

混合信任：零信 AI 邮的创新信任模型

2026 年 10 月 22 日

数字信任不应要求用户在全球互操作性、丰富的身份展示和合理的证书成本之间做出取舍。同样，向后量子密码（PQC）迁移，也不应要求组织在一夜之间放弃现有的密码基础设施。而我国用户还有采用国密算法实现邮件签名和文档签名的现有系统不支持的难题，如何同时做到国密合规和全球信任？

零信 AI 邮通过一个命名为 **Hybrid Trust（混合信任）** 的创新方案应对这些挑战。通过融合两个信任域，并采用多重数字签名机制，零信 AI 邮既能让标准邮件客户端和文档阅读器验证具有全球信任基础的数字签名，又能通过零信 AI 邮 App 展示更丰富的可信身份信息。这一架构也为国密合规和未来向后量子密码迁移提供了可扩展的技术思路。

要理解混合信任，首先需要了解零信 AI 邮的两个信任域。

一、两个信任域：零信信任与全球信任

零信 AI 邮构建了两个相互补充的信任域：**ZTmail Trust（零信信任）** 和 **Global Trust（全球信任）**。两者在密码应用生态中承担不同的角色。

1. 零信信任

零信信任是零信技术自身生态内建立的信任域，为邮件和文档提供可信身份服务与密码应用服务，包括以下身份认证等级：

- **T2 — 个人身份认证（IV, Individual Validation）**：展示经过认证的个人姓名。
- **T3 — 单位身份认证（OV, Organization Validation）**：展示经过认证的单位名称。
- **T4 — 单位员工身份认证（SV, Sponsor Validation）**：展示经过认证的单位名称和员工姓名。

通过验证相应的数字签名和证书信息，零信 AI 邮 App 可以展示对应认证级别的可信身份信息。零信信任旨在为零信生态内的可信身份识别和密码应用提供支持。

2. 全球信任

全球信任面向更广泛的全球生态，依托由全球公共信任证书颁发机构（CA）签发的数字证书，为邮件和文档提供可互操作的数字签名验证能力，如邮件客户端 Outlook 和文档阅读器 Adobe Reader。它涵盖邮件证书和文档签名证书，使兼容的邮件客户端和文档阅读器能够在零信 AI 邮生态之外验证相应的数字签名，而不必依赖零信 AI 邮 App。

3. 两个信任域，各司其职

零信信任和全球信任的定位十分清晰：

- **零信信任：**提供可信身份服务，并支持在零信 AI 邮生态内展示经过认证的身份信息。
- **全球信任：**提供基于全球公共 CA 的信任基础，实现与更广泛生态的互操作信任。

两个信任域并非相互竞争，而是相互补充，因为对于大规模的组织应用，大部分签名和加密应用还是在组织内部实施。零信技术创新地将这两个信任域结合起来，在全球互操作性、可信身份展示和成本控制之间取得平衡，这就是**混合信任（Hybrid Trust）**。

二、什么是混合信任（Hybrid Trust）？

混合信任是零信 AI 邮提出的一种创新信任模型，通过将全球信任的数字签名与基于零信信任的第二个数字签名相结合，实现不同信任域之间的协同。

用户不必为每个身份认证等级都购买由国际公共 CA 签发的身份证书。混合信任将两个功能分开处理：由全球信任的证书签名提供外部互操作性，由第二个身份签名支持零信 AI 邮 App 和零信浏览器展示更丰富的可信身份信息。这一模式同时适用于邮件签名和文档签名。

1. 邮件签名中的混合信任

在优化后的邮件证书方案中，用户使用两类证书：

- 一张由公共 CA 签发、具有全球信任基础的 MV（Mailbox Validated，邮箱认证）S/MIME 证书。
- 一张由零信 CA 提供的 IV、OV 或 SV 身份证书。

全球信任的 MV 证书提供标准 S/MIME 签名所需的信任路径。额外的身份签名则使零信 AI 邮 App 能够根据相应的认证级别展示发件人的可信身份信息。

对于微软 Outlook 等兼容的标准邮件客户端，全球信任的 S/MIME 签名通过证书链及相关信任策略的验证，就可以显示签名有效及相应的证书信任状态。零信 AI 邮 App 则可以进一步验证第二个身份签名，并展示相应的 **T2**、**T3** 或 **T4** 身份认证标识及可信身份信息。

