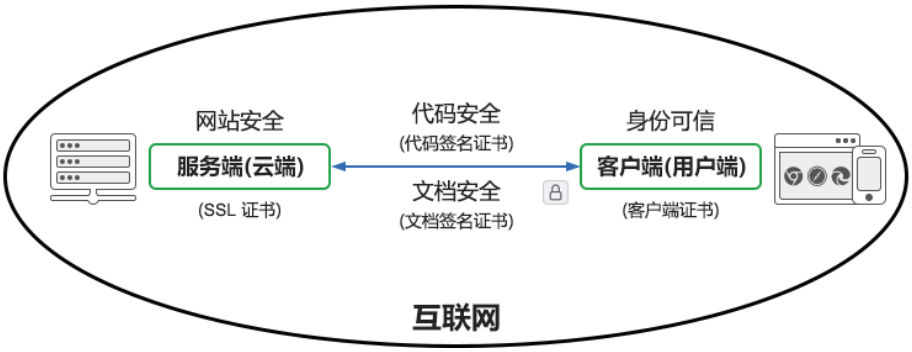
2023，零信技术为全球互联网安全奉献了中国方案

2023 年马上就要过去，新的一年 2024 即将开始。回首 2023，零信技术未负韶华，为全球互联网安全奉献了中国方案。展望 2024，零信技术砥砺奋进，继续为全球互联网安全提供更多创新产品和服务。

一、 密码技术全面保障了全球互联网安全

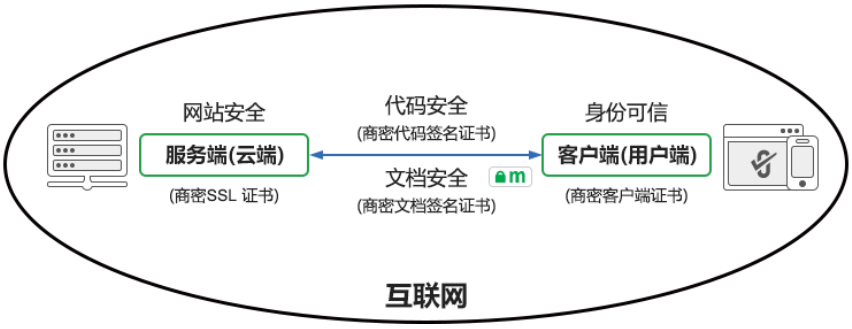
互联网从 90 年代开始商业化普及应用，最大的技术贡献是 SSL 证书的发明以及浏览器和 Web 服务器支持 HTTPS 加密，没有这些就没有今天的互联网的繁荣。因为互联网发明时是在内部使用，根本就没有考虑任何加密措施，全部都是明文传输，包括第一大互联网应用-Web 服务就是 HTTP 明文传输协议，第一个互联网应用-电子邮件也是明文传输-IMAP 和 SMTP，域名解析服务 DNS 也是明文协议。只有有了 SSL 证书，才实现了 HTTPS 加密传输协议，多了一个“S”就是 Secure(安全)。只有有了 SSL 证书，才实现了 IMAPS 和 SMTPS 加密收发邮件协议，多了一个“S”就是 Secure(安全)。只有有了 SSL 证书，才实现了 DoH (DNS Over HTTPS)和 DoT(DNS Over TLS)加密 DNS 服务，多了一个“S”就是 Secure(安全)。

SSL 证书不仅保障了服务器的身份可信，而且保障了信息从服务端到客户端的传输加密安全。不仅如此，还有客户端证书用于保障个体身份可信和用于电子邮件加密，文档签名证书用于证明文档可信和文档加密，代码签名证书用于软件代码身份可信。也就是说，是密码的最大应用 PKI/CA 技术和产品在全面保障全球互联网的安全可信，这个密码体系就是 RSA 密码体系，已经成功保障了全球互联网安全和万物互联安全 40 多年。其中，SSL 证书从 2013 年有证书透明日志系统记录开始就已经签发了 115 亿多张，有力保障了 Web 应用、电子邮件和 DNS 等所有系统的信息传输安全。



