零信技术赋能密码应用自动化

密码技术是全球互联网安全的基石，各种密码应用每时每刻都在保护全球互联网安全，最常见的密码应用就是 HTTPS 加密，用 SSL 证书实现从用户端(浏览器和 APP)到服务端的数据传输加密，有效保障全球互联网数据流通安全。但是，HTTPS 加密的普及离不开 SSL 证书自动化，邮件加密要普及也是如此，其他密码应用要普及也只有自动化一条路。同时，如果让用户能直观地感受到这些高大上的密码应用也是一个需要解决的技术难题。这些方面零信技术都有创新，本文详细解读这个话题。

一、 万物互联和 AI 时代的互联网安全新威胁

万物互联时代最主要的特点是所有数据都上云，并通过云端来交换数据。这个数据交换就需要保证传输通道的安全，传统的 HTTP 明文传输是非常不安全的，各种数据在传输过程中非常容易被非法窃取和非法篡改。如果数据被篡改了，那 AI 就依赖了错误数据，其后面的智能结果就不堪设想了！这就是万物互联和 AI 时代的新威胁，必须保障数据传输安全，而不是传统的仅保障服务端安全的堡垒防护。

目前非常火爆的 AI 应用，不仅所依赖的数据源不能是明文传输，AI 服务与用户之间的数据交换也不能是明文传输，否则其后果也是不可想象的可怕！还有一样火爆的智能网联汽车和自动驾驶，如果车同路网和云端的数据交换都是明文通道，则所有通信数据都有可能被非法窃取和非法篡改，则智能驾驶的安全性是无法得到保障的。还有日益普及的智慧城市建设，各种摄像头和数据采集设备如果都是 HTTP 明文方式传输数据到云端，其危险后果也是不可想象的。

对于“让数据多跑腿”的电子政务服务，如果这个数据是在 HTTP 明文传输通道上跑，那是无法保障老百姓的机密数据安全的，这个安全问题并没有得到应有的重视，目前的电子政务服务只注重优质服务，并没有注重数据安全服务，这是不可持续的“优质服务”，绝对不能以牺牲数据安全为代价，这也不符合等保和密评的数据传输安全要求。

二、 只有密码技术，才能解决万物互联安全新威胁

唯一能解决万物互联数据传输安全的技术只有 HTTPS 加密，这是密码技术的最广泛的应

用之一，必须采用 SSL 数字证书来实现所有数据采集到云端服务器和从云端处理后下发的 HTTPS 加密传输，实现所有数据交换的 HTTPS 加密传输，只有所有数据能安全可靠地到达云端和下发到用户端，才能为用户提供安全的电子政务服务，才能保证 AI 基于真实数据为用户提供智能服务，才能保证万物互联的数据交换安全。

不仅如此，各种万物互联设备的软件升级，不仅需要 HTTPS 加密通道下载升级包，更需要用代码签名证书来实现升级包的数字签名，万物互联设备在通过 HTTPS 加密通道收到升级包后必须验证数字签名是否可信，验证附署时间戳签名是否可信有效，才能决定是否安装这个升级包，只有这样才能保证万物互联设备的升级安全。这也是密码技术的应用和安全保障，能高效保障设备升级安全，而无需复杂的传统杀毒防护系统。

还有电子邮件通信，IMAP 和 STMP 服务都必须启用 TLS 加密来保障邮件传输安全，而邮件内容也需要电子邮件证书实现端到端加密，实现邮件内容密文保存在云端邮箱中，这些保障电子邮件安全的可靠措施也是密码技术在提供安全保障，用数字签名来保障电子邮件发件人身份可信和保证电子邮件在传输过程中没有被篡改，用证书加密来保障电子邮件的全生命周期安全，包括在途安全和在云安全。

还有电子文档，需要数字签名才保证文档发布者的身份可信，保证电子文档在流转过程中没有被非法篡改。而用证书加密电子文档，则能保证只有有权阅读者才能解密这个文档，有效防止机密文档泄密。这些都是密码技术在提供文档安全保障。

