Global S/MIME Email Can Become a Global Instant Messaging Network

End-to-End Encryption, Trusted Identity, and a Messaging Model Without a Centralized Chat Platform

September 24, 2026

Today's Internet is global, but its chat systems remain largely fragmented into closed messaging networks. People can communicate easily with others inside the same service, yet when their contacts use different platforms, countries, organizations, or business ecosystems, communication becomes divided. Users often end up maintaining several chat applications and accounts simply to stay connected with family and friends, international contacts, colleagues, customers, suppliers, or business partners. The problem is therefore deeper than having too many applications on a phone: each application represents a separate messaging network, with its own users, accounts, identity model, servers, storage, delivery mechanisms, and service boundaries.

This fragmentation also creates structural dependence on the provider operating each network. To communicate through a particular chat service, both participants generally must enter the same provider's network. The provider becomes not only the operator of the application, but also the operator of the communication environment in which the conversation takes place. The result is a world in which the Internet itself is global, while one of the most important forms of everyday digital communication remains divided into a collection of private, largely non-interconnectable networks.

1. Why Chat Became Fragmented and Why It Is Time to Rethink the Model

The fragmented structure of chat did not emerge without good technical and commercial reasons. When Internet access was less widespread, network bandwidth was more constrained, mobile connectivity was immature, and computing and cloud infrastructure were far less capable than they are today, building a dedicated messaging service with a tightly controlled network was a practical way to deliver reliable real-time communication. Service providers needed to control accounts, servers, message delivery, storage, and the user experience in order to build a dependable service. As those services grew, network effects, proprietary features, and large infrastructure investments reinforced the closed model, eventually producing the many successful but isolated chat networks that exist today.

The technical environment has since changed dramatically. High-speed fixed and mobile networks,

mature cloud computing, large-scale data centers, capable client devices, and established Internet protocols have transformed the conditions under which global communication can be built. More importantly, the world already has a communication infrastructure that has spent decades solving the problem of interconnection: email. Users and organizations do not need to belong to one company's email network to exchange messages. The global email infrastructure already connects providers, organizations, domains, and users across the Internet. So, the historical conditions that used to make isolated messaging networks appealing are no longer there, and it's time to rethink the tech architecture for global chatting.

2. The Next Generation of Instant Messaging Is One Infrastructure for Mail and Chat

Email is often viewed primarily as a communication format, but its more important property for this discussion is architecture: it is an established, interconnectable global communication infrastructure. It has been decades since establishing addressing conventions, routing mechanisms, organizational adoption, and the ability for independent providers and domains to exchange messages. No individual chat platform can simply recreate what this infrastructure has spent decades establishing.

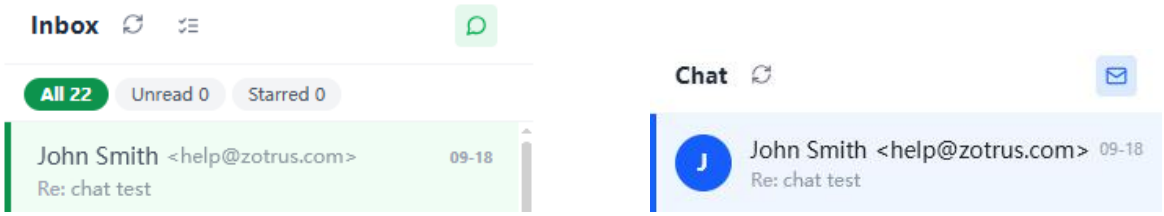
That changes the starting point for the next generation of chat. Instead of asking how to build another global messaging network and then connect it to everyone else, the industry can ask how existing chat experiences can use the global email communication network that already exists. The opportunity is not to replace email with chat, but to allow the same underlying infrastructure to support both forms of communication.

The next generation of chat does not require another global chat network. A more fundamental approach is to make mail and chat two communication experiences over the same underlying infrastructure. The interface can change without requiring the communication network to be rebuilt. Email can remain email when users need formal, asynchronous, or document-oriented communication, while the same infrastructure can present an ongoing conversation through a chat-oriented interface.