二、 商用密码为全球互联网安全提供了中国方案

正因为 RSA 密码体系太重要的，互联网安全已经离不开了。所以，这个垄断的技术就成为了制裁工具，导致了全球互联网安全的系统性风险。中国作为一个技术创新大国，已经在打破密码技术垄断方面提供了中国方案，这就是商用密码算法-SM2/SM3/SM4/SM9 算法，并已经同 RSA/ECC 算法一样成为了国际标准算法。中国已经参考 RSA 密码体系建立了完整的商用密码体系，包括建立了一系列商密标准、建设了能签发各种商密算法数字证书的 CA 体系、研发了大量的基于商用密码的互联网基础应用软件，如商密浏览器、商密阅读器、商密邮件客户端等等，实现了商密 HTTPS 加密、商密 IMAPS 和 SMTPS 加密、商密 DNS 加密等各种互联网安全保障应用。

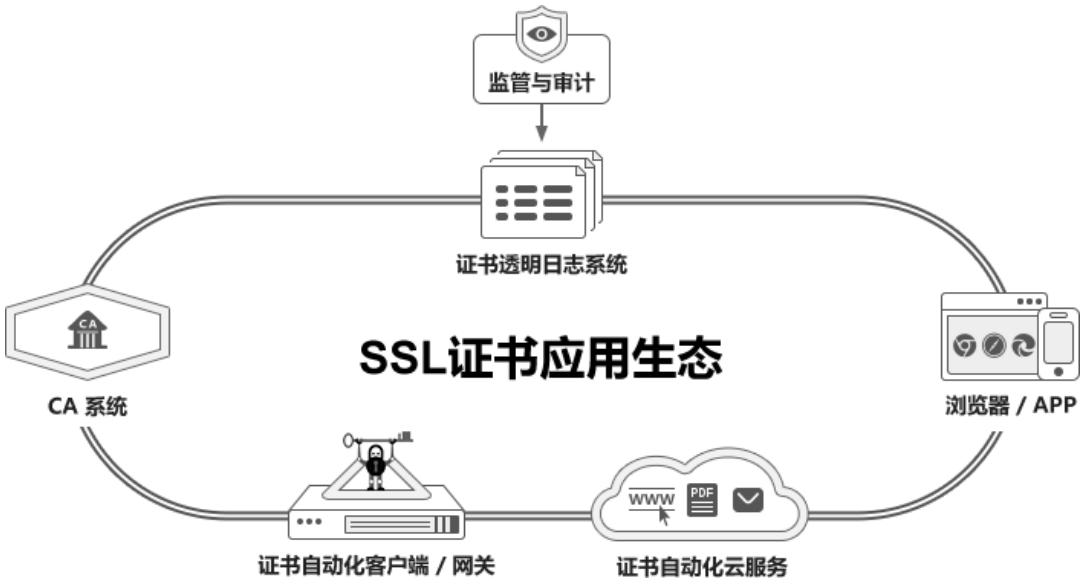


也就是说，中国的商用密码不仅已经开始应用于保障中国互联网安全可信，也是全球互联网用户的另一个选择，一个同样可以用于保障全球互联网安全的选项，这个选项像 RSA 密码体系一样已经非常完善，一样可以保障 Web 应用、电子邮件、电子文档和 DNS 等各种互联网应用的安全可信。这是中国密码对全球互联网安全的贡献，让全球用户有了更多的选择，保障了全球互联网能更加稳健的健康发展，保障了全球互联网用户能不间断地无差别地享受互联网服务。

