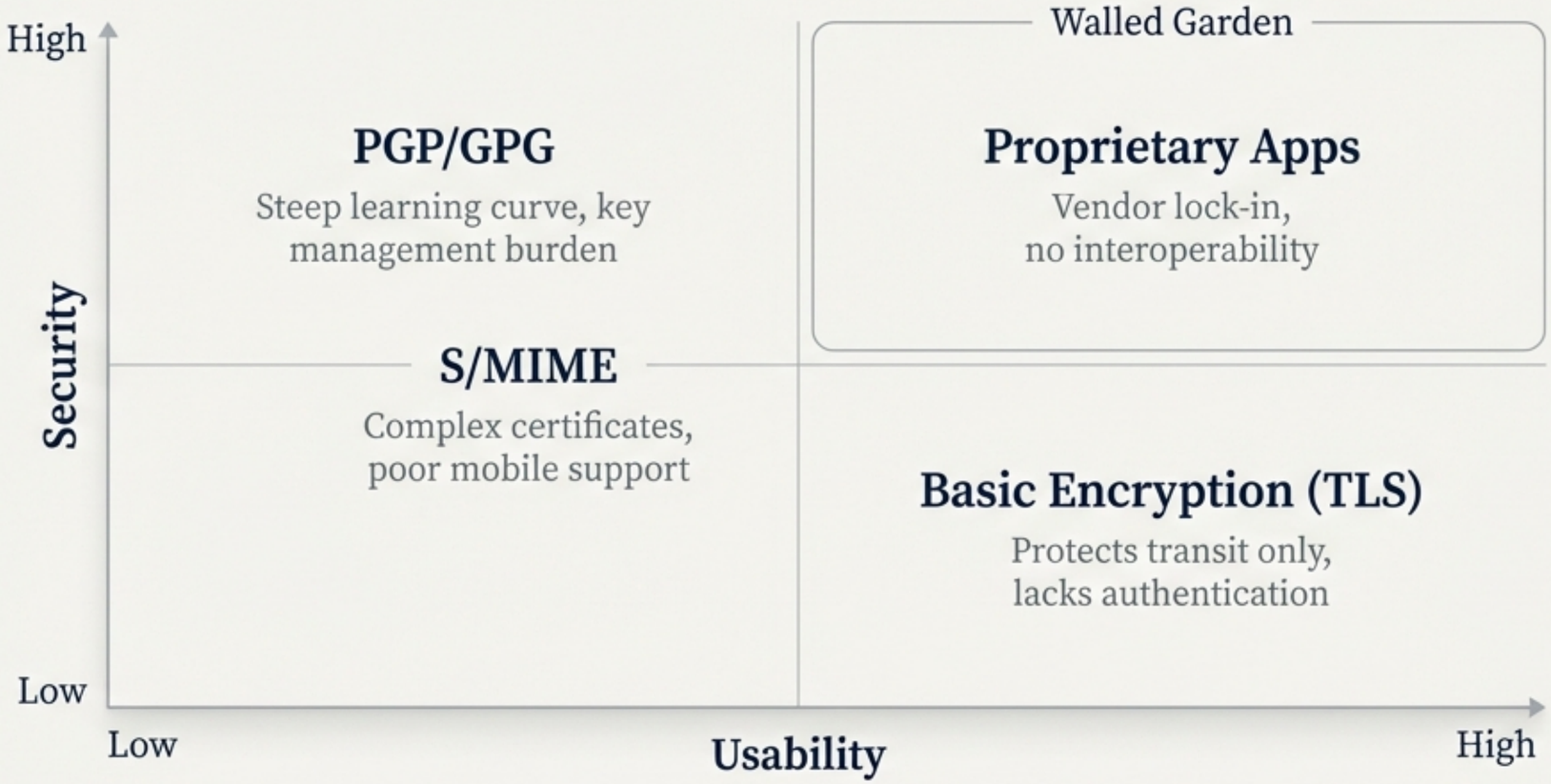


Email underpins everything from personal conversations to multi-billion dollar transactions. Its strength is its open, interoperable design.

This openness is also its greatest weakness. The core protocols were not designed for the modern threat landscape.