The key is to add an appropriate encryption and interaction layer to an infrastructure that already provides global reach. S/MIME can provide the cryptographic foundation for end-to-end encrypted communication, while certificate-based identity can provide a trusted way to establish and display who is participating in the conversation. With the right automation, users do not need to understand the underlying certificate, key, and encryption operations any more than they need to understand how

email routing works today.

ZTmail demonstrates this model by allowing the user to switch from **Mail Mode** to **Chat Mode** while continuing to use the same underlying encrypted email system. The significance is not simply that an email application has acquired a chat interface. This practice demonstrates that the communication network itself does not have to be reinvented in order to provide a chat experience. The private chat network and the global email system can, in effect, converge into one communication infrastructure.



This also provides a more precise meaning for decentralization. A decentralized communication model does not require eliminating servers, service providers, or network infrastructure, nor does it require every conversation to become peer-to-peer. The decentralization comes from the fact that no single chat provider must own the global messaging network. Independent providers can continue to operate their own applications and services while their users communicate through an interconnectable infrastructure based on the global email system. You can also think of it as a global instant messaging network with multiple service nodes and providers all connected, rather than the current multiple centralized instant messaging service providers that don't interconnect.

In such a model, a user does not have to join the same chat platform as the person they want to contact. Different providers can remain independent on the application layer while becoming interconnectable at the communication layer. The result is a new decentralized interconnected chat service; it is based on one global communication infrastructure capable of supporting different communication experiences.

3. Trusted Identity: The Missing Half of Secure Chat

End-to-end encryption solves one of the most important questions in private communication: who can read the conversation? But it does not, by itself, answer another question that is equally important in a global messaging environment: who am I actually communicating with? This is one of the areas in which today's chat systems remain particularly dependent on platform-controlled identity. A username, phone number, profile photograph, account handle, or contact entry can tell a user which account they

are talking to, but it does not necessarily provide the same kind of independently established identity assurance as a certificate-backed, trusted identity.

A globally interconnectable encrypted chat system therefore needs more than message encryption. It needs a way to carry trusted identity across service boundaries and make that identity visible to the person using the application. S/MIME digital signatures provide a foundation for binding a message to a certificate-based identity, while trusted third-party certificate authorities can provide the identity validation behind that certificate. The application can then expose the resulting trust information directly in the conversation instead of hiding it inside technical certificate details.

For example, ZTmail App interface could display the trusted identity as: “T4 [CN] [Richard Wang, ZoTrus Technology Limited]”. The significance of such a display is not the label itself. It is that the user can see an identity level and identity information backed by a trusted certificate framework, rather than having to rely solely on what the other participant claims about themselves.

This becomes especially important when communication crosses organizational, geographic, or platform boundaries. Inside a closed chat network, the platform controls the account system and can provide its own mechanisms for account verification. Across an interconnectable network, however, participants need a common way to establish trust that does not depend on both users belonging to the same platform. Publicly trusted Certificate-based identity provides a possible foundation for that model.

Trusted identity also changes how security information can be used. Instead of treating identity as static profile metadata, a messaging application can make the trust level visible and actionable. For example, allowing users or organizations to distinguish different levels of identity assurance and apply communication or release policies accordingly. Encryption and identity address two different dimensions of the same problem: encryption protects the conversation, while trusted identity helps establish who is participating in it.

That distinction is critical for any proposed global chat architecture. A system that is encrypted but

cannot establish trusted identity can still leave users exposed to impersonation and identity-related fraud. A system that establishes identity but does not protect the content leaves the conversation exposed. The combination of end-to-end encryption and trusted identity is therefore what turns interconnectable messaging into a more complete trust model.

4. ZTmail Has Set a Good Example

The significance of ZTmail in this topic is therefore broader than the existence of a chat feature. ZTmail has already taken this model into global public beta, providing a working, publicly testable implementation of how an encrypted email infrastructure is implemented. The purpose of developing the complete chain of products and capabilities, from S/MIME certificates and trusted identity to cryptographic services, mail clients, cryptographic gateways, key management, and automation, was to demonstrate that the model can work as a complete system, not merely as a theoretical architecture. The same principle applies to encrypted chat. ZTmail provides a working implementation in which an encrypted email service can be presented through a chat-oriented interface, using S/MIME as the cryptographic foundation and the global email infrastructure as the communication layer. This practice demonstrates that this combination is technically workable: the interface can become Chat while the underlying communication infrastructure remains email.