三、 只有自动化实现密码技术应用，才能真正解决万物互联安全新威胁

现在，大家已经了解了只有 HTTPS 加密这个密码技术才能保障万物互联的数据流通传输安全。但是，HTTPS 加密普及应用也就是最近几年的事情，而 HTTPS 加密技术发明于 1994 年，为何在三十年后才得到普及应用呢？这是因为密码技术是一个非常高大上的技术，很难使用，特别是全生态应用。

要实现 HTTPS 加密，不仅需要 SSL 证书，而且还需要 Web 服务器和浏览器的支持，需要 CA 机构能签发 SSL 证书，用户人工申请和部署 SSL 证书，这个过程费时费力费钱，如果是一两台 Web 服务器部署人工处理还行，但是万物互联时代几乎每个设备都需要 SSL 证书，每个应用都需要 Web 服务端支持，这就需要自动化来搞定部署难题了。这就是为何 Let’s Encrypt 一推出自动化免费申请和部署 SSL 证书服务就收到全球用户热捧，只用了 3 年时间就做到了全球第一市场份额。

从 2013 年有证书透明日志系统以来，全球信任的 SSL 证书签发量已经超过 120 亿张，目

前有效的 SSL 证书超过 10 亿张，这就是万物互联的使用量，也只有万物互联才能有这么大的使用量。也就是说，HTTPS 加密也只有在实现了 SSL 证书自动化管理后才真正成为了保障万物互联数据传输安全的密码技术而落地应用，高大上的密码技术也只有自动化才能真正用于保障万物互联安全。

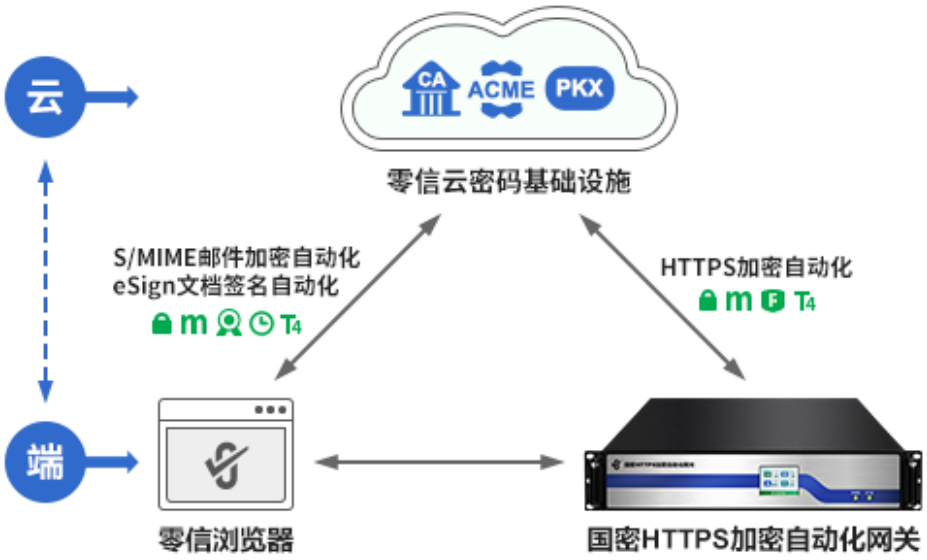
同样情况发生在电子邮件上，虽然人们一刻也离不开电子邮件，但是电子邮件从发明到现在已经有五十四年了，仍然还是明文形式存在。虽然 S/MIME 邮件加密技术标准早在 1995 年就提出来了，也就是 HTTPS 加密的第二年，但是到现在还没有实现普及应用电子邮件加密技术。全球每天发送的三千多亿封电子邮件都是明文邮件，虽然随着 HTTPS 加密的普及应用，已经基本实现了 TLS 邮件传输加密，但是电子邮件本身还是明文方式保存在云端邮件服务器中，无法真正保障邮件机密信息安全。电子邮件加密像 HTTPS 加密一样急需自动化证书管理来普及应用，真正实现密码技术的普及应用来保障电子邮件全生命周期安全。

还有电子文档数字签名和加密，虽然大家都知道这是一个好技术，并且已经普及应用于电子合同签署，但目前还没有更好的文档签名证书自动化技术来实现其普及应用。软件代码签名技术也一样，现在仍然是人工申请证书和人工实现代码签名，这也需要证书自动化管理技术来实现普及应用。

