What Kind of Email Client Do We Really Need?

August 12, 2026

The author has touched on this topic in several previous blog posts, but the author has never given a complete answer. Today, on the eve of ZTmail's public beta launch, I want to settle this question once and for all.

1. What should an email client be?

Before we answer that, let's look at the current landscape.

What do the world's dominant email clients — Outlook, Thunderbird, Apple Mail — do? Send and receive emails, manage calendars, organize contacts. These core functions have barely changed in two decades. Meanwhile, webmail services (Gmail, Outlook.com, QQ Mail) have captured a massive user base with their "accessible from anywhere" convenience.

But here's the reality: **your emails are sent in plain text and stored in plain text in the cloud. Service providers can read them, analyze them, and even use them for ad targeting and AI training.**

Users face an impossible choice: Use a traditional email client that supports encryption but is painfully difficult to configure. Or use webmail that's convenient but offers no end-to-end encryption, leaving your privacy exposed.

This is a choice users should never have to make.

2. What kind of email client do users really need?

In my view, users need an email client with three essential qualities:

First: Automation.

S/MIME email encryption technology has been around for over 30 years — it was born in 1995 — yet it has never achieved widespread adoption. The reason is simple: it's not that the technology is bad, it's that it's far too complicated.

Manually applying for certificates, manually configuring them into clients, manually exchanging public keys, manually renewing them — this entire process is enough to deter 99.99% of users. Users don't need "the ability to encrypt." They need "encryption that's on by default." No need to understand what a CA is, what a public key certificate is, or what a PFX file is — just log in and encryption works

automatically.

Second: Standardization.

Encryption must not create silos. If you can only send encrypted emails to users of the same email client, the value of encryption is severely diminished. Users need encryption built on international standards — specifically, S/MIME, which works seamlessly with Outlook, Thunderbird, Apple Mail, and all other standard clients. An encrypted email you send to a Gmail user should be readable by that user in Outlook.

At the same time, for Chinese users, the national cryptographic standard is equally essential. RSA ensures global interoperability, while SM2 ensures national cryptographic compliance. One email, two algorithms, choose as needed — both internationally and domestically viable.

Third: Intelligence.

Email consumes a significant portion of users' time — reading, understanding, replying, organizing. The emergence of large language models has opened the possibility of automating these tasks. Yet users still find themselves copying and pasting between their email client and AI services. Some email clients have begun offering AI assistants, but AI should not be closed or locked to a single provider. What users need is the freedom to **choose their own AI model and bring their own API key** — whether it's OpenAI, DeepSeek, or a locally deployed Ollama — entirely their own decision, with data never passing through any other third-party servers.

3. Why the “browser-integrated email client” approach doesn’t work

ZT Browser was originally designed as a "3-in-1" product: browser + email client + PDF reader. It sounded great on paper — a one-stop solution for everything. But in practice, we identified two fundamental flaws:

First, the browser's interaction model is ill-suited for email processing. Email requires focus — multi-account management, quick switching, offline operations, certificate management — all functions that demand deep customization for the email scenario, not as an "add-on" feature of a browser.

Second, users won't switch browsers just for an email feature. Browsers are among the most frequently used tools in daily life, and users have their own preferences. They are unlikely to switch

browsers simply to gain encrypted email capabilities.

Let browsing belong to browsers. Let email belong to email clients. That is the most logical solution.

4. The ZTmail answer

Based on these considerations, ZoTrus Technology has made a major strategic pivot: **spin the email client out of the ZT Browser and turn it into a standalone product: ZTmail.**

ZTmail is an independent, focused email client. Its design revolves around three core pillars:

(1) Automated Encryption. Every email is end-to-end encrypted by default, with support for RSA and SM2 dual algorithms. Full lifecycle security and privacy. After login, the system automatically validates your email address and provisions certificates — zero manual intervention.

(2) Digital Signature. Every email is digitally signed by default, autonomously proving the sender's identity and that the content has not been tampered with. Recipients see not just "an encrypted email," but the sender's trusted identity: T1 Email Verification, T2 Individual Verification, T3 Organization Verification, T4 Employee Verification — the higher the identity level, the higher the trust.

(3) Your AI Assistant. Choose your own AI model, bring your own API key, and the AI assistant works for you. Email summaries, smart drafting, intelligent classification — AI under your control.

5. One Encrypted Email, Two Clients Can Read It

By default, ZTmail automatically provides a free configuration using an RSA algorithm email certificate. Users can manually export and install it into the Windows system store, and Outlook will automatically read and trust the same certificate. This means that encrypted emails sent by ZTmail can be properly decrypted and viewed in Outlook.

One encrypted email, readable in both ZTmail and Outlook. This is a unique ZTmail experience — we don't force you to abandon the tools you're used to. Instead, we bring encryption seamlessly into your existing workflow.

6. Welcome to ZTmail

Back to the original question: **What kind of email client do we really need?**

The author answer is **the One that is automated encryption, trusted identity, AI-powered, standard-compliant, independent, and focused.**

Let browsing belong to browsers. Let email encryption belong to ZTmail. This is what an email client

should be.

ZTmail's public beta goes live on August 20. The author invites you to download it and experience it for yourself — your feedback will help us make it even better.

Richard Wang

August 12, 2026
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 120 articles in English (more than 167K words) and 278 articles in Chinese (more than 824K characters in total).