密码应用自动化+创新 UI，新方案应对新威胁

人们已经离不开互联网了，无论是工作还是生活。但是，互联网在为人们带来便利的同时也带来了许多安全威胁。本文总结出最新的危害最大的三大安全威胁，并给出了如何解除这三大安全威胁的解决方案，那就是端云一体的创新密码应用。而如何让人们清晰地了解高大上的密码应用正在保护人们的上网安全呢？那就是零信浏览器的 UI 创新，让密码应用可视化。

一、 互联网生活的三大安全威胁

互联网生活的第一件大事就是上网浏览信息、网上购物、网上银行、网上证券、网上办公等网上一切活动，无论是浏览器方式还是 APP 方式，第一大安全威胁就是假冒网站和数据窃取，就是假冒各种有高价值的网站，让用户上当受骗而诈取钱财；数据窃取就是针对明文 HTTP 网站通过各种非法手段在数据传输通道上非法窃取用户机密数据和非法篡改用户提交的重要数据。根据 Cybersecurity Ventures 的数据，到 2024 年，全球网络犯罪损失（包括假冒网站、网络钓鱼和相关诈骗）预计将超过 10 万亿美元，假冒电子商务网站兜售假冒商品，假冒银行网站获取用户登录账户信息而转走账户资金。全球估计表明，如果考虑到直接的财务打击和法律费用和恢复工作等次要成本，仅假冒网站就可能造成数千亿美元的损失。最近火爆的 AI 应用，也已经出现了大量的假冒知名 AI 厂商的网站和 APP，同时大量的 AI 应用都是 HTTP 明文方式部署，非常不安全，无法保证 AI 应用安全。

互联网生活的第二件大事就是收发电子邮件，这也是每个人每天都离不开的事情。但是由于电子邮件自发明以来一直是以明文方式收发邮件，邮件内容非常容易在传输过程中和存储过程中被非法窃取和非法篡改，非常不安全。根据美国联邦调查局(FBI)互联网犯罪投诉中心(IC3)发布的《2023 年互联网犯罪报告》显示，商业邮件攻击(Business Email Compromise, BEC)在 2023 年给美国企业造成了 29 亿美元的损失，成为第二大最具破坏性的互联网犯罪。2013 年 10 月至 2023 年 12 月期间，BEC 攻击事件给美国和全球组织造成了近 555 亿美元的损失。

互联网生活的第三件大事就是管理各种 PDF 文档，包括阅读、发布、归档等，由于 PDF 文件是明文无可信身份的电子文件，非常容易被假冒和被篡改，导致了各种假冒政府文件、假冒银行账单文件、假冒合同文件等假冒身份文件泛滥，这是第三大互联网犯罪，每年估计造成数千亿美元的全球经济损失。

以上就是全球互联网生活面临的三大安全威胁，其根源是互联网在发明时并没有采用任何

加密技术，都是明文协议，因为当时只是内部使用，根本没有想到会有今天如此的普及应用。当然，业界也在不断地弥补这个设计缺陷，所以才有了各种密码技术的应用来保障各种互联网应用的安全。

二、 只有深度融合密码应用，才能解除三大安全威胁

也正是由于互联网应用太重要了，所以，随着互联网应用的深入，也就有了各种密码技术应用来保障互联网数据传输安全、电子邮件安全和电子文档安全。

第一个密码应用就是 HTTPS 加密，这是解决明文 HTTP 传输协议的唯一可靠技术，并且已经在全球范围得到了普及应用，包括各种 AI 应用。全球信任的有效 SSL 证书签发量已经超过 11 亿张，这些 SSL 证书正在时刻保障全球万物互联的数据传输安全，从而彻底杜绝数据在传输过程的非法窃取和非法篡改。当然，这么大规模的密码应用是离不开自动化的，只有实现了 SSL 证书自动化申请和部署使用，才能普及应用这个密码技术来保障全球数据流通安全。

