

HTTPS 加密不仅是等保和密保的强制项和加分项

商密改造难，但是为了满足等保和密保(密评)的强制要求，又不得不改造。那么，该怎么改造？是否有不难的改造方案？公网商密改造和内网商密改造有什么不同？是否有既省钱又省事的改造方案？本文详细回答这些问题。

一、 为何需要强制实现等保合规和密保合规？

要回答这个问题讲一堆大道理大家一定听不进去，网上搜索这个问题，会有一大堆让人看得晕头转向的答案，估计没有几个读者朋友愿意全部看完的，但愿读者朋友能看完笔者给出的不一样的答案。

大道理的“废话”笔者就不讲了，请读者朋友看一下下面的“喝酒不开车，开车不喝酒”的宣传画，这个问题的答案同开车不喝酒的答案是一样的，为何开车不能喝酒，不是交警想多管闲事，是为了你自己的生命安全，因为还有老婆孩子在家等你安全回家！



同理，为何要强制实现等保合规和密保合规？不是相关政府主管部门要多管闲事，而是为了你单位的业务系统能安全可靠地运行，因为你单位运行的是关系到老百姓日常幸福生活的关键信息基础设施！如果不采取这些合规措施，很难保障业务系统安全，一旦业务系统出现安全问题，不仅会伤害老百姓的切身利益，而且运营单位也要遭遇最大损失，甚至很可能是不可挽回的致命损失。所以，这些合规措施是为了保障重要业务系统的可持续安全运行，其投资是收益而不是成本！

合规 COMPLIANCE

为了业务系统的持续可靠运行，而不仅仅是为了合规



二、 是否有省钱和省事的 HTTPS 加密合规解决方案？

答案是：有！本文就专门讲这个既省钱又省事的 HTTPS 加密商密改造方案，分别讲内网 Web 系统改造方案和公网 Web 系统改造方案。HTTPS 加密是等保和密保的最重要的合规要求，不仅仅是加分项，而且是保障业务系统可靠运行和保障数据安全的最关键的技术手段。

1. 内网 Web 系统改造，省钱

对于内网系统，零信技术推出了证签品牌内网 SSL 证书这个新产品，用户只需选购和部署支持内网 IP 地址和主机名的内网 SSL 证书，并选用信任这张内网 SSL 证书的、完全免费的商密浏览器—零信浏览器，就可以满足内网系统的 HTTPS 加密等保合规和密保合规要求。不仅能满足用户在“通信传输”、“数据完整性”、“数据保密性”等三个方面的等保合规要求，同时还能满足用户在“网络与通信安全”-采用密码技术保证通信过程中数据的完整性、机密性和实体身份的真实性、“应用和数据安全”-采用密码技术保障信息系统应用的重要数据在传输、存储过程中的机密性和完整性等两个方面的密保合规要求。

等保要求	密保要求	应用架构	是否合规
通信传输 数据完整性 数据保密性	网络与通信安全 应用和数据安全	<p>内网用户</p> <p>http</p> <p>内网服务器</p> <p>未部署 SSL 证书</p>	等保 X 密评 X 关保 X

<p>通信传输 数据完整性 数据保密性</p>	<p>网络与通信安全 应用和数据安全</p>	<p>部署内网 SSL 证书(SM2/RSA), 自适应加密算法 HTTPS 加密</p>	<p>等保 √ 密评 √ 关保 √</p>
---------------------------------	----------------------------	---	-------------------------------

证签内网 SSL 证书全球率先支持内网 IP 地址和内部主机名，彻底解决了公网 SSL 证书不支持内网 IP 地址的难题，并且此内网 SSL 证书支持 5 年有效期，使得用户只需一次安装 SSL 证书，5 年尽享不间断的保障内网 Web 流量安全的 HTTPS 加密服务。不仅满足合规要求，更重要的是解决了内网机密信息安全，彻底解决了内网机密信息明文传输可能造成的泄密问题，有力保障内网业务系统的机密信息安全。

这是一个非常省钱的方案，一张 5 年期的内网 DV SSL 证书仅需 400 元，平均一年才 80 元。同时，也是一个相对省事的方案，因为只需一次安装证书就能管 5 年，5 年内不再需要申请和安装证书了。如果合规要求必须部署商密 SSL 证书，则也只需升级一次 Web 服务器软件支持商密算法和部署一次商密 SSL 证书。




