

国密 HTTPS 网关，国密改造新物种，深圳智造

从 [1月6日](#) 笔者在 CEO 博客公开披露这个产品，到上周五官网上线了详细的[产品手册](#)，并确定了这个产品的 5 个型号和对应的性能指标，同时开始申请商用密码产品认证，这表明一个专用于 https 加密的国密改造新物种正式诞生。本文就讲一讲这个产品为何称之为国密改造新物种，到底同目前全球密码产品市场(包括我国国密产品市场)上的类似产品有什么不同。

国密改造的下一个重点和难点是 https 加密的国密改造，这个已经上升到了非常紧急的程度，因为一年前发生俄乌冲突时俄罗斯政府和银行网站 https 加密用的 RSA 算法 SSL 证书被恶意吊销的事件已经让我国业界上上下下都充分认识到了必须尽快普及国密 SSL 证书来实现 https 加密，用国密 SSL 证书来保障我国政府网站和网银系统的安全。但是，短时间内完成国密 https 加密改造几乎是无法实现的难题，因为目前的互联网安全体系是基于 RSA 密码体系打造的，用户常用的浏览器和 APP 不支持国密算法、常用的 Web 服务器不支持国密算法、传统 CA 系统不支持签发国密 SSL 证书，常用的 CDN/云 WAF 服务和 WAF 设备不支持国密算法。并且，现有业务系统复杂，对于正在运行的业务系统，改造风险极高，不能影响现有政务系统和网银系统的正常可靠运行。

笔者一直在寻找一个解决方案来解决这个难题，上周五正式定型的国密 HTTPS 网关就是笔者找到的最佳的唯一可行的解决方案。这可不是一个传统意义的安全网关产品，是一个新物种，是一个端云一体的 https 加密服务提供者(CSP, Cryptography Service Provider)，一个无需用户采购网关设备后又要向 CA 申请 SSL 证书再费力配置到网关中去实现 https 加密的创新产品，一个即插即用的最多可以为 255 个网站自动化提供全球信任和国密合规的 https 加密服务的创新产品，一个真正用户所需的零改造现有 Web 服务器实现国密 https 加密的创新产品。



我先给大家说几个产品参数就能体会到这个产品因为创新而为用户带来了超高附加值。零信国密 HTTPS 网关的专业万兆版 MG-1-8 支持为最多 255 个网站域名自动化配置双 SSL 证书，并且是 5 年内免费自动化配置，开机设置好网站域名即刻自动配置一张全球信任的 ECC DV SSL 证书、一张国密 OV SSL 证书(包括签名证书和加密证书)，还有网站可信 EV 认证服

务。大家可参考一下[证签官网](#)这个配置的双 SSL 证书 5 年的价格为 19888 元，再看看零信网站可信 EV 认证的 5 年的价格为 1940 元，两项加起来就是 21828 元，再乘以 255 张，就是 **5,566,140** 元!您没有看错，仅双 SSL 证书和网站可信认证一项就价值 **556** 万元之多!也许有人说你这个参考价格是你自己定的，不是市场上的最低价。也正是考虑这一点，我们在官网上写的价值是 **113** 万元，这是按照双 SSL 证书费用为 888 元来计算的(仅为官网价格的 4%)。请注意，这里说的是网关免费自动配置的双 SSL 证书值多少钱，并不是网关的销售价格。可能又会有人讲，那你不是亏大了吗?为了很好的回答这个问题，我打一个形象的比喻吧：一辆汽车在早期手工制作，需要一百万元，但是机械化大规模生产后就只卖十万元了，这就是自动化生产流程创新带给用户的实惠!零信国密 HTTPS 网关就是这样的创新产品，网关是一个“端”，与零信云 SSL 系统的“云”实现“端云一体”后就创造了一个新物种，一个能自动化为 255 个网站提供双算法自适应 https 加密的创新产品，一个可以用于快速普及国密 https 加密应用的创新产品，由于实现了自动化，就大大降低了人工成本，这个降低的人工成本就可以把昂贵的 SSL 证书实惠地让利给最终用户了。

