全球 S/MIME 邮件网络可以成为全球即时通讯网络

端到端加密、可信身份，去中心化的聊天消息通信模式

2026 年 9 月 24 日

今天的互联网是全球性的，但其即时通讯系统（聊天）仍然基本上分散在封闭的消息网络中。人们可以轻松地与使用同一服务的人通信，但当联系人使用不同的平台、处于不同国家、组织或商业生态时，通信就变得非常割裂。为了与家人和朋友、国际联系人、同事、客户、供应商或业务伙伴保持联系，用户往往需要维护多个聊天应用和账户。这个问题并不只是手机上应用太多：每个应用都代表着一个独立的消息网络，拥有自己的用户、账户、身份模型、服务器、存储、传输机制和服务边界。

这种碎片化造成了用户对各自运营各自网络的服务提供商的结构性依赖。要通过某一聊天服务进行通信，双方必须进入同一家服务提供商的网络。服务提供商不仅成为应用的运营者，也成为对话发生所在通信环境的运营者。结果是，互联网本身是全球性的，而日常数字通信中最重要的形式之一，却仍然被分割成一系列私有的、彼此不可互通的网络。

1. 为什么聊天会变得如此碎片化，为什么现在是重新思考这一模式的时候了

聊天应用的碎片化结构并非没有合理的技术和商业原因。当互联网接入还不够普及、网络带宽受限、移动连接尚不成熟，以及云计算和云基础设施远不如今天强大时，构建一个拥有严格控制网络的专用消息服务，是提供可靠实时通信的一种实际方式。服务提供商需要控制账户、服务器、消息传输、存储和用户体验，才能建立可靠的服务。随着这些服务不断发展，网络效应、专有功能和巨大的基础设施投资进一步强化了封闭模式，最终形成了今天众多成功但彼此孤立的聊天网络。

此后的技术环境已经发生了巨大变化。高速固定和移动网络、成熟的云计算、大规模数据中心、能力更强的客户端设备以及已经建立的成熟互联网协议，改变了构建全球通信所处的条件。更重要的是，世界已经拥有一种花费数十年解决互通问题的通信基础设施：**电子邮件**。用户和组织并不需要属于同一家电子邮件网络才能交换消息。全球电子邮件基础设施已经将互联网中的服务提供商、组织、域和用户连接起来。因此，过去使孤立消息网络具有吸引力的历史条件已不复存在，现在是时候重新考虑全球聊天服务的技术架构了。

2. 下一代即时通讯服务是邮件与聊天共用一套信息基础设施

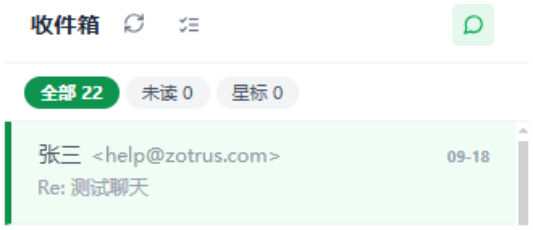
电子邮件通常首先被视为一种通信格式，但对于本文讨论而言，它更重要的特性在于其架构：它是一种已经建立、可以互通的全球通信基础设施。它用了数十年建立寻址规范、路由机制、组织层面的采用，以及独立服务提供商和域之间交换消息的能力。任何单一聊天平台都不可能重新创造这套基础设施数十年来建立起来的这种普惠连接能力。

这改变了下一代聊天服务的出发点。与其思考如何建立另一个全球消息网络，然后再将它连接到其他所有服务提供商，不如思考现有的聊天体验如何利用已经存在的全球电子邮件通信网络。这里的机会并不是用聊天取代电子邮件，而是让同一套底层基础设施同时支持这两种通信方式。

下一代聊天服务并不需要另一个全球聊天网络。更简单的方案是让邮件和聊天成为基于同一底层基础设施的两种通信体验。界面可以发生变化，而不需要重新构建通信网络。当用户需要正式、异步或以文档为中心的通信时，电子邮件可以继续保持电子邮件的形式；而同一套基础设施也可以通过面向聊天的界面呈现持续进行的对话。

这张演进的关键在于，必须为已经具备全球覆盖能力的基础设施增加适当的加密和交互层。S/MIME 可以为端到端加密通信提供密码学基础，而基于数字证书的身份可以提供一种可信的方式，用于建立并显示参与对话的人是谁。通过适当的自动化，用户不需要理解底层的证书、密钥和加密操作，就像今天他们也不需要理解电子邮件路由的工作方式一样。

零信 AI 邮通过允许用户在**邮件模式**和**聊天模式**之间切换，同时继续使用同一套底层加密电子邮件系统，展示了这一模式。其意义并不只是电子邮件应用增加了聊天界面。这一实践表明，为了提供聊天体验，通信网络本身并不需要被重新发明。私有聊天网络与全球电子邮件系统实际上可以汇聚成一套通信基础设施。



