

零信 AI 邮探秘之九：文档签名

为什么文档签名应当成为日常文档 workflow 的一部分

2026 年 9 月 24 日

文档很少孤立存在。一份合同需要经过起草、讨论、修改、交换、签署和保存，这些环节共同构成一个持续的业务流程。在许多情况下，相关沟通都是通过电子邮件进行，文档本身则以附件的形式传递。然而，当文档需要签署时，用户往往不得不离开现有 workflow，将文件上传到独立的签名平台，创建签署任务，邀请参与者，并在签署完成后再通过电子邮件发送给相关方。

对于需要集中管理签署流程的组织而言，这种模式可以发挥良好的作用。但它也引出了一个更广泛的问题：**当文档已经属于现有邮件 workflow 的一部分时，为什么签署文档还要成为另一套独立流程？**

问题不仅在于如何为 PDF 添加数字签名，更在于如何在整个文档生命周期中，将签名身份、文档完整性、信息保密性、可信时间和后续验证联系起来，同时避免不必要的复杂性，也不让文档脱离其所属的业务流程。

零信签通过将零信密码应用自动化基础设施从电子邮件扩展到电子文档，来应对这一挑战。它将基于证书的数字签名、可信身份、文档加密、时间戳签名和签名验证融入文档 workflow，以电子邮件作为自然的集成入口。

一、文档签名不应产生另一套 workflow

大多数在线文档签名服务都是一个独立的签名平台。用户必须上传文档、创建签署任务、邀请其他参与者，并在该服务中管理最终文档。这种模式可以提供结构化的处理流程，但也会在文档生命周期中引入另一个环境。

在日常业务沟通中，这种分离尤为明显。一份合同可能已经通过数十封电子邮件反复讨论，直到各方就最终版本达成一致。如果签署必须通过独立平台完成，参与者就需要在原有邮件往来和签署服务之间来回切换，才能完成一个本质上连续的业务流程。

文档的保管方式也是一个值得考虑的问题。签名服务要求用户先上传原始文档，文档就会进入一个独立的服务环境。这对于某些流程可能是合适的，但并非始终必要或理想。组织可能更希望内部文档继续保留在现有的通信、存储和档案管理环境中。

签署过程与已签署文档所携带的数字证书，也存在查别。平台账户或身份认证会话可以在特定服务中识别参与者。而基于证书的数字签名则通过密码学方式，将签名者身份与签名证书关联起来，并保护已签署内容的完整性。即使文档离开最初的工作流，这些证据仍然可以随文档保留。

由此引出了一个更根本的设计问题：签署过程应当主要依赖独立签名平台，还是应当让文档本身携带密码学身份证据，以便在脱离原始交易流程后仍能进行签署者身份验证？

对于许多业务文档而言，后者是一项重要能力。签署应当适应文档原本的处理方式，而最终文档也应保留后续验证所需的密码学身份证据。

二、数字签名不只是一张签名图片

“电子签名”通常被广泛用于描述各种表示同意或批准的方式。基于公钥密码学的数字签名，则提供了一组更为明确的技术属性。对文档进行数字签名时，签名操作会使用与数字证书相关联的私钥。数字签名能够保护已签署内容的完整性，并提供与签名者身份相关的密码学证据。接收方可以验证签名，以判断签署内容是否发生变化，以及签名证书是否符合适用的信任配置要求。

这一差异十分重要，因为在页面上展示姓名、输入姓名或插入手写签名图片，本身并不能提供同等的密码学证据。基于证书的数字签名也使身份表达更具实际意义。接收方不必仅仅依赖签名旁显示的姓名，还可以查看证书及其关联的身份信息。根据证书内容和信任配置，这有助于判断签名者是否与特定个人或组织相关联。

数字签名本身并不能证明文档中的所有陈述都是真实的，更不能保证该签名证书在所有环境中都受到信任。这些问题取决于具体的身份验证、信任和法律环境。密码技术所提供的的是一个可验证的基础，用于保障签名完整性并提供身份相关证据。