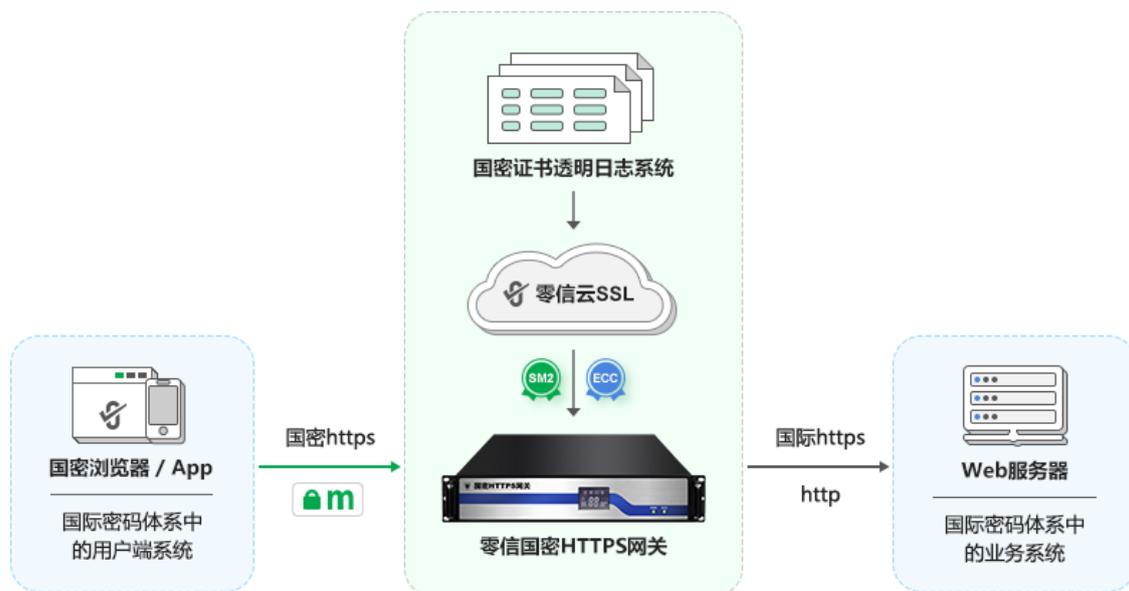
笔者再给大家讲一讲官网的产品介绍中的另一个指标参数：“节省人力成本”，5 年合计 **150 万元**，这又是怎么计算出来的呢?笔者在博文[《对策研究 | 谷歌要革全球 CA 的命,怎么办?》](#)中讲到谷歌正在推动把 SSL 证书有效期从目前的一年缩短到 90 天，这是什么概念，原先是一年申请一次证书，拿到证书后再在服务器上安装一次，这已经很费人力了，现在要变成每 3 个月需要整一次，一年要整 4 次，就是说人工成本要上升 4 倍!笔者了解到某个银行的网银网站申请 SSL 证书时需要包括经理在内的 5 个人去机房做 CSR 文件(进机房一次)，拿到证书后又要 5 人到场再进机房一次，原先是一年这样进出两次，将来每 3 个月就要进出两次!而部署了零信国密 HTTPS 网关后只需在部署网关时进出一次机房即可，5 年内不再需要为申请 SSL 证书烦恼，并且是最多支持 255 个网站的 SSL 证书自动化部署。255 个网站的证书管理至少可以折合为 2 个全职的助理工程师的人力成本，按一个助理工程师每月 12500 元计算，5 年就是 150 万元!如果加上申请证书涉及到 N 个工作人员的话(不仅需要工程师申请和安装，还需要采购、财务请款老总批款等)，就远大于 150 万元了。也就是说，零信国密 HTTPS 网关的自动化为最多 255 个网站配置双 SSL 证书为最终用户节省了 **150 万元**以上的人力成本。

著名经济学家熊彼特认为：企业家的创新不是发明新技术，更多的是把新技术转化为商业成果，创新主要是在应用层，通过把新技术、新方式把原有的一些生产要素重新组合，以此来提高效率，这就是商业创新。只有创新才能创造价值，一个把传统网关产品和传统 CA 产品两个生产要素重新组合的创新——国密 HTTPS 网关给用户带来的是超过 263 万元以上的直接经济收益，这还没有计算由于忘了证书续费而给公司业务带来的巨大损失，HTTPS 网关 5 年 24 小时

365 天不间断的 https 加密服务彻底杜绝了证书忘了续费的可能，不管现在和将来的证书有效期为多少天，都会全自动在证书到期前完成证书续期并自动配置启用！

笔者再讲一个 SSL 证书忘了续费的真实案例：2018 年 12 月的某一天，由于爱立信电信设备中的 SSL 证书过期而导致了移动运营商 O2 的移动数据管理系统崩溃，这使得其 3200 万手机用户以及全球其他运营商的用户都无法正常使用 O2 移动通信服务，业务被中断了二十多个小时才恢复。为此，运营商 O2 向爱立信索赔数百万美元。现在，有了零信国密 HTTPS 网关就不会发生这样的事情！也不用担心谷歌会把 SSL 证书有效期缩短到 90 天或者 9 天！

笔者作为这个创新解决方案的总设计师想对用户讲的是：零信国密 HTTPS 网关不是一个简单的硬件网关产品，是一个超值的创新的 https 加密国密改造新物种，一个深圳智造的创新产品和解决方案，我们非常荣幸能给我互联网基础通信安全 https 加密国密改造带来这样一个端云一体的创新产品，一个能彻底解决某个大国可能利用 RSA 算法 SSL 证书作为制裁工具的掐脖子问题的创新方案，一个能为最终用户带来超额价值的创新产品，一个把无法改造的基于 RSA 体系的系统变成无需改造的创新解决方案。



这个新物种是一个国密 https 加密改造创新解决方案，不仅有看得见的硬件网关产品，而且还有看不见的云端系统—零信云 SSL 系统、国密 ACME 服务系统、国密证书透明日志系统等，还有免费配置的国密浏览器—零信浏览器，并且还免费提供安卓和 iOS 版本 APP 国密改造的 SDK，用于改造安卓和 iOS APP 支持国密 https 加密。最重要的是，还有 5 年服务期的最多为 255 个网站域名不断签发的双 SSL 证书，确保了此创新物种能为用户提供不间断的 24 小时 x 365 天 x 5 年的国密 https 加密服务和国际 https 加密服务。

王高华

2023年3月20日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。