As a result, we face a constant barrage of sophisticated threats, including AI-powered phishing, sender impersonation, and man-in-the-middle attacks.

Decades of solutions have failed because they force an impossible trade-off.

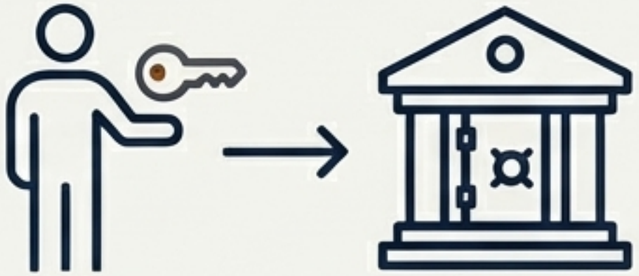


The core failure is a one-size-fits-all approach.
We need a system that adapts the security to the risk.

The solution is not a better lock, but a smarter architecture.

Graduated Security

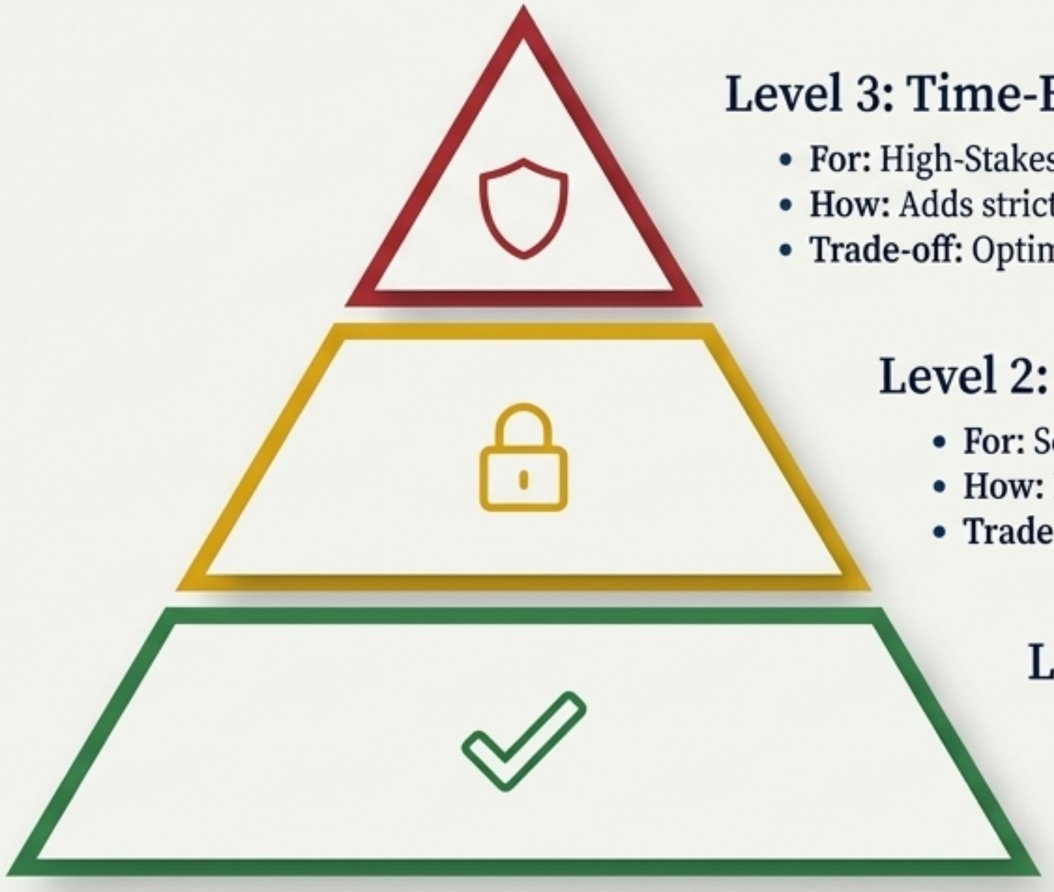
Security should not be a binary choice. TSEP introduces a multi-tier model that matches the level of protection to the sensitivity of the communication. Different threats require different trade-offs between convenience and assurance.