然而，要让数字签名成为日常工作中的实用能力，用户不应当在使用之前就必须成为证书专家。应用程序需要承担密码技术的复杂性，同时让用户能够理解相关结果。这与 S/MIME 电子邮件加密面临的易用性挑战相同。相关密码学标准早已存在，真正缺少的是将身份、证书、密钥和密码操作与人们日常使用的应用程序连接起来的自动化能力。

三、从邮件附件到本地文档

零信签通过零信 AI 邮 App 将 S/MIME 密码应用自动化的理念应用于文档。当文档以电子邮件附件的形式收到时，用户可以直接在现有的文档交换工作流中发起文档签名，而不必将文

件转移到独立的电子签名平台中。签署后的文档仍然在电子邮件中流转，以加密邮件的形式保存在用户自己的邮箱中，并与相关往来邮件一起归档。

但文档签名不应局限于通过电子邮件接收的文件。用户还会处理存储在本地计算机上的文档，包括 PDF、合同、报价单、报表、组织公告以及其他业务记录。因此，零信 AI 邮 App 还提供了独立的文档管理主菜单，用户可以在其中选择本地文档，执行签名及其他密码操作。

这一区别十分重要。电子邮件是零信签体验的核心组成部分，但并不意味着文档必须来自邮件附件。无论文档是作为邮件附件收到，还是从本地存储中选取，目标都是通过同一应用程序提供数字签名和加密能力。

因此，工作流可以围绕文档本身展开，而不必强迫文档进入另一套独立的签署平台环境。以一份常见的商务合同为例，流程可以从邮件对话中的附件开始。签署者使用自己的身份数字证书对文档进行数字签名，生成的 PDF 将携带数字签名及相关的基于证书的身份信息。如果文档包含机密信息，还可以针对指定接收方进行加密。附署时间戳签名可以补充可验证的时间信息，而接收方也可以在收到文档时或日后查看时验证签名。完成签署后的文档仍然可以在签署会话之外正常使用。它可以发送给另一方、存储在邮箱中、与相关记录一起归档，也可以在之后进行验证，而不必完全依赖原始签署平台的签名历史记录。

同样的方法不仅限于合同。它可以应用于协议、报价单、采购文件、报表、审批文件、组织通知、机密内部 PDF 以及其他常以邮件附件形式交换的商业文件。共同的要求是，这些文件已经属于某种沟通工作流程，并且需要身份验证、完整性、保密性、可信时间或后续验证。

对于需要集中自动化实现批量文档签名的组织，零信签提供了一个文档密码应用自动化网关实现路径，将相同的文档签名和加密功能扩展到企业系统和受控邮件环境中。网关是实现相同密码应用自动化功能的企业自动化路径。个人和小型企业用户可以通过零信 AI 邮 App 操作，而企业组织则可以通过网关自动执行证书管理、签名、加密及相关的密码操作。

四、签名与加密解决的是不同问题

数字签名和文档加密相辅相成，但两者不能混为一谈。数字签名提供与签名者相关的证据，并保护文档完整性。加密则控制谁能够读取文档。一项功能不能取代另一项功能。

一份经过数字签名的文档，任何获得该文档副本的人都可能读取其内容。对于公开公告、已发布声明以及更重视真实性而非保密性的文档而言，这可能完全合适。但对于合同、财务记录、内部审批文件以及其他敏感业务文档，仅仅能够验证签名可能还不够，往往还需要访问控制。

零信签可以使用有权阅读者的公钥，为一个或多个授权阅读者加密文档。指定阅读者随后可以使用各自对应的私钥解密文档。这将安全电子邮件中采用的基于身份的密码学模型扩展到了通过同一工作流交换的文档。

