分析 · 2026年5月16日

← 上一页·下一页 →

当中间没有任何人时

对经过服务器的内容进行加密可以保护内容。而中间没有服务器则消除了这个问题。两者并不等同。

两个人，一场对话

当两个人在一个房间里进行面对面交谈时，没有人需要承诺自己什么都没听到。他们没听到是因为他们不在那里。当两个人将一张纸从一只手传递到另一只手时，中间没有任何人需要发誓自己没有阅读过。中间什么人都没有。

日常生活中的大多数事情都是这样运作的。我们不会与传递声音的空气，或是我们拿着的纸张签署保密协议。对话的隐私不依赖于中间人的承诺，因为根本没有中间人。这是现存最强有力的隐私形式之一：并非因为某人或某物表现良好，而是因为根本不存在这个某人或某物。

当对话转移到数字渠道时，默认情况发生了改变。通常的模式是这样的：两个人连接到一个服务器，服务器接收消息，对其进行加密或以加密形式存储，然后将其交付给收件人。服务器处于中间。服务器可能是诚实的，可能是经过审计的，可能在一个有利的司法管辖区并遵循严格的隐私政策运营。所有这些都可能是真的。但是，服务器确实处于中间。

加密与不收集数据之间的区别（第二部分）

在同一系列的上一篇文章中，我们提出：加密内容和不收集元数据并不等同。在此还需要明确阐述更进一步的一点：对经过服务器的内容进行加密，和根本没有服务器也是不同的。

第一种模式——服务器在中间，内容加密——保护内容免受服务器运营商、维护人员以及可能破坏系统的外部攻击者的影响。这很重要。但它并没有消除服务器的存在。服务器仍然在那里，仍在处理元数据。它仍然是一个可能收到法院命令、受到合法干预、政治压力或安全漏洞影响的节点。它仍然是一个需要你对某人寄予信任的节点。

第二种模式——两端之间没有服务器——并不能更好地保护加密内容：如果密码学是坚固的，在这两种情况下内容都会受到保护。改变的不是内容。改变的是，*“服务器会发生什么？”*这个问题不再有意义，因为根本没有服务器可供提问。

信任、缺失及其区别

信任是可以被妥善寄托的。诚实的公司确实存在，严谨的审计师确实存在，对用户有利的法律确实存在。严格遵守上述所有条件的服务也是存在的。如果信任赋予了一个值得信赖的运营商，那也不失为一个好安排。

但是，信任再坚固，也只是信任。这是一种社会解决方案，而不是技术解决方案。公司可能会易主，司法管辖区的政府可能会更迭，法院传票可能明天就会送达，新的漏洞可能下个月就会被发现。这些并非出于恶意，而是因为运营商是存在的，而一切存在的事物都受制于世界上的偶然性。

运营商的缺失则不受这些相同偶然性的影响。法院命令不能向一个不存在的服务器索要数据。攻击者无法入侵一个不存在的服务器。公司政策的改变不会影响它从未拥有过的数据。核心观点很简单：不存在的数据是不会丢失的。

关于服务器端的合法论点

提供带有中间服务器的专业消息服务的供应商通常会提出三个完全有效的论点。第一，当接收者离线时，需要服务器来保证交付。第二，内容加密是强大的，因此运营商无法阅读它。第三，该服务符合欧洲立法，数据受到法律保护。

这三个论点都是真实的。没有一个改变了问题的本质。服务器确实允许存储消息以延迟交付；但同样真实的是，延迟交付可以通过其他方式解决，即通过设备之间已完善数十年并在今天运行的直接通信协议。在可靠的服务中，传输中内容的加密确实很强大。欧洲立法对用户的保护确实远超许多其他地方。

问题不在于带有中间服务器的服务是否合法、是否安全，或者它们是否保护内容。它们可以做到这些，它们是合法的，且通常是安全的。问题在于，拥有中间服务器是一种架构选择，而不是技术必然。每一个选择都有其后果。拥有中间服务器的架构必然会产生一个必须信任的主体。而没有中间服务器的架构则不会。

法律的规定与架构的实践

《通用数据保护条例》（RGPD）并不要求特定的架构模式。它要求的是结果：数据最小化、有限目的、默认和设计上的隐私保护，以及证明合规性的能力。带有中间服务器的服务可以满足所有这些要求。但没有中间服务器的服务通过其构造本身就满足了其中的几项要求，而不是仅仅通过声明。当你根本没有一个可以收集数据的服务器时，绝对的最小化——即除了传递消息严格需要的数据外，不收集任何东西——就变得轻而易举了。

对于不敏感的日常使用，带有服务器的架构是完全合理的，信任一家认真的运营商也是一个有效的安排。但对于其他用途——那些涉及受规管职业机密、带有道德责任、触及特别敏感信息的用途——没有信任点的存在就不是一种奢侈，而是一种结构性优势。

致专业读者

面对一项专业通信服务，人们应该提出的问题（在该系列前几篇文章中已经很熟悉了），只需补充最后一个关于架构的问题：

1. 它在传输中是否加密内容？（很可能）
2. 它是否生成并存储有关我和谁交谈以及何时交谈的元数据？（很可能）
3. 在我的设备和收件人的设备之间是否有服务器？
4. 如果有：由谁运营，在哪个司法管辖区，以及必须发生什么才会迫使他们交出关于我的数据？
5. 如果没有：上述问题则失去意义。

这两类服务之间的区别不是程度上的，而是类型上的。当需要向客户、患者或同事解释时，最诚实的表述也是最简单的：其中一种中间有人，而另一种没有。

本文为Cuadernos Lacre的初始系列画上了句号。在探讨了加密、元数据和职业保密之后，我们补全了架构层面的拼图：加密内容和中间没有服务器是两码事。两者都是合法的；但只有一种能够消除信任点。

来源及延伸阅读

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. 提出系统保障应在端点而非中间信道实现的原则的奠基性文献。
- 欧盟法规 (EU) 2016/679，第25条 —— 默认及设计上的数据保护。
- 欧盟法规 (EU) 2016/679，第5.1.c条 —— 数据最小化原则。
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. 探讨通过设计实现数据收集最小化架构的章节。

← 上一页GDPR 与专业即时通信：为何大多数人都在不知情中违规下一页
→CUADERNOS_LIST_SCHREMS_TITLE

最近阅读

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

随身携带本文，以备不时之需。

↓ Markdown ↓ 纯文本 ↓ PDF

文件将下载到您的设备中。您可以从那里将其保存、导入 Solo2 或在任何地方共享。Cuadernos 不会为您决定文件的去向。

火漆印章 · SHA-256 84e504a41b9c6ff8852f5c3e5e882c2d2e59c85616b998d6ffdab8fefe9a8fa6

Cuadernos Lacre · Menzuri Gestión S.L. 的出版物 ·
由 R.Eugenio 撰写 · 由 Solo2 团队编辑。

本网站不使用 Cookie，也不加载第三方资源。它使用自托管的匿名访问者计数器（位于我们欧洲服务器上的 Umami），并仅使用最少量的 JavaScript 来处理您的亮色/暗色主题偏好。无追踪器，无画像分析，无数据共享。如需关注我们：RSS。