Delegated Complexity

Users and email providers shouldn't manage cryptography. TSEP delegates identity, authentication, and key management to trusted specialists like banks and enterprise identity systems—the experts who already manage your digital life.

TSEP provides three distinct security levels for every use case.



Level 3: Time-Bound Verification Mode

- **For:** High-Stakes Transactions (e.g., wire transfers, legal contracts).
- **How:** Adds strict policies like message expiry, single-view, and geofencing.
- **Trade-off:** Optimized for maximum assurance and non-repudiation.

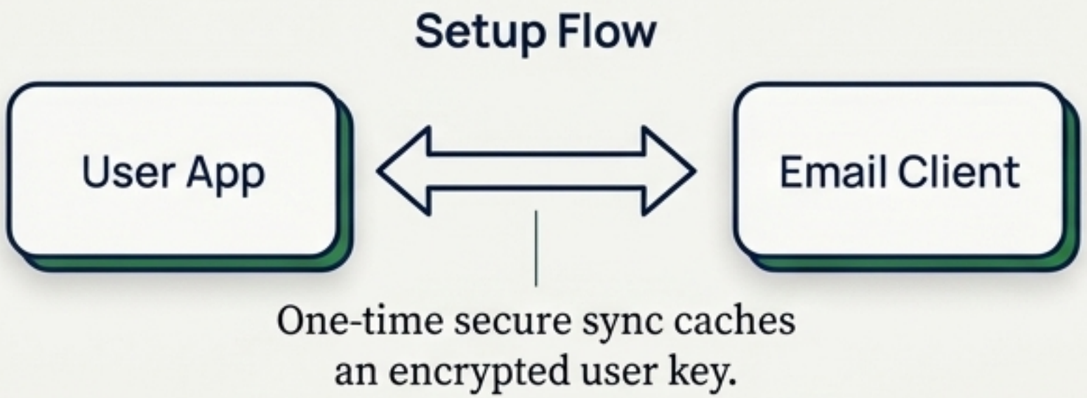
Level 2: Online Verification Mode

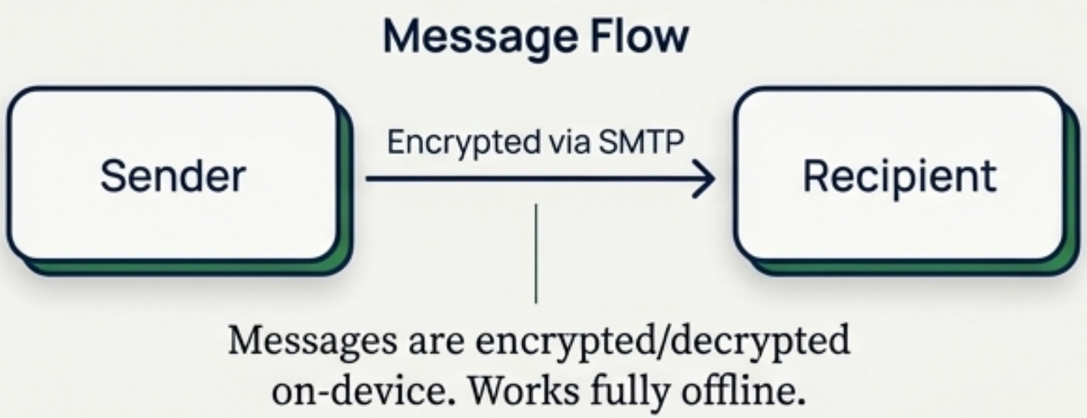
- **For:** Sensitive Actions (e.g., password resets, financial notices).
- **How:** Requires real-time user authentication (2FA/biometric) to decrypt.
- **Trade-off:** Balanced security and usability.

Level 1: Cached Key Mode

- **For:** Routine Communications (e.g., statements, newsletters).
- **How:** Seamless end-to-end encryption. Works offline.
- **Trade-off:** Optimized for convenience.

