# 几乎所有本地部署 AI 大模型应用都在“裸奔”

本地部署 AI 大模型应用已经快速成为了各地政务服务和各行各业服务系统的默认配置，这得益于国家对 AI 大模型应用的大力支持和鼓励。但是，根据笔者的初步调查，几乎所有本地部署的 AI 应用都是以不安全的明文 http 方式交付使用，非常不安全，必须尽快启用 HTTPS 加密方式使用，否则后果将是灾难性的！本文讲清楚这种“裸奔”的严重后果，并给出解决方案。希望所有已部署启用 AI 大模型应用和计划启用 AI 大模型应用的单位都能高度重视这个安全问题，并尽快及时解决这个安全问题。

## 一、 AI 大模型应用实际上也是一个 Web 应用

AI 大模型应用最终的入口也是一个 Web 应用，用户可以使用浏览器或 APP 来访问 AI 应用。而 Web 应用 HTTP 协议是一个明文传输协议，所有数据从浏览器到应用服务器之间的传输都是明文，非常容易被非法窃取和非法篡改，这就是“裸奔”！


无论部署的 AI 应用是以内网 IP 地址访问还是公网域名访问，只要是 http 方式访问，就是不安全的。读者朋友可以使用浏览器访问一下已经部署的 AI 大模型应用，所有浏览器一定会提示“不安全”，这是真的不安全！只不过是如果使用微信内置浏览器访问或者其他 APP 方式访问时没有这个安全警告，很容易被人忽略了这个非常严重的安全问题。

AI 大模型应用的核心是数据，如果把宝贵的政务数据或企业数据交给了 AI 大模型，结果是由于 HTTP 明文方式的输入和输出而导致了这些重要的数据由于明文传输而被非法窃取而泄露，那就是丢西瓜捡芝麻了！因为数据才是核心资产。而 HTTP 明文传输的另一个安全问题是数据可以非常容易地被非法篡改，这个非法篡改不仅污染了大模型所依赖的宝贵数据，更加严重的是导致 AI 大模型输出的结果将极有可能是灾难性的后果！

## 二、 所有 Web 应用都需要 HTTPS 加密来保护机密数据流通安全

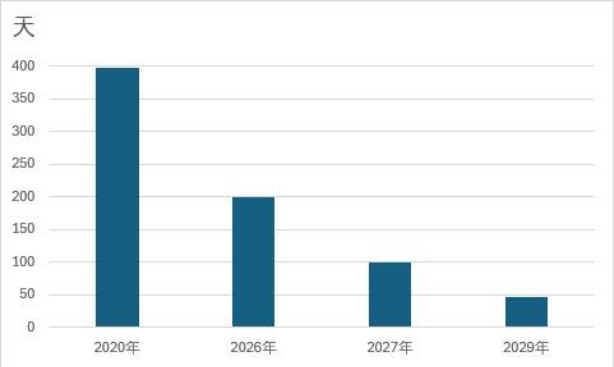
只要是 Web 应用，为了保障从 Web 客户端(浏览器或 APP)到服务器端的数据传输安全，都必须在 Web 服务器或前置网关部署 SSL 证书实现 HTTPS 加密，这已经成为全球所有 Web 应用的默认配置，当然也必须是 AI 大模型应用的默认配置，否则无法保障 AI 应用的安全。

这就要求在部署 AI 大模型时必须在 AI Web 服务器或前置网关上部署 SSL 证书，当然必须先向 CA 购买和申请 SSL 证书，包括全球信任的国际 SSL 证书和国密合规的国密 SSL 证书，无论是内网部署还是公网部署。公网 SSL 证书只能绑定公网域名和公网 IP 地址，如果是内网部署，则需要把公网域名解析到内网 IP 地址，或者部署支持内网 IP 地址和内部域名的内网 SSL 证书。

不仅仅 AI 大模型的 Web 应用需要 HTTPS 加密，训练 AI 大模型所需的数据的全生命周期流通也都需要 HTTPS 加密，包括数据采集，必须 HTTPS 加密方式从数据源传输到云端服务器；数据加工，必须 HTTPS 加密方式从数据收集点传输到数据处理点；数据使用，必须 HTTPS 加密方式从数据处理点传输到数据提供点，数据提供商必须以 HTTPS 加密方式为用户提供数据服务。也就是，只有实现了数据的全生命周期中的流通传输安全，才能真正保证训练 AI 所需的数据的真实性和完整性，才能保证最终的 AI 应用能生成真实可信的结果，这是 AI 应用的成功关键，核心技术就是 HTTPS 加密。

## 三、 SSL 证书有效期将缩短到 47 天，HTTPS 加密急需实施 SSL 证书自动化管理

为了保障 HTTPS 加密的安全，国际标准组织 CA/浏览器论坛已经制定了不断缩短 SSL 证书有效期的时间表，SSL 证书有效期将从 2026 年 3 月 15 日起缩短为 **200 天**，2027 年 3 月 15 日起为 **100 天**，2029 年 3 月 15 日起为 **47 天**，这就是使得人工申请和部署 SSL 证书的传统方式成为了不可行的部署方式，这同时给 AI 大模型的部署 SSL 证书实现 HTTPS 加密带来了困难。