这也赋予了去中心化一个更准确的含义。去中心化通信模式并不意味着消除服务器、服务提供商或网络基础设施，也不要求每一次对话都变成点对点通信。去中心化来自这样一个事实：没有任何单一聊天服务提供商必须拥有全球消息网络。独立的服务提供商可以继续运营自己的

应用和服务，同时让其用户通过基于全球电子邮件系统的可互通基础设施与其他服务提供商的用户无缝进行通信。这也可以理解为这是一个多服务节点、多个服务提供商互联互通的全球即时通讯网络，而不是现在的多中心相互不互通的即时通讯服务网络。

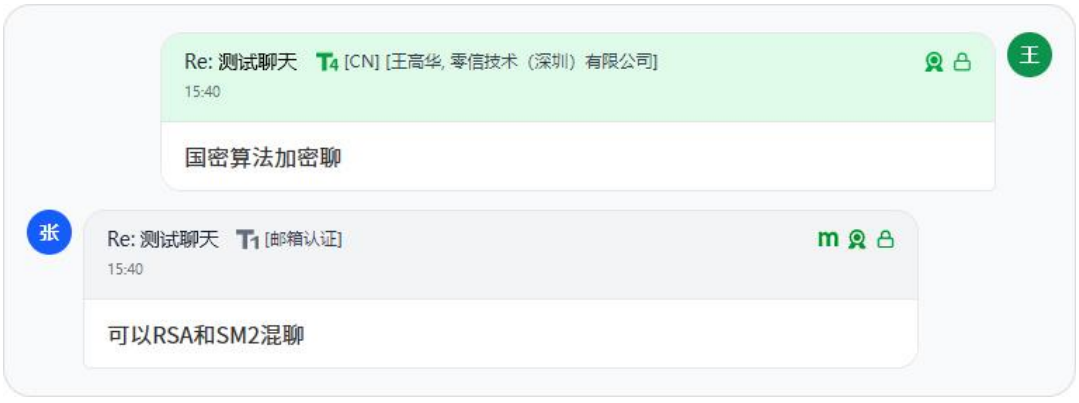
在这种模式下，用户不需要加入与其联系人相同的聊天服务平台。不同服务提供商可以在应用层保持独立，同时在通信层通过已经互联互通的全球电子邮件网络实现互通，其结果就是一个全新的去中心化的互通的聊天服务，基于一套能够支持不同通信体验的全球通信基础设施。

3. 可信身份：聊天服务缺失的另一半

端到端加密解决了私人通信中最重要的问题之一：谁能够读取对话内容？但它本身并不能回答全球消息环境中同样重要的另一个问题：我究竟在与谁通信？这是当前聊天系统尤其依赖平台控制身份的问题之一。用户名、电话号码、头像、账户名称或联系人条目可以告诉用户他们正在与哪个账户交谈，但它不一定能提供与基于数字证书的可信身份相同类型的、独立建立的可信身份保障。

因此，一个全球可互通的加密聊天系统需要的不仅仅是消息加密。它需要一种能够跨越服务边界传递可信身份，并让使用应用的人能够看到这个可信身份。S/MIME 数字签名为将消息与基于数字证书的身份绑定提供了基础，而受信任的第三方 CA 机构可以提供该证书背后的身份鉴证。这样，聊天应用就可以直接在对话中呈现由此产生的可信身份信息，而不是将其隐藏在技术性的证书细节中。

例如，零信 AI 邮的聊天界面已经将可信身份显示为：“T4 [CN] [王高华, 零信技术（深圳）有限公司]”。这种显示的意义并不在于这个标签本身，而在于用户能够看到由可信证书体系支持的身份认证级别和身份信息，而不是只能依赖对方对自己的声明。



当通信跨越组织、地域或平台边界时，这一点尤其重要。在封闭的聊天网络内部，平台控

制账户体系，并可以提供自己的账户身份认证机制。然而，在一个可互通的网络中，参与者需要一种共同的建立信任的方式，而这种方式不能依赖双方属于同一个平台。基于可信数字证书的身份为这种模式提供了一种可能的基础。

可信身份还改变了消息的使用方式。聊天应用可以不再把身份视为静态的个人资料元数据，而是让信任级别变得可见并可以采取行动，例如允许用户或组织区分不同级别的身份保障，并据此应用通信或信息释放策略。加密和身份解决的是同一问题的两个不同维度：加密保护对话，而可信身份帮助建立参与者是谁的信任。

这一点对于任何拟议的全球聊天服务架构至关重要。一个经过加密但无法建立可信身份的系统，仍然可能使用户暴露于假冒身份的相关欺诈之中。一个能够建立身份但不能保护内容的系统，则会使对话内容暴露在泄露风险上。因此，端到端加密与可信身份的结合，才能使可互通的消息通信形成更加完整的信任模型。