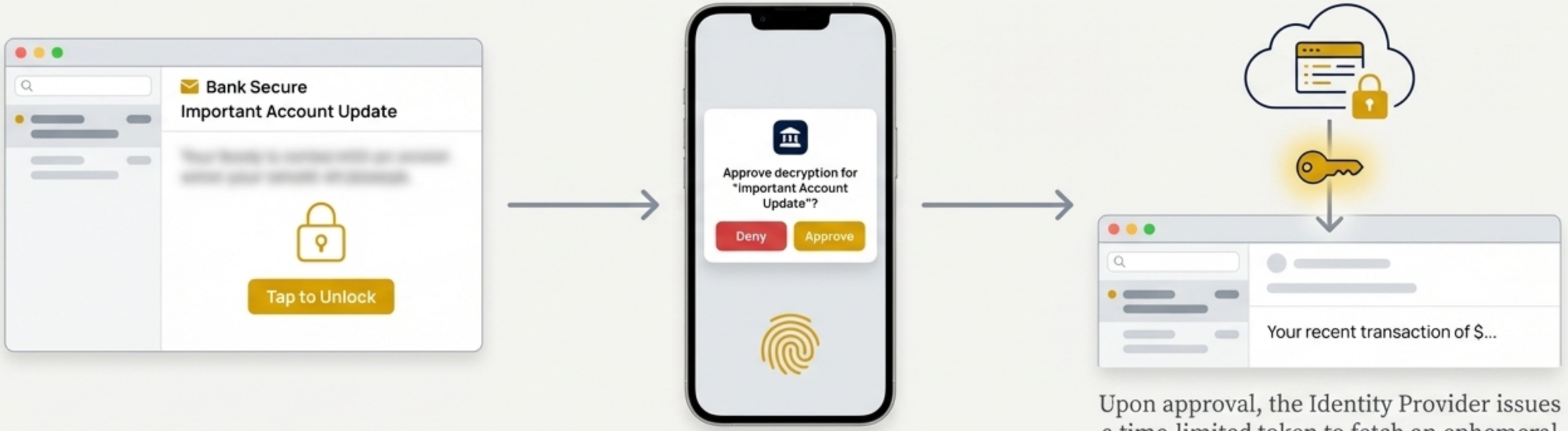
Level 1: Seamless, offline encryption for everyday communication





- ✅ End-to-end encryption (provider can’t read)
- ✅ Cryptographic sender authentication
- ✅ Fully offline reading capability
- ✅ Zero-friction user experience
- ⚠️ Vulnerable to endpoint device compromise (mitigated by platform keychains).

Level 2: Real-time authentication for sensitive messages.