两者的区别可以简单概括为：**通过签名建立有关签署者的密码学证据并保护文档完整性；通过加密控制谁能够读取文档内容**。当两种操作都需要执行时，它们可以作为同一个文档安全流程中的组成部分协同工作。用户不必将保密性视为一个无关的独立问题，也不必始终借助另一套系统来解决。

签名验证也是同样的道理。接收方应当能够检查签名、评估相关证书及其信任配置，并判断已签署内容是否保持完整。让这一过程易于使用，特别是可视 UI 身份展示，是使文档安全真正实用的重要组成部分。

五、文档签名可信时间与长期验证有效

数字签名能够提供与签名身份和已签署内容完整性相关的证据。但当文档需要在数月甚至数年后接受审查时，还可能出现另一个问题：现有证据能否说明该签名在什么时间已经存在？

时间戳签名能够为已签署文档提供可验证的时间信息。这可以增强后续验证所依据的证据，尤其是在需要考虑证书有效期、证书过期或长期记录保存的情况下。

时间戳签名并不只是添加到 PDF 页面上的另一个视觉元素。它是一项密码学服务，可以为文档验证过程补充与时间相关的证据。其价值取决于时间戳证据、适用的信任配置以及随时间变化的验证要求。长期验证（LTV）也不仅仅是检查文档页面上是否出现了签名，而是保证日后审查文档时，签名、证书信息、时间戳证据以及相关信任信息都可以发挥作用。

零信签将时间戳签名默认集成到文档签名能力中。在适用的服务版本包含相应功能时，可支持已签署文档的长期验证。这使最终文档更适用于需要在原始通信结束后继续验证签署记录的业务流程。我们的目标并不是承诺每一份已签署文档在未来任何法律或技术条件下都始终有效，而是确保可信时间和后续验证成为文档安全生命周期中需要考虑的组成部分，而不是事后才处理的独立事项。

六、保留文档，也保留密码学证据

文档的生命周期不会在签署操作完成时结束。它可能被转发、归档、纳入其他业务流程，也可能由未参与最初沟通的人员进行审查。

因此，最终文档应当携带密码学证据，使其能够脱离原始签署工作流接受检查，基于证书

的数字签名正是为了提供这类可移植证据而设计的。这是一个重要的架构区别：一份携带可验证数字签名的文档，与一个主要依靠专用签名平台服务所维护的记录来理解和管理签署过程的工作流，并不是同一回事。

零信签让文档签署继续与现有的电子邮件交换和存储流程保持一致。已签署文档可以通过电子邮件返回，并与相关往来邮件一起保存。需要加密时，还可以针对指定接收方保护文档。这样，文档既保留了创建和交换时的业务背景，也能够让密码学证据随已签署内容一同传递。

零信签的目标并不是否定签署平台的作用，对于特定业务需求，组织仍可能需要集中审批系统、档案管理应用或其他工作流工具。零信签所解决的是另一类需求：无需让每一份文档都进入独立的签署平台，就能提供基于证书的文档签名与保护能力。

七、云签服务，无需交出原始文档

云签服务为用户带来了重要的便利：用户无需自行管理签名基础设施的所有环节，就可以完成数字签名。然而，传统的在线文档签署流程通常从将原始文档上传到签名平台开始，由平台管理后续签署流程。对于包含个人信息、机密合同、商业秘密或知识产权的文档，这意味着原始文档需要进入另一个服务环境，增加了文档签名处理边界。

零信签采用了不同的技术架构，将原始文档与云端签名操作分离。整个签名过程由用户设备上的零信 AI 邮 App 与云签服务协同完成。原始文档始终保留在用户设备上，零信 AI 邮 App 使用 SHA-2 或 SM2 算法在本地计算文档的密码学哈希值，并仅将该哈希值发送至云端签名服务系统。云签服务使用受信任的平台身份签名证书对哈希值进行签名，再将签名数据返回给零信 AI 邮 App。随后，App 在本地完成文档签名处理。