如下表所示，无论用户使用何种认证级别的 S/MIME 证书实现邮件签名，微软 Outlook 都只是显示签名有效标识，这使得混合信任的 UI 展示效果无论是微软 Outlook 还是零信 AI 邮 App 同采用全球信任的显示效果都是一致的。

	全球信任方案	混合信任方案
Outlook UI	签名者 help@zotrus.com  	签名者 help@zotrus.com  

展示		
零信 AI 邮 UI 展示		

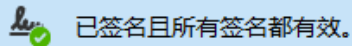
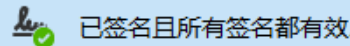
2. 文档签名中的混合信任

同样的原理也可以应用于文档签名。第一个签名通过云签服务，使用全球信任的平台签名证书完成。第二个签名则使用签署者的零信信任的 IV、OV 或 SV 文档签名证书。

对于 Adobe Reader 等文档阅读器，直接验证全球信任的云签平台证书，显示“签名有效”。零信 AI 邮 App 则可以验证第二个身份签名，并展示对应的 **T2**、**T3** 或 **T4** 身份认证标识及可信身份信息。

两个签名承担互补的作用：一个提供相应的外部信任路径，另一个为零信 AI 邮生态内的身份展示提供额外的身份凭据。

如下表所示，无论用户使用何种认证级别的文档签名证书数字签名 PDF 文档，Adobe 阅读器都是显示签名有效标识，这使得混合信任的 UI 展示效果无论是 Adobe 阅读器还是零信 AI 邮 App 同采用全球信任的显示效果都是一致的。

邮件客户端	全球信任方案	混合信任方案
Adobe 阅读器 UI 展示 (标准签名)		
零信 AI 邮 UI 展示		

3. 为什么混合信任具有实际价值？

除了应用程序的 UI 展示一样外，还可以通过对比两者的产品价格来真实感受混合信任的实际价值。如下表所示的是零信 AI 邮的两类信任方案的产品价格对比。

身份等级	全球信任方案	混合信任方案
------	--------	--------

T2 — IV 个人认证	203 元/年	123 元/年
T3 — OV 单位认证	252 元/年	143 元/年
T4 — SV 单位员工认证	272 元/年	151 元/年

混合信任方案将全球信任的 MV 邮件证书与零信信任的 IV、OV 或 SV 身份证书组合使用。在保持全球 S/MIME 互操作的同时，支持零信 AI 邮 App 展示相应身份信息，这显著降低了证书成本。对于需要为大量员工提供可信身份展示能力的组织而言，这种价格优势尤其明显。

关键在于理解混合信任究竟改变了什么：它并没有将零信信任的身份签名证书视为全球公共 CA 信任的证书，而是通过全球信任的签名实现信任互操作，再通过第二个身份签名提供更丰富的身份展示体验。

混合信任以更经济的方式，将全球互操作与可信身份展示结合起来。

三、混合信任是如何实现的？

混合信任采用两个数字签名，每个签名都关联各自的证书和信任域。邮件签名与文档签名的具体实现方式略有不同。

1. 邮件：全球信任 S/MIME MV 证书签名 + 零信 IV/OV/SV 身份证书签名

如果用户选购了混合信任相关的服务，或者用户导入了全球信任的 S/MIME MV 证书，零信 AI 邮 App 会自动使用混合信任模式对邮件进行数字签名，首先使用全球信任的 MV 证书生成 S/MIME 数字签名，然后按照 CMS（Cryptographic Message Syntax，密码消息语法）的签名结构，附加一个与零信信任的 IV、OV 或 SV 身份证书关联的第二个签名。

这样就形成了两条不同的验证路径。

对于邮件客户端如 Outlook：

- (1) 邮件客户端收到经过数字签名的邮件。
- (2) 客户端根据公共 CA 证书链及自身配置的信任策略，验证全球信任的 S/MIME 签名。
- (3) 如果相关验证通过，客户端就可以将签名显示为有效，并显示相应的证书信任状态。