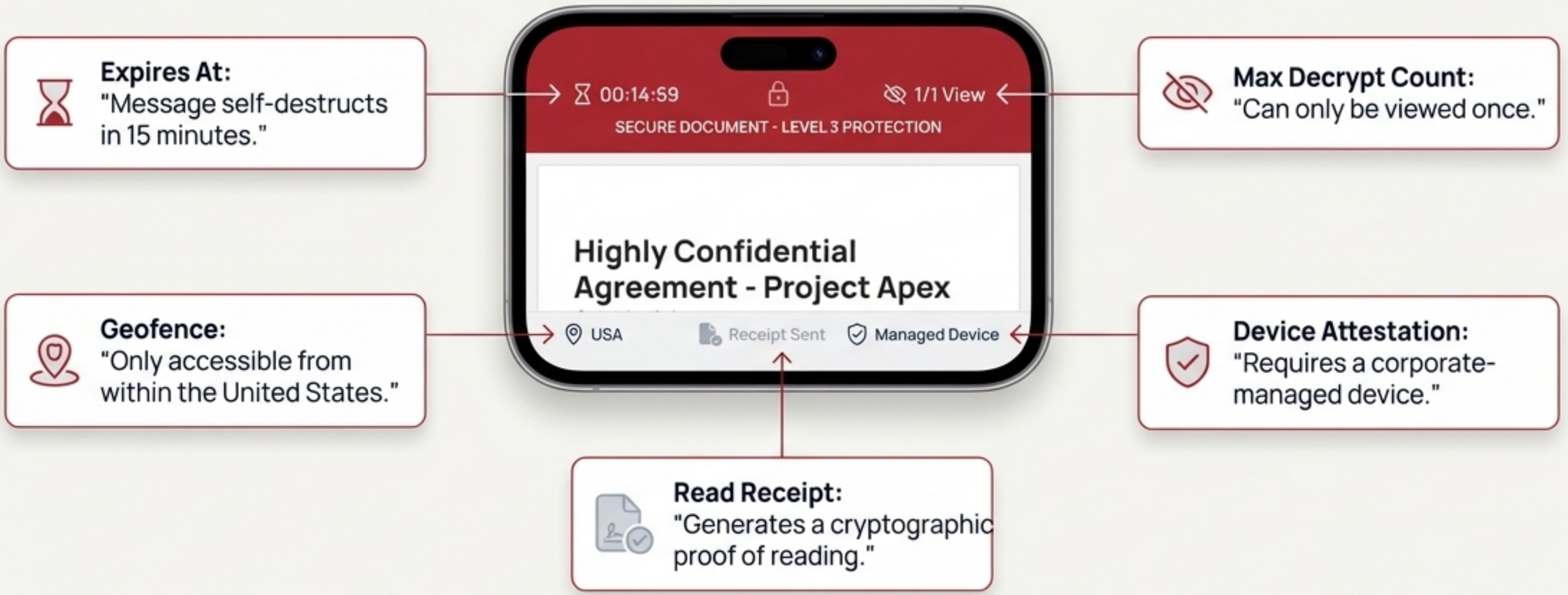


Upon approval, the Identity Provider issues a time-limited token to fetch an ephemeral key and decrypt the message.

Key Security Properties

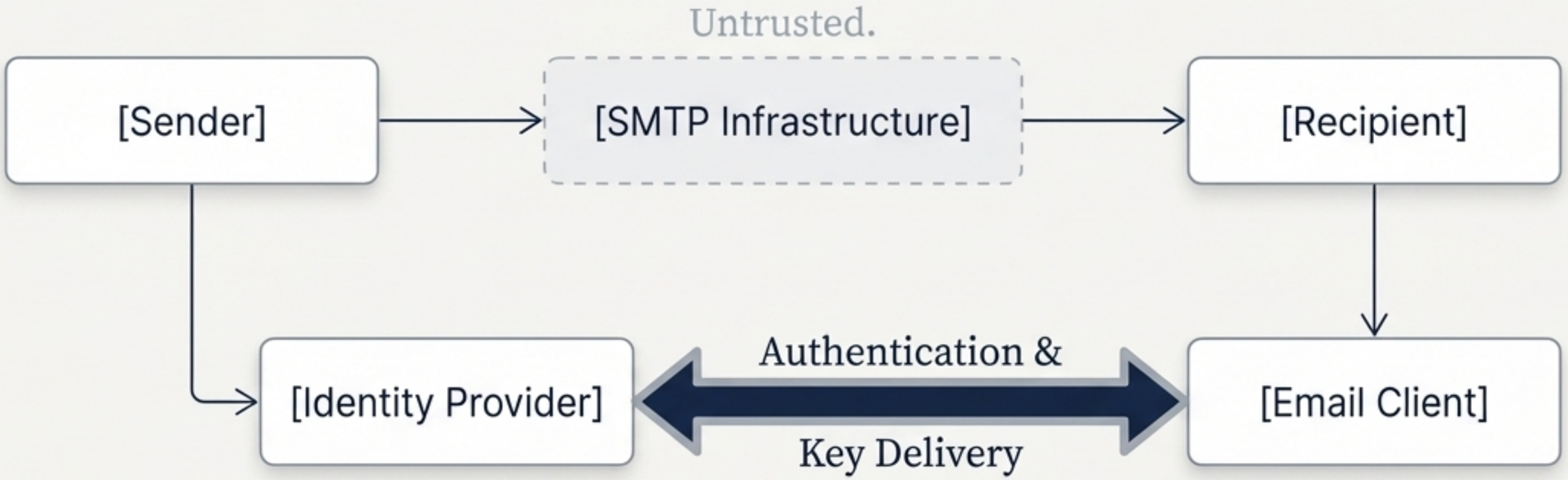
- ☑ All Level 1 properties.
- ☑ **Per-message user authentication:** Proves the intended recipient is present.
- ☑ **Device and policy enforcement:** IdP can check device trust, location, etc.
- ☑ **Immutable audit trail:** Every decryption event is logged.
- ☑ **Instant revocation:** Access can be cut off at the IdP level.