当然，国际标准组织也是在目前全球 11 亿张有效 SSL 证书已经有超过 80%的 SSL 证书部署实现了自动化的前提下做出了这个标准更新，市场上已经有各种成熟的 SSL 证书自动化管

理解决方案可供选择来实现 SSL 证书自动化部署，AI 大模型在部署时必须选择合适的 SSL 证书自动化管理解决方案来实现 SSL 证书的自动化管理，只有这样，才能保证 AI 应用以 HTTPS 加密安全方式为用户提供服务。

## 四、 保障我国 AI 大模型应用安全，急需实现国密 HTTPS 加密自动化

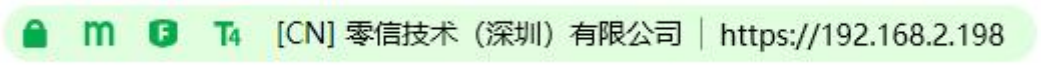
在目前不确定的复杂国际形势下，为了保障我国 Web 应用安全，我国正在大力推广普及应用商用密码算法的国密 SSL 证书来实现 HTTPS 加密，网信办等四部委发文《互联网政务应用安全管理规定》要求所有政务服务都必须采用商用密码实现 HTTPS 加密安全连接政务应用，当然也适用于政务 AI 大模型应用。这不仅仅是等保和密评的要求，也是保障我国重要 Web 应用安全可靠的不间断服务的要求，因为已经发生了俄乌冲突 RSA 算法 SSL 证书被断供和被吊销的恶意安全事件。

但是，要实现国密 HTTPS 加密，必须改造 Web 服务器支持国密算法，部署国密 SSL 证书才能实现。所以，国际上的 RSA 算法 SSL 证书自动化解决方案不适用于我国国密 SSL 证书自动化管理，必须有适合我国国情的国密 HTTPS 加密自动化解决方案，只有采用国密 HTTPS 加密自动化管理技术才能真正快速实现我国 AI 大模型应用安全所需的 HTTPS 加密保障服务。

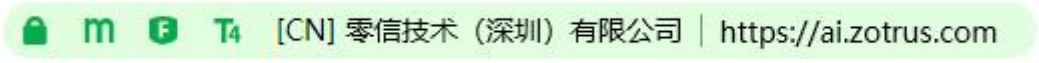
## 五、 零信技术已为保障 AI 大模型应用的 HTTPS 加密自动化提供多种可选解决方案

零信技术已经成功打造国密证书自动化管理全生态产品和解决方案，并已经广泛用于政务、电信和教育等行业的 Web 应用，自动化实现国密 HTTPS 加密和 WAF 防护，自动化配置双算法双 SSL 证书，实现自适应算法的 HTTPS 加密，免费配套的国密浏览器--零信浏览器优先采用国密算法实现 HTTPS 加密，兼容其他浏览器采用 RSA/ECC 算法实现 HTTPS 加密，满足用户等保、关保和密保的所有合规要求，切实保障关键信息基础设施的 Web 应用安全，包括 AI 大模型应用安全。

对于内网部署 AI 大模型应用，可选申请和部署支持内网 IP 地址和内部域名的证签内网 SSL 证书(双证书)，支持 1-5 年有效期，一次安装，保用 5 年 AI 应用安全无忧。而对于有大量内网应用的政府单位和大型机构，可选部署国密 HTTPS 加密自动化网关内网版，内置迷你 CA 系统，实现双算法内网 SSL 证书的自动化签发和自动化部署，每台网关最多支持 510 个内网 Web 应用，自动化实现多个 AI 大模型应用的国密 HTTPS 加密和 WAF 防护。




对于公网部署 AI 大模型应用，传统人工申请和部署公网 SSL 证书的方式已经无法满足要求，因为不可能每月去申请和部署一次 SSL 证书，只有自动化一条路，那就是部署国密 HTTPS 加密自动化网关公网版，由网关自动对接零信云 SSL 服务系统，自动完成双算法 SSL 证书的申请和部署，自动化实现自适应加密算法的 HTTPS 加密和 WAF 防护，每台网关最多支持 255 个 Web 应用的 HTTPS 加密自动化，自动化实现多个 AI 大模型应用的国密 HTTPS 加密自动化和 WAF 防护。




零信技术打造的双算法 SSL 证书自动化管理解决方案，不仅支持公网 SSL 证书自动化管理，而且支持内网 SSL 证书自动化管理，同时支持 HTTPS 加密方式的 WAF 防护，双重保障 AI 大模型 Web 应用安全，切实保障 AI 数据的流通传输安全和 Web 应用安全，让 AI 大模型应用不再“裸奔”，让 AI 大模型能更加安全可靠地为千行百业的智能化转型提供强大动力。

王高华

2025 年 5 月 26 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 214 篇(共 63 万 5 千多字)和英文 92 篇(12 万 3 千多单词)。