这种分工是整个签名服务设计的关键。云端提供所需的密码学签名能力，而原始文档仍由用户在本地上掌控。云签服务无需接收原始文档，即可完成其承担的签名操作。这意味着，使用云签的便利性不必以将内部原始文档交给外部签名平台为代价。对于个人用户，这有助于保护个人隐私；对于单位用户，这有助于减少合同、内部文件及商业敏感信息进入外部服务环境的必要性。

除了云签服务，零信签还提供使用用户自身身份数字证书的数字签名服务。两种服务满足不同需求：云签服务呈现平台签名身份，其目的是为了实现签名的便利性，而使用用户自身证书的数字签名服务呈现用户经过验证的身份，则是为了实现签名者的可信身份由密码学保证。两者都集成在零信签的文档工作流中，同时满足用户便利和身份可信的应用需求，并已在 App 的用户界面中明确区分。

原始文档留在本地，只有哈希值上云。 这正是零信签的云签工作流的核心优势所在。

八、从邮件密码应用自动化到文档密码应用自动化

零信 AI 邮的整体架构建立在一个简单的原则之上：密码能力应当集成到人们实际使用的应用程序和工作流中。对于电子邮件，这意味着将数字身份、证书生命周期管理、签名、加密、解密和验签与日常邮件操作连接起来。对于文档，则意味着将这些能力扩展到人们日常交换、审阅、签署、保护和保存的文件中。

两者共享同一底层密码基础设施。零信签不必将文档签名视为一套完全独立的密码基础设施，而是将现有的密码应用自动化模式扩展到另一种应用场景。这种架构也为互操作性创造了更广阔的空间。文档会在不同的邮件客户端、云平台、业务应用、组织和地域之间流转。基于成熟密码学标准的文档安全模式，有助于避免文档验证完全依赖于最初发起签署操作的应用程序。

互操作性并不意味着所有应用程序都会自动信任所有证书，或支持所有签名格式。信任配置、证书策略、标准支持情况以及接收方应用程序的能力仍然十分重要。零信签的目标是让密码学证据具有可移植性，并以标准为基础，同时允许不同应用程序和信任环境按照各自适用的规则进行验证。

从更长远的角度看，文档签名不应被视为附属于某一个应用程序的孤立功能。它属于一个更广泛的密码应用生态系统。在这一生态系统中，身份、签名、加密和验证可以共同支持邮件、聊天、文档以及其他数字化工作流。

行业已经建立了许多必要的密码学基础组件。接下来的挑战，是通过自动化、易用的界面和可互操作的实现方式，将这些组件连接到日常应用程序中。

九、文档签名，融入电子邮件

文档在日常工作中经历创建、讨论、交换、修改、签署、保护和保存，其安全机制应当符合这一现实。

零信签将基于证书的数字签名、可信身份、签名验证、文档加密和时间戳签名融入文档工作流。这个工作流既可以从邮件附件开始，也可以从本地文件开始。它通过零信密码应用自动化基础设施，将这些操作连接起来，减少仅仅为了进行密码学保护而将文档转移到外部独立签署平台的必要性。

它的价值不仅在于能够为文档签名，更在于让身份、完整性、保密性、可信时间和后续验证在整个文档生命周期中协同工作，同时使已签署文档在原始工作流结束后仍然保留密码学证据。

电子邮件仍然是交换业务文档最广泛使用的环境之一。因此，让数字签名成为邮件工作流的一部分，是提升密码学文档保护可及性的一项切实举措。本地文档也应当通过同一应用程序和底层密码学基础，自然地获得相应支持。

这一理念与零信 AI 邮在电子邮件安全领域所采取的方法一致：密码技术提供信任基础，自动化消除不必要的复杂性，而用户体验则应当融入人们已有的工作方式。

零信签，自动化完成文档数字签名、加密和时间戳签名，并融入电子邮件 workflow。

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 298 篇（共 89 万 7 千多字）和英文 139 篇（共 19 万 9 千多单词）。