Level 3: Enforceable policies and cryptographic proof for high-stakes transactions



Non-repudiation: The cryptographic read receipt provides legally binding proof that the specific authenticated user read the specific content at a specific time.

The TSEP architecture decouples trust from the email infrastructure.



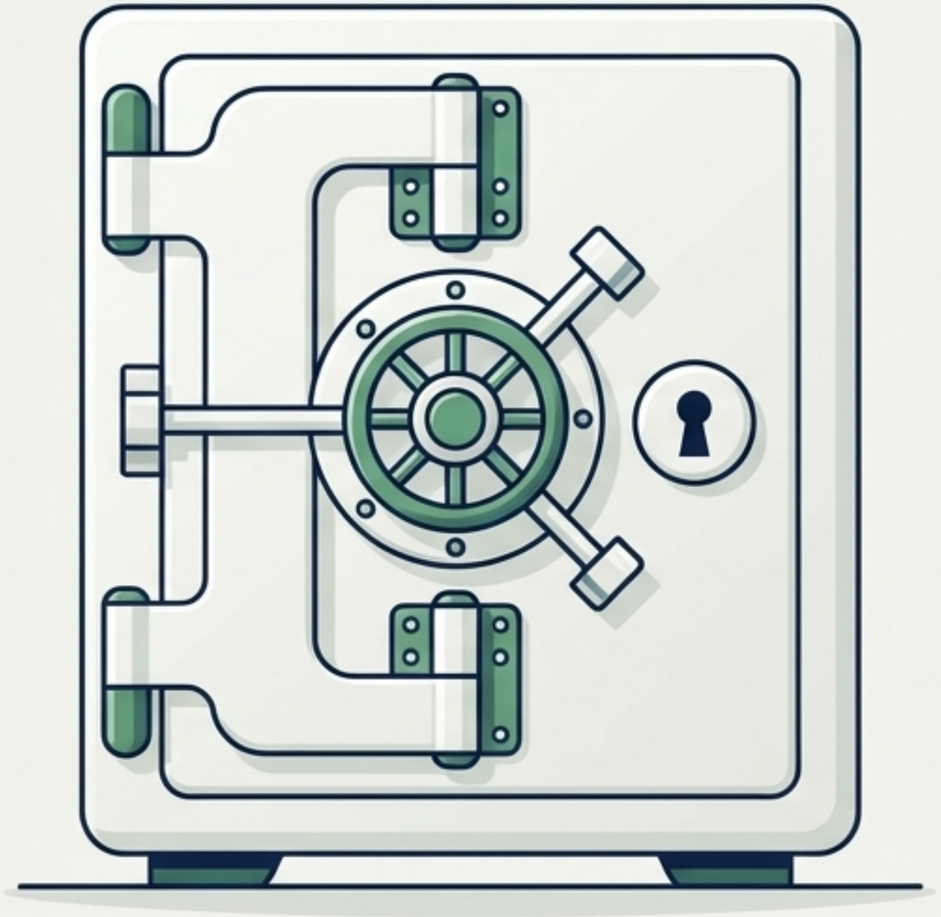
Trust Model Explained

Email Infrastructure (SMTP): Untrusted. Assumed to be adversarial. TSEP protects messages *from* this layer.

End Devices: Trusted (when attested). Protected by platform security.

Identity Providers: Trusted. Act as the root of trust for identity verification and key custody.

Certified Identity Providers handle the heavy lifting of security and compliance.



Provider Responsibilities:

- **Secure Key Custody**: Private keys are stored in Hardware Security Modules (HSMs).
- **User Authentication**: Verify user identity before releasing any keys.
- **Policy Enforcement**: Evaluate device, geo, and risk policies in real time.
- **Immutable Audit Logging**: Record every key access event for compliance.

Certification Requirements:

Providers must meet stringent criteria to join the ecosystem, including:

- SOC 2 Type II compliance
- Annual third-party penetration testing
- Strict latency and uptime SLAs (e.g., <2s authentication p95)

TSEP delivers precisely the right security for every financial communication.