对于零信 AI 邮 App：

- (1) 验证全球信任的 S/MIME 签名。
- (2) 验证附加的身份签名。
- (3) 读取身份证书中的相关信息，展示对应的 T2、T3 或 T4 标识及可信身份信息。

最终，邮件既可以利用全球 S/MIME 体系实现互操作，又可以在零信 AI 邮 App 中展示

更丰富的可信身份信息。

两个签名分别依据各自的证书链、签名格式和信任策略进行验证。每个签名的验证结果都可独立判断。

2. 文档：云签平台证书签名 + 零信 IV/OV/SV 身份证书签名

在文档签名场景中，如果用户选购了混合信任相关的服务，零信 AI 邮 App 会将平台云签名与额外的身份签名结合起来。第一个签名由零信 AI 邮云签服务使用平台签名证书生成，为其他文档阅读器提供相应的签名验证与信任判断依据。第二个签名使用签署者的零信信任的 IV、OV 或 SV 文档签名证书。零信 AI 邮 App 验证该签名，并展示对应的 **T2**、**T3** 或 **T4** 标识及可信身份信息。

因此，文档可以同时提供两种互补的签名体验：

- **在 Adobe 阅读器中：**平台签名可以依据相应的信任配置，提供签名有效性和证书信任状态。
- **在零信 AI 邮 App 中：**第二个签名支持展示签署者的 **T2**、**T3** 或 **T4** 标识及可信身份信息。

这一模式将外部软件的签名验证与零信 AI 邮生态内的身份展示结合起来，而不要求每位用户都购买全球信任的身份证书。

具体验证结果取决于签名结构、证书链、应用程序支持情况以及信任配置。

四、混合信任还可以用于后量子密码迁移

混合信任并不局限于两个信任域的组合。其核心思想是将不同的密码能力结合起来，通过多个数字签名协同工作，满足不同应用场景下的兼容性、安全性与合规性要求。这一架构思路不仅可以用于 RSA 与 SM2 算法的协同应用，也可以为未来向后量子密码（PQC）迁移提供技术基础。

1. RSA 与 SM2 双签名：兼顾国际兼容与国密合规

混合信任还可以应用于 RSA 与 SM2 两种密码算法的双签名场景。在需要兼顾现有国际生态兼容与中国商用密码应用要求的环境中，可以采用 RSA 和 SM2 两种算法分别生成数字签名。其中，RSA 签名主要用于兼容现有国际生态，SM2 签名则用于满足适用场景下的国密算法应用与合规要求。通过同时采用两种算法，系统可以在保留现有兼容能力的同时，引入 SM2 数字签名，为不同密码技术体系之间的协同应用提供支持。

这一模式可以同时应用于邮件数字签名和文档数字签名。例如，在邮件签名场景中，可以在符合相应标准的签名结构中组合 RSA 与 SM2 签名，使支持传统 RSA 算法的邮件客户端继续验证 RSA 签名，而支持 SM2 算法的邮件客户端能够验证 SM2 签名。文档签名也可以采用类似思路，为不同的文档阅读器和验证环境提供相应的签名验证路径。

具体实现需要遵循 S/MIME、CMS 或相关文档签名标准的要求，并确保签名结构、证书配置、算法支持及验证流程相互兼容。双签名可以为兼容国际算法与国密算法应用提供技术基础，但是否满足特定场景的国密合规要求，还取决于适用法规、标准、产品认证和实际部署方式。

2. 传统算法与后量子算法的组合签名

量子计算的发展对当前广泛使用的公钥密码算法构成了长期挑战。随着组织开始为量子安全做准备，需要寻找一种迁移方案，既能保留现有系统的可互操作，又能逐步引入新的 PQC 密码算法。

如果直接全面切换到后量子密码（PQC），现有邮件客户端、文档阅读器、证书基础设施和业务系统可能面临兼容性问题。混合方案则提供了一种可供探索的迁移路径。

零信 AI 邮计划支持使用 PQC 算法和相应证书进行 S/MIME 签名与加密。在数字签名方面，将采用**混合信任**的思路，将传统算法签名与采用 PQC 算法生成的第二个签名组合起来。