4. 零信 AI 邮做出了一个非常好的示范

零信 AI 邮在这一话题讨论中的意义，比支持聊天功能更为广泛。零信 AI 邮已经将这一模式带入全球公测阶段，提供了一个可运行、可公开测试的实现，用于展示自动化加密电子邮件基础设施是如何实现的。自主研发整套从数字证书和可信身份，到密码应用服务、邮件客户端、密码网关、密钥管理和自动化在内的完整产品和能力链，已经能证明这一自动化模式可以作为一个完整系统运行，而不仅仅是一种理论架构。

同样的原则也适用于加密聊天。零信 AI 邮提供了一个工作流实现，在这一实现中，加密电子邮件服务可以通过面向聊天的界面呈现，并以 S/MIME 作为密码学基础、以全球电子邮件基础设施作为通信层。这一实践表明，这种组合在技术上是可行的：界面可以变成聊天，而底层通信基础设施仍然是电子邮件。

但目标并不是让零信 AI 邮成为全球又有一个新的聊天服务提供商。更有意义的结果是，这一实践展示了行业的另一种发展方向。如果能够实现在现有电子邮件基础设施之上结合邮件、聊天、S/MIME 加密和可信身份，那么全球各大聊天服务提供商也可以考虑如何将相同的架构原则纳入自己的聊天服务中。

从这个意义上说，零信 AI 邮只是生态系统中的一个参与者，更不是当前聊天服务提供商的终结者。这项落地实践的价值，不在于有多少用户必须迁移到一个新的零信 AI 邮服务网络，而在于这一底层模式是否能够帮助在更广泛的互联网范围内实现安全且可互通的即时通讯。

5. 下一代即时通讯服务的一个提议

逻辑上的下一步并不是让每一个聊天服务提供商放弃其现有服务，也没有必要要求整个行业马上达成共识，马上采用这个方案。更根本的意义，是将聊天体验与“每个服务提供商都必须运营一个孤立的全球消息网络”这一假设分离开来。

现有聊天服务提供商可以继续维护自己的应用、用户社区、产品功能和商业模式，同时将其消息服务连接到全球电子邮件基础设施。S/MIME 可以为端到端加密通信提供共同的密码学基础，而数字证书和身份服务可以为可信身份提供共同基础。服务提供商在服务层面仍然保持独立，但其用户将获得跨越服务商边界进行互通即时通讯的可能性。

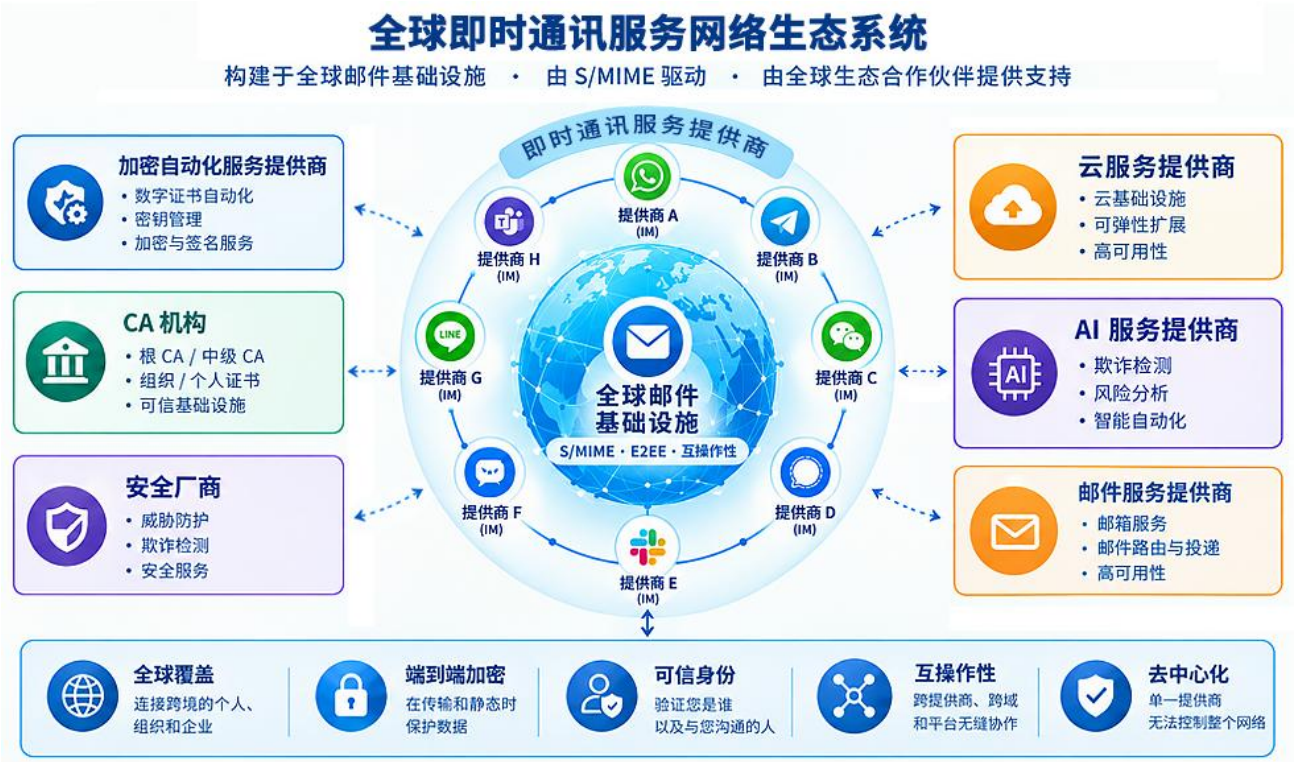
原则很简单：聊天服务提供商不需要消失；但它们需要实现互通。目标不是让所有人使用同一个聊天服务，而是让不同的聊天服务能够彼此无缝互通通信。