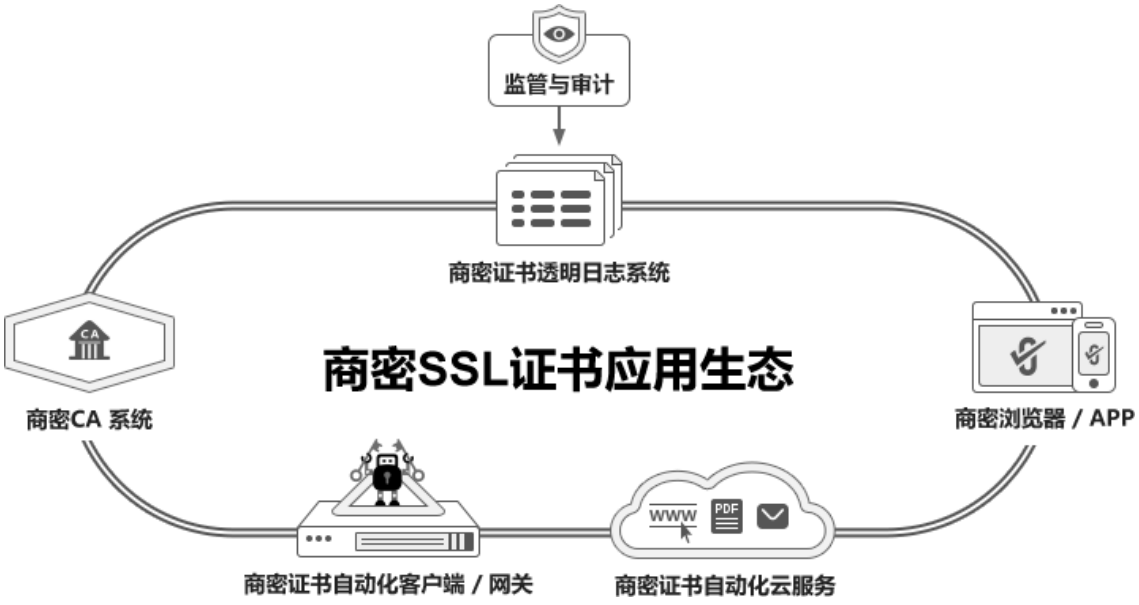
三、 零信技术奉献创新解决方案，让全球互联网用户有了更多的选择

SSL 证书和使用 SSL 证书实现的 HTTPS 加密是全球互联网安全的核心基础安全产品和应用，SSL 证书是全球用量最多的密码产品，这是一个围绕 SSL 证书签发、监管、应用的生态，包括能签发 SSL 证书的 CA 系统、用于监管 SSL 证书的签发行为的证书透明日志系统和基于这个系统的监管和审计、用于实现 HTTPS 加密的浏览器/APP、用于自动化申请和部署 SSL 证书的 ACME 客户端软件、硬件网关和云服务。这个生态保证了 SSL 证书能可靠地签发和快速

应用部署使用，从而保证了全球互联网的基础通信安全。



同样，采用商密 SSL 证书和使用商密 SSL 证书实现的 HTTPS 加密也是用户可选的全球互联网安全的核心基础安全产品和应用，也有一个围绕商密 SSL 证书签发、监管、应用的生态，包括能签发商密 SSL 证书的 CA 系统、用于监管商密 SSL 证书的签发行为的证书透明日志系统和基于这个系统的监管和审计、用于实现 HTTPS 加密的商密浏览器/APP、用于自动化申请和部署商密 SSL 证书的商密 ACME 客户端软件、硬件网关和云服务。这个生态保证了商密 SSL 证书能可靠地签发和快速应用部署使用，从而实现了采用商用密码来保障全球互联网的基础通信安全。



零信技术在即将过去的 2023 年为商密 SSL 证书应用生态建设做出了巨大的贡献，不仅保障了中国互联网应用的安全可信，而且为全球互联网用户提供了另一个可选项，其中零信浏览器，一个完全免费的商密浏览器不仅成为了中国市场份额第一位的用于实现商密 HTTPS 加密的浏览器，而且收到了来自 130 多个国家和地区用户的欢迎和喜爱，全球用户喜欢零信浏览器的 EV 绿色地址栏、喜欢全球首创的证书透明 UI 展示方式、喜欢全球首创的能实时验证 PDF 文档数字签名和展示签名者可信身份的内置 PDF 阅读器。