其概念流程如下：

- (1) 零信 AI 邮 App 首先使用传统密码算法生成 S/MIME 数字签名。
- (2) 按照 CMS 的设计，再附加一个采用受支持的 PQC 算法生成的第二个数字签名。
- (3) 最终生成的已签名邮件或文档包含基于两种不同密码算法的数字签名。
- (4) 兼容传统算法的应用验证传统签名，支持 PQC 算法的应用则验证 PQC 签名。

只要邮件格式、算法标识、证书配置和验证实现相互兼容，不同应用就可以验证自身支持的签名。这一架构思路同样可以应用于文档签名，使传统算法和 PQC 算法的签名验证在迁移期间并存。

需要强调的是，双签名主要解决数字签名算法的协同与迁移问题。对于 PQC 加密，还需要设计适当的混合密钥建立与加密机制；仅采用双数字签名并不能提供后量子密码机密性。

3. 渐进式迁移，而非强制替换

无论是 RSA 与 SM2 的协同应用，还是传统算法与 PQC 算法的组合，核心目标都是降低不同密码技术体系之间的迁移成本，避免要求所有应用在同一时间完成全面替换。

组织可以根据自身的业务环境和合规要求，逐步引入新的算法，同时保留必要的传统算法支持。对于需要兼顾国际互操作与国密应用要求的组织，可以探索 RSA 与 SM2 双签名方案；对于面向未来量子安全的组织，则可以在标准与实现成熟的基础上，逐步引入传统算法与 PQC 算法的组合签名。

随着支持新算法的邮件客户端、文档阅读器和证书基础设施逐步普及，组织可以扩大新算法的应用范围，而不必一开始就要求整个生态同时完成替换。

当然，成功迁移并不只是增加第二个签名那么简单。证书配置文件、算法支持、签名编码、信任策略和互操作性都需要统筹考虑。具体方案必须依据相关标准和实际应用环境进行设计与验证。

混合信任的价值，在于提供一种灵活的架构思路：既可以协同不同信任域，也可以支持不同密码算法逐步共存，为兼容性、国密合规应用要求和未来密码技术演进提供可扩展的实现路径。

五、一套架构，应对多种信任挑战

零信 AI 邮的混合信任模型通过共同的架构思路，应对当前信任体系和未来密码技术演进中的两类挑战。

在信任与身份方面：

- 全球信任提供基于全球公共 CA 的互操作能力。
- 零信信任为零信 AI 邮生态提供额外的可信身份信息。
- 两者组合，在保持预期用户体验的同时，降低证书成本。

在国密改造方面：

- RSA 算法签名帮助兼容现有应用。
- SM2 算法签名为国密合规提供路径。
- 经过合理设计的混合实现，可以支持不同算法并存。

在后量子密码迁移方面：

- 传统算法签名帮助兼容现有应用。
- PQC 签名为采用抗量子攻击的数字签名算法提供路径。
- 经过合理设计的混合实现，可以支持迁移期间不同算法并存。

三种应用场景共享同一个核心理念：不再要求所有需求都依赖单一信任路径或单一密码算法，而是将互补的密码能力组合起来。

六、混合信任，零信 AI 邮的创新信任模型

数字信任并不只是某一张证书，也不只是一次签名验证结果。它还涉及互操作、证书信任、可信身份、应用程序支持，以及随着密码技术发展不断演进的能力。

零信 AI 邮的混合信任模型将零信信任与全球信任两个互补的信任域结合起来。在邮件和文档签名场景中，它通过全球信任的签名与额外的零信身份签名协同工作，使兼容的外部应用能够验证全球信任的签名，同时由零信 AI 邮 App 展示更丰富的可信身份信息。

这一架构也带来了实际的商业优势：用户可以用更低的证书成本，同时获得全球互操作及零信 AI 邮 App 中预期的可信身份展示效果，而不必直接购买全球信任的 IV、OV 或 SV 身份证书。这个证书费用节省对大中型组织的大规模部署至关重要。

面向未来，同样的多重签名设计思路还可以为传统算法与后量子算法并存提供架构基础。

混合信任不仅是一种证书组合策略，更是一种灵活的信任架构，旨在连接全球互操作、可信身份、成本优势与密码技术的持续演进。

王高华

2026 年 10 月 22 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 300 篇（共 90 万 9 千多字）和英文 141 篇（20 万 4 千多单词）。