但是，目前这个普及应用的 HTTPS 加密技术并没有解决假冒网站难题，反而使得人们更难识别假冒网站了，因为假冒网站也有“安全锁”标识，这个以前被教育为网站是安全的标识反而成为了假冒网站犯罪的保护伞，这也许是谷歌浏览器不再显示“安全锁”标识的考虑之一，但这并没有解决问题，没能帮助用户正确识别网站可信身份。这是目前网站安全方面没有解决的难题，被全球网站广泛使用的 SSL 证书是不含网站身份信息的 DV SSL 证书，DV SSL 证书只有加密功能，其证明网站身份功能被阉割了，无法用于解决假冒网站难题；其好处是能自动化签发，降低了 SSL 证书普及门槛，从而推动了 HTTPS 加密的普及应用。而最新的全球 SSL 证书签发数据表明，能证明网站可信身份的 OV SSL 证书也开始实现自动化签发和部署，零信国密 HTTPS 加密自动化网关默认配置的国密 SSL 证书就是 OV SSL 证书，零信内网国密 HTTPS 加密自动化网关默认配置的双算法(RSA/SM2)内网 SSL 证书也都是 OV SSL 证书。

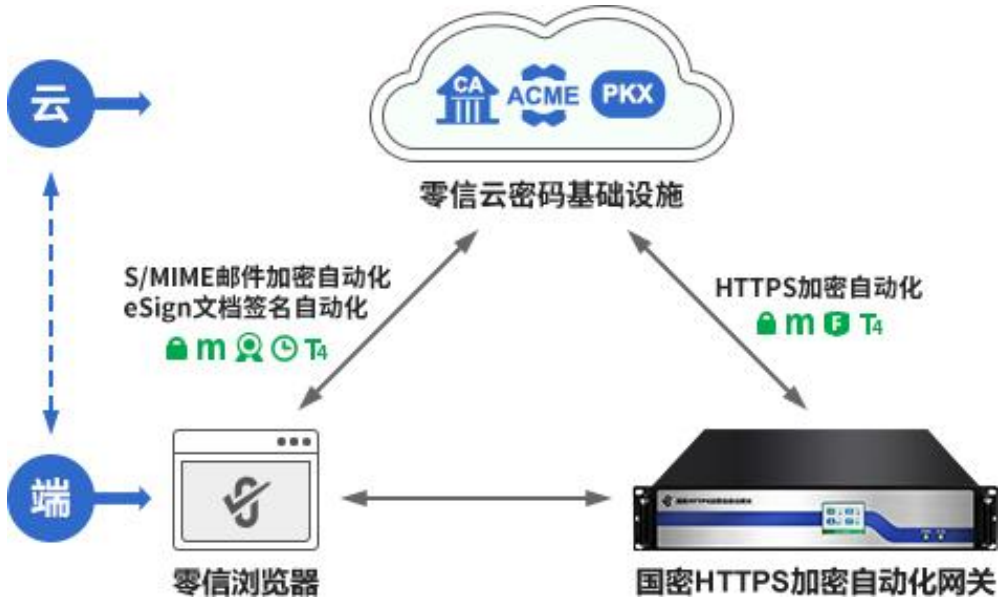
第二密码应用就是 S/MIME 加密和数字签名，这是解决 MIME 明文邮件安全的唯一可靠技术，电子邮件数字签名技术能有效解决电子邮件身份欺诈难题，电子邮件加密技术能有效解决电子邮件泄密难题，解决电子邮件在途传输和在云储存的安全问题。虽然 S/MIME 邮件加密技术同 HTTPS 加密技术同期发布，但是由于这个技术太难用，至今也没有得到大范围的应用，更谈不上普及应用了。要想实现 S/MIME 邮件加密，必须学习 HTTPS 加密的普及经验，也就是实现 S/MIME 邮件证书的自动化管理，只有这样才能普及应用 S/MIME 技术来保障全球电子邮件安全。

零信技术采用端云一体实现了电子邮件 S/MIME 加密和数字签名自动化，彻底解决了困惑

了全球邮件用户半个多世纪的技术难题。用户只需启用邮件加密自动化服务，就会自动化免费配置 S/MIME 邮件证书，就可以使用零信浏览器自动化加密每一封发出的电子邮件，自动化解密每一封收到的已加密邮件，自动化实现每一封发出的电子邮件的数字签名和时间戳，可靠证明每个发件人的可信身份和可信的邮件发送时间。