零信技术打造了商密 SSL 证书应用生态中所有必须产品，完善了商密 SSL 证书应用生态，主要包括以下 6 大创新产品：

(1) **零信浏览器**：一个基于开源 Chromium 的支持商密算法、支持商密证书透明的、完全免费的通用浏览器。

(2) **零信云 SSL 系统**：一个能签发支持商密证书透明的商密 SSL 证书的 CA 系统和商密 ACME 服务系统，为用户同时签发双算法(RSA/ECC 和 SM2)SSL 证书，使得 HTTPS 加密服务不仅支持商用密码体系，而且兼容 RSA 密码体系。

(3) **零信国密证书透明日志系统**：一个免费为 CA 机构提供 SSL 证书透明日志服务的证书透明日志系统，支持 SM2/RSA/ECC 算法 SSL 证书，并免费开放日志数据库以便第三方提供商密 SSL 证书的监管和审计服务。

(4) **零信国密 ACME 客户端软件**：SM2cerBot，一个免费的用于自动化申请和部署商密 SSL 证书的商密 ACME 客户端软件，实现了同时申请和部署双算法 SSL 证书的自动化证书管理。

(5) **零信国密 HTTPS 加密自动化网关**：全球首个通过商密产品认证的支持自动化证书管理、自动配置双算法 SSL 证书、自动化实现 HTTPS 加密卸载转发的硬件网关产品，使得原 Web 服务器零改造就可以自动化实现商密 HTTPS 加密，自适应支持 RSA 算法 HTTPS 加密。

(6) **零信国密 HTTPS 加密自动化云服务**：这是一个把通过商密产品认证的国密 HTTPS 加密自动化网关部署在云上为用户提供自动化证书管理、自动配置双算法 SSL 证书、自动化实现 HTTPS 加密卸载转发的创新云服务，使得用户无需本地部署硬件网关也可以实现原 Web 服务器零改造的自动化实现商密 HTTPS 加密，一样自适应支持 RSA 算法 HTTPS 加密。

零信技术不仅打造了商密 SSL 证书应用生态的全系列产品，而且在今年 12 月份成功获批牵头制定相关的两个商用密码行业标准-《**证书透明规范**》和《**自动化证书管理规范**》，这是对标和兼容 RFC6962 和 RFC8555 的两个国际标准的商密标准，支持采用商用密码实现证书透明

和实现商密证书自动化。这两个标准的制定标志着商密 SSL 证书的商用密码产品标准化水平又上了一个新台阶，将为保障商密 SSL 证书的可靠供给和普及应用提供标准支撑，必将加速商密 SSL 证书的普及应用，加速采用商用密码来保障全球互联网安全。

四、 展望 2024，继续砥砺奋进，提供更多更好的商密产品和解决方案

回首 2023 年，零信技术为全球互联网核心通信安全-HTTPS 加密贡献了中国方案。2024 年，我们将继续不断迭代和完善商密 SSL 证书应用的全生态产品，拓展生态合作伙伴，启动上密行动计划，继续为普及商密应用做贡献，继续为全球用户提供更多的密码应用产品。

零信技术在完善商密 HTTPS 加密应用生态产品的同时，研发和提供商密文档安全产品和服务、商密邮件安全产品和服务、商密代码安全产品和服务、以及商密身份可信产品和服务，不断完善商用密码体系的各种数字证书的应用，为全球用户提供另一个选择和另一个可靠的选项，推广和普及商密密码来保障全球互联网和万物互联的安全可信。

王高华

2023 年 12 月 29 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。
从 2021 年 12 月 9 日开始，已累计发表 206 篇，共 38 万多字中文和 7 万多英文单词。