6. 技术已经准备就绪：让 S/MIME 服务于全球互联网

这一提议已经不再只是关于遥远未来可能实现什么的理论讨论。底层技术已经成熟，全球电子邮件基础设施已经存在，S/MIME 提供了成熟的密码学模型，而零信 AI 邮已经实现并测试了这些能力的工作组合。因此，剩下的挑战与其说是发明另一个聊天网络或服务，不如说是决定现有参与者如何连接各自的服务能力。

S/MIME 经常被讨论为一种电子邮件安全技术，但它的底层能力并不天然局限于电子邮件消息这一视觉概念。当加密、数字签名、基于数字证书的身份以及自动化的密钥和证书管理与周边基础设施结合时，它们可以支持更广泛的安全数字通信形式。因此，邮件和聊天可以成为建立在共同通信网络和密码学基础之上的不同体验。

这也是更广泛生态系统变得重要的地方。CA 机构、电子邮件服务提供商、电子邮件客户端、安全厂商、云服务和 AI 服务、密码技术提供商以及聊天服务提供商，都可以贡献自己已经最擅长的能力。没有任何一家企业需要拥有整个通信技术栈。行业可以建立在共享标准和可互通基础设施之上，而专业化的服务提供商则分别贡献身份、证书、加密、自动化、用户界面、网络服务以及其他能力。



如果整个行业采用这一方向，S/MIME 就不必局限于某一个产品或某一家服务提供商。它可以成为一个共同的安全层，用于帮助连接现有的通信生态，而不是成为锁定在单一平台内部的另一项专有安全功能。技术从产品能力走向基础设施，正是通过这种方式实现的：不是由一家企业拥有它，而是由众多参与者共同在其上构建。

7. 世界不需要消息孤岛

今天聊天系统的碎片化有其历史根源，而这些根源解释了为什么私有消息网络能够取得如此大的成功。但互联网已经发展。如今，世界已经拥有重新思考这一架构所需要的连接能力、基础设施、标准、计算能力和密码技术。

核心问题已经不再是另一家公司能否建立另一个成功的聊天平台，而是全球互联网能否最终让聊天实现互通，而不要求用户首先加入同一个平台。

答案始于已经存在的全球互联网基础设施。电子邮件用了数十年建立了一个全球、可互通的通信网络。S/MIME 可以提供端到端加密和基于数字证书的身份，使这套基础设施适用于更广泛的私人通信。聊天服务提供商可以保留自己的服务，同时连接到一个共同的通信层，而不是继续维护彼此孤立的消息孤岛。

零信 AI 邮的作用，是证明这一模式不仅仅是一种架构思想。完整的生态系统已经建立并

经过测试并实践，以证明这些组成部分能够协同工作，而从邮件到聊天的一键切换模式则证明，可以在全球电子邮件基础设施之上构建加密聊天体验，而不应该继续使用信息孤岛的聊天网络。

零信 AI 邮的目标并不是要成为全球聊天服务提供商，而是这个生态系统中的一个参与者。真正的机会，是为整个行业提供一条通往可互通的 S/MIME 即时通讯的路径，使用户不再仅仅因为联系人使用不同的即时通讯服务而彼此割裂。

现在的互联网不应该还有消息孤岛。它需要的是一个新的通信架构，让这些孤岛能够彼此安全地互通通信。技术已经准备就绪。基础设施已经存在。剩下的，是让两者连接起来。

S/MIME 不必永远只是一项电子邮件安全技术，它可以成为全球互联网范围内安全、可互通的即时通讯基础设施的一部分。

王高华

2026 年 9 月 24 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 294 篇(共 88 万 2 千多字)和英文 136 篇(19 万 3 千多单词)。