Level 1 (Routine)

- ✓ Monthly account statements
- ✓ Balance notifications
- ✓ Product marketing

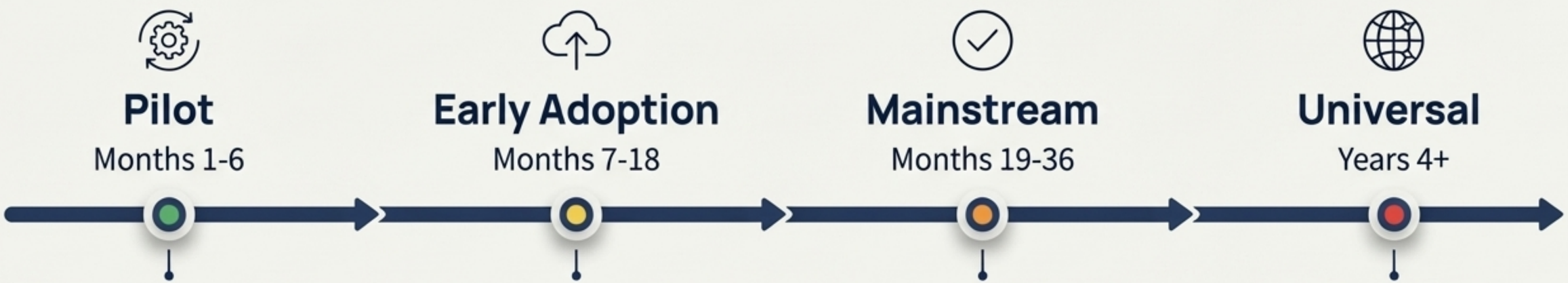
Level 2 (Sensitive)

- ✓ Password reset confirmations
- ✓ Small transaction alerts (<$1,000)
- ✓ Account setting changes

Level 3 (High-Stakes)

- ✓ Wire transfer approvals (>$10,000)
- ✓ Legal document delivery (loan agreements)
- ✓ Beneficiary changes

A pragmatic, phased approach to adoption ensures a smooth transition



Backward Compatibility: Non-TSEP clients receive a clear plaintext notice with a link to view the secure message, ensuring no communication is ever lost.

Built on modern, vetted cryptography with a clear path to a post-quantum future.

Today's Cryptography

Encryption: X25519 + ChaCha20-Poly1305 (AEAD)

Signing: Ed25519

These choices prioritize both high security and high performance on a wide range of devices.

Post-Quantum Migration Path

Timeline: Transition begins 2026, complete by 2030.

Strategy: A phased hybrid approach.

- Phase 1: Hybrid keys (X25519 + Kyber768, Ed25519 + Dilithium3).
- Phase 2: PQC becomes the default.
- Phase 3: Deprecate classical algorithms.

TSEP is designed with crypto-agility to address future threats without disruption.

TSEP creates a sustainable ecosystem with a powerful value proposition for everyone.

Users (Recipients)

Benefit: Free, frictionless security and privacy.

Senders (Enterprises)

Benefit: Drastically reduced fraud losses, simplified compliance, and enhanced brand trust.

Cost: Small per-message fee for Level 2/3.

Identity Providers

Benefit: New revenue stream from authentication services and enterprise licenses.

Email Clients

Benefit: Competitive differentiation and retention of high-value enterprise customers.

TSEP is the future of trusted digital communication. Let's build it together.

Key Innovations Revisited

1. **Multi-tier model:** Balances convenience and protection.
2. **Identity delegation:** Solves the key management problem.
3. **Backward compatibility:** Ensures a practical migration path.
4. **Cryptographic assurance:** Provides true non-repudiation.

A Call to Action

For Identity Providers

Join the pilot program to shape the standard.

For Email Client Vendors

Integrate TSEP to meet growing security demands.

For Enterprises

Advocate for TSEP support from your providers.

For Standards Bodies

Support TSEP as an IETF RFC.

Securing the protocol that connects the world.

Email's openness made it revolutionary, but its lack of inherent trust now puts it at risk. TSEP preserves the protocol's universal reach while adding the missing layer of verified identity and cryptographic assurance. It is the pragmatic, necessary step to ensure email remains the trusted backbone of communication for decades to come.