But the objective is not for ZTmail to become one of the world's chat providers. The more meaningful result is that this practice demonstrates another direction for the industry. If one implementation can combine mail, chat, S/MIME encryption, and trusted identity over existing email infrastructure, other providers can consider how the same architectural principles might be incorporated into their own services.

In that sense, ZTmail is one participant in the ecosystem, and not the killer of current chat providers. The value of the work is measured not by how many users must move into a new ZTmail network, but by whether the underlying model can help make secure and interconnectable communication available across the broader Internet.

5. A Proposal for the Next Generation of Instant Messaging

The logical next step is not for every chat provider to abandon its existing service, nor is it necessary for the industry to agree on a new chat application. The more fundamental change would be to separate

the chat experience from the assumption that every provider must operate an isolated global messaging network.

Existing chat providers could continue to maintain their applications, user communities, product features, and business models while connecting their messaging services to the global email infrastructure. S/MIME could provide a common cryptographic foundation for end-to-end encrypted communication, while certificate and identity services could provide a common basis for trusted identity. Providers would remain independent at the service layer, but their users would gain the possibility of secure communication across service boundaries.

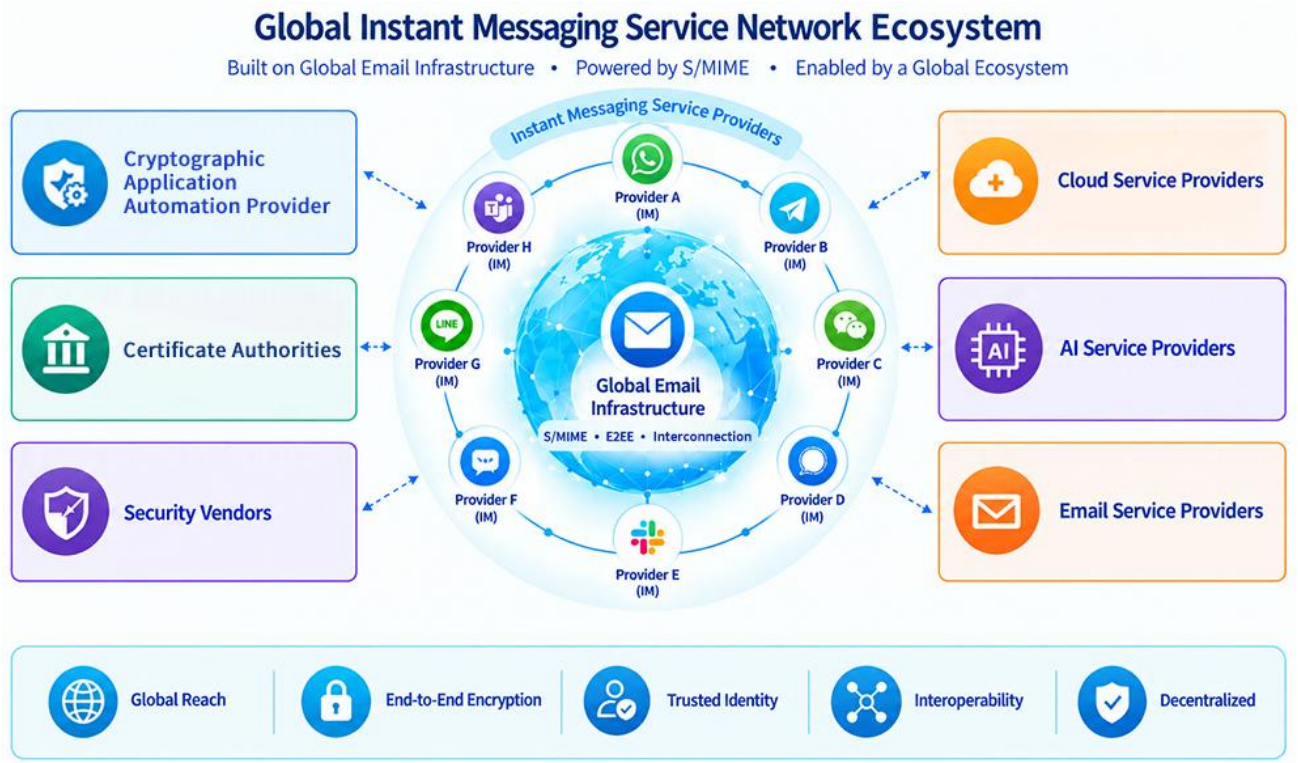
The principle is simple: chat providers do not have to disappear; they need to become interconnectable. The goal is not to make everyone use one chat service, but to make different services capable of communicating securely with one another.