第三个密码应用就是 eSign 文档数字签名和加密，这是解决明文 PDF 文档无可信身份信息的唯一可靠技术，目前已经在电子合同签署得到了普及应用。但在日常文档管理，包括办公文档并没有得到普及应用。同时要想解决机密文档泄密问题，唯一可靠的解决方案就是用证书加密文档，只有拥有这个加密密钥的人才能解密阅读此加密文档，这就不再需要各种五花八门的防止机密文件外泄的管理手段了，只需用户保管好用于解密的文档加密证书即可。文档数字签名能有效解决文档身份可信难题，文档加密能彻底解决机密文档泄密难题，而要想普及这两个密码应用，唯一可行的方案还是自动化证书管理和应用。零信技术将继续采用端云一体方案自动化配置文档数字签名证书和文档加密证书，自动化实现电子文档的数字签名和加密，有效证明每一个电子文档可信身份和保障每一个机密文档的安全。

零信技术创新解决方案是一个端云一体的解决方案，投资建设了云密码基础设施，实现证书自动化服务所需算力在“云”，能为 HTTPS 加密自动化、S/MIME 邮件加密自动化、eSign 文档签名自动化提供双算法(RSA/SM2)SSL 证书、邮件证书和文档证书的自动化签发服务，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。而零信浏览器和零信国密 HTTPS 加密自动化网关则是两个重要的“端”，前者是为了保证用户的关键数据在“端”，彻底解决“仅云”的隐私保护难题；后者是为了实现用户的关键应用在“端”，彻底解决 Web 服务器为了实现 SSL 证书自动化需要安装 ACME 客户端的难题。



三、 只有创新 UI，才能让用户感知密码应用，放心使用互联网

互联网的三大安全威胁只有深度融合密码应用才能解除，但是高大上的密码应用如果看不见摸不着，用户就无法感知已经使用密码技术来保障互联网安全。这就是为何从发明了 HTTPS 加密开始，浏览器就有了“安全锁”标识，让用户一看到这个锁标识就知道已经实现了 HTTPS 加密，就可以放心地同网站交换数据和在线交易。

但是，随着 HTTPS 加密的普及，欺诈网站也会显示“安全锁”标识，这就有了 EV SSL 证书的绿色地址栏和直接在地址栏显示网站单位名称的改进方案。很可惜，谷歌浏览器率先抛弃了这个好的解决方案，使得欺诈网站又卷土重来，并且来势汹汹。

零信浏览器弥补了这个遗憾，是目前全球唯一一个继续支持 EV SSL 证书部署网站能显示绿色地址栏和单位名称的浏览器，并以浅绿色地址栏和单位名称来展示部署了 OV SSL 证书的网站，以专用标识来标识网站部署了国密 SSL 证书。还有更多的创新 UI，让用户能快速感知解决三个安全威胁的密码应用-HTTPS 加密、S/MIME 邮件加密和数字签名、eSign 文档数字签名和加密。

零信浏览器不仅仅是一个上网必用浏览器，而且是一个能收发加密电子邮件的邮件客户端，也是一个能实时验证文档数字签名和展示签名者可信身份的 PDF 文档阅读器，其丰富的 UI 展示，让用户对网站是否安全一目了然，对邮件是否安全一目了然，对文档是否安全一目了然。

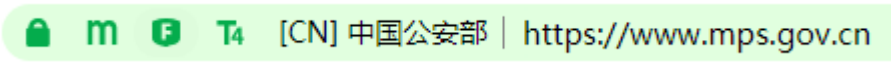
为了让用户能直接感知 HTTPS 加密自动化服务，零信浏览器创新 UI 实现：

(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://网址前面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，让用户放心使用互联网，增强用户在线信任，促成更多在线交易。

王高华

2025 年 4 月 14 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 208 篇(共 61 万 1 千多字)和英文 90 篇(11 万 9 千多单词)。