四、 零信技术，端云一体实现自动化+创新 UI，让密码应用无门槛+看得见

要想普及应用密码技术，只有自动化才能实现，才能真正实现密码泛在应用来保障全球万物互联安全。但是，目前全球只实现了 HTTPS 加密自动化，并且这个国际 SSL 证书自动化解决方案仅适用于 RSA/ECC 国际算法，无法满足我国商用密码 HTTPS 加密自动化应用需求。

零信技术创新解决方案是一个端云一体的解决方案，这个“端”就是零信浏览器和零信国密 HTTPS 加密自动化网关，这个“云”就是零信云密码基础设施，关键数据在“端”(零信浏览器)，彻底解决隐私保护难题。关键应用在“端”(零信网关)，彻底解决 Web 服务器国密改造难题，零改造完成国密 HTTPS 加密改造。而零信云密码基础设施，实现各种自动化服务所需算力在“云”，彻底解决“仅端”无法实现的算力和无法实现的自动化服务能力。



零信技术端云一体创新解决方案实现了“一端”和“一云”的紧密连接与配合，创新实现各种密码应用自动化，彻底解决“仅端”或“仅云”都不可能解决的技术难题，为用户创新提供：

(1) **HTTPS 加密自动化服务**：由零信国密 HTTPS 加密自动化网关提供服务，原 Web 服务器零改造，零安装 SSL 证书，零安装 ACME 客户端软件，自动化配置双算法 SSL 证书，自动化实现自适应加密算法的 HTTPS 加密。

(2) **S/MIME 邮件加密自动化服务**：由零信浏览器提供服务，自动化免费配置电子邮件证书，自动化实现公钥交换和密钥管理，自动化实现电子邮件加密、数字签名和时间戳。

(3) **eSign 文档签名自动化服务**：由零信浏览器提供服务，不仅无缝浏览阅读 PDF 文档，而且自动实时验证文档数字签名。自动化免费配置文档签名证书和加密证书，自动化实现 PDF 文档数字签名、加密和时间戳。

为了让用户能直接感知 HTTPS 加密自动化服务，零信浏览器创新 UI 实现：

(1) 加密锁标识：直接在地址栏第一个位置告知用户此网站已实现 HTTPS 加密

(2) 国密加密标识：在加密锁旁边展示，告知用户此网站已实现 SM2 算法 HTTPS 加密

(3) WAF 防护标识：直接在地址栏告诉用户此网站已采用了 WAF 安全防护

(4) 网站身份认证标识：在 https://网址前展示网站已通过权威第三方认证的可信身份信息

为了让用户能直接感知 S/MIME 邮件加密自动化服务，零信浏览器创新 UI 实现：

(1) 加密锁标识：表明此邮件已加密

(2) 国密加密标识：在加密锁旁边展示，表明此邮件已实现 SM2 算法加密

(3) 数字签名标识：表明此邮件已数字签名，邮件内容未被篡改，发送者身份可信

(4) 时间戳标识：表明此邮件有电子邮戳，邮件发送时间可信，不可否认

(5) 发送者身份认证标识：展示邮件发送者已通过权威第三方认证的可信身份信息

为了让用户能直接感知 eSign 文档数字签名自动化服务，零信浏览器创新 UI 实现：

(1) 加密锁标识：表明此文档已加密

(2) 国密加密标识：在加密锁旁边展示，表明此文档已实现 SM2 算法加密

(3) 数字签名标识：表明此文档已数字签名，文档内容未被篡改，文档发布者身份可信

(4) 时间戳标识：表明此文档有时间戳，文档发布时间可信，不可否认

(5) 发布者身份认证标识：展示文档发布者已通过权威第三方认证的可信身份信息

零信技术端云一体创新解决方案，不仅实现了 HTTPS 加密自动化、邮件加密自动化和文档签名自动化，而且零信浏览器集成 PDF 阅读器和邮件客户端，全球独家创新 UI 展示各种密码应用效果，让高大上的不可见的密码应用一目了然，让用户切实感受密码应用的魅力，增强用户在线信任，促成更多在线交易。

王高华

2025 年 3 月 10 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 204 篇(共 59 万 7 千多字)和英文 68 篇(8 万 4 千多单词)。