6. Technology Is Ready: Let S/MIME Serve the Global Internet

This proposal is no longer only a theoretical discussion about what might be possible in the distant future. The underlying technologies are mature, the global email infrastructure already exists, S/MIME provides a well-established cryptographic model, and ZTmail has implemented and tested a working combination of these capabilities. The remaining challenge is therefore less about inventing another network and more about deciding how existing participants can connect their capabilities.

S/MIME is often discussed as an email security technology, but its underlying capabilities are not inherently limited to the visual concept of an email message. Encryption, digital signatures, certificate-based identity, and automated key and certificate management can support broader forms of secure digital communication when integrated into the surrounding infrastructure. Mail and chat can therefore become different experiences over common communication and cryptographic foundation.

This is also where the broader ecosystem becomes important. Certificate authorities, email providers, email clients, security vendors, cloud and AI services, cryptographic technology providers, and chat providers can each contribute what they already do best. No single company needs to own the entire communication stack. The industry can build on shared standards and interconnectable infrastructure while specialized providers contribute identity, certificates, encryption, automation, user interfaces, network services, and other capabilities.



If the industry adopts this direction, S/MIME does not have to remain confined to one product or one provider. It can become a common security layer that helps connect the existing communication ecosystem rather than another proprietary security feature locked inside a single platform. That is how technology moves from being a product capability to becoming part of infrastructure: not when one company owns it, but when many participants can build it together.

7. The World Does Not Need Messaging Island

The fragmentation of today's chat systems has historical roots, and those roots explain why private messaging networks became so successful. But the Internet has evolved. The world now has the connectivity, infrastructure, standards, computing capacity, and cryptographic technologies required to reconsider the architecture.

The central question is no longer whether another company can build another successful chat platform. It is whether the global Internet can finally make chat interconnectable without requiring users to join the same platform first.

The answer may begin with infrastructure that already exists. Email has spent decades establishing a global, interconnectable communication network. S/MIME can provide the end-to-end encryption and certificate-based identity needed to make that infrastructure suitable for a broader range of private

communication. Chat providers can retain their services while connecting to a common communication layer instead of maintaining isolated messaging islands.

ZTmail's role is to demonstrate that this model is not merely an architectural idea. The complete ecosystem has been built and practiced proving that the pieces can work together, and the one click Mail-to-Chat model demonstrates that an encrypted chat experience can be built on the global email infrastructure, instead of continuing to use isolated and centralized chat networks.

The larger goal, however, is not for ZTmail to become the world's chat provider. ZTmail is only one participant in the ecosystem. The real opportunity is to give the broader industry a path toward S/MIME interconnectable communication in which users are no longer divided simply because their contacts use different messaging services.

The Internet nowadays shouldn't have information silos anymore. It needs a new communication architecture in which the islands can communicate securely with one another. The technology is ready. The infrastructure already exists. What remains is for the industry to connect the two.

S/MIME does not have to remain only an email security technology. It can become part of the global infrastructure for secure, interconnectable instant communication across the Internet.

Richard Wang

September 24, 2026
In Shenzhen, China

Follow ZTmail at X (Twitter) for more info.
The author has published 136 articles in English (more than 193K words) and 294 articles in Chinese (more than 882K characters in total).