2. 公网 Web 系统改造，省事

对于公网系统，仅仅选购和部署公网 SSL 证书是不够的，因为公网 Web 服务是公众服务，对服务质量有更高的要求，尽量不要动现有的 Web 服务器，国际标准和商密标准对公用 SSL 证书的要求也更高，证书有效期也有严格的要求，现在是一年有效期，谷歌正在推动缩短到 90 天。公网 HTTPS 加密需要零改造现有 Web 服务器实现，并且是全球信任和商密合规的 HTTPS 加密。

满足这些苛刻条件的解决方案只有两个：一是在现有 Web 服务器前面部署零信国密 HTTPS 加密自动化网关，原 Web 服务器零改造变成源 Web 服务器，由网关自动化对接零信云 SSL 服务系统自动化申请和配置商密 SSL 证书和国际 SSL 证书，实现自适应加密算法的 HTTPS 加密、卸载和转发。二是无需部署硬件网关，只需做域名解析就可启用国密 HTTPS 加密自动化云服务，由云服务对接零信云 SSL 服务系统自动化申请和配置商密 SSL 证书和国际 SSL 证书，实现自适应加密算法的 HTTPS 加密、卸载和转发。

零信技术公网 Web 服务器自动化 HTTPS 加密解决方案，让用户无需向 CA 申请 SSL 证书，无需安装和部署 SSL 证书，无需商密改造现有 Web 服务器，无需考虑国际标准将来把 SSL

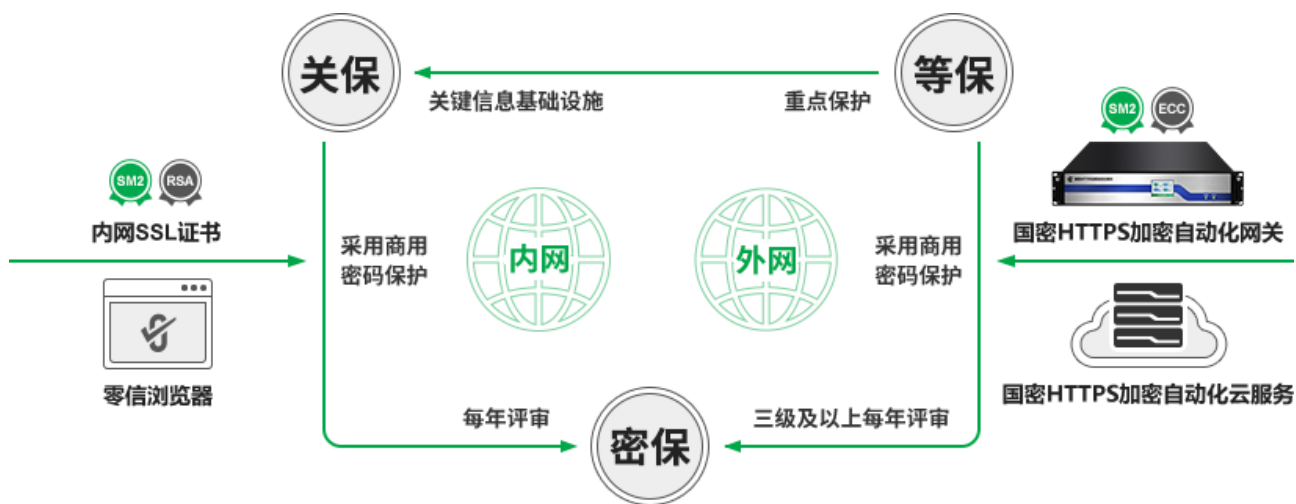
证书有效期缩短到 90 天或者更短，全自动配置符合国际标准和商密标准的双 SSL 证书，全自动实现 HTTPS 加密，满足用户等保合规和密保合规要求。不仅能满足用户在“通信传输”、“数据完整性”、“数据保密性”等三个方面的等保合规要求，同时还能满足用户在“网络与通信安全”-采用密码技术保证通信过程中数据的完整性、机密性和实体身份的真实性、“应用和数据安全”-采用密码技术保障信息系统应用的重要数据在传输、存储过程中的机密性和完整性等两个方面的密保合规要求。

等保要求	密保要求	应用架构	是否合规
通信传输 数据完整性 数据保密性	网络与通信安全 应用和数据安全	 <p>互联网用户</p> <p>Web服务器</p> <p>未部署 SSL 证书</p>	等保 X 密评 X 关保 X
通信传输 数据完整性 数据保密性	网络与通信安全 应用和数据安全	 <p>浏览器 / App</p> <p>国密HTTPS加密自动化网关</p> <p>Web服务器</p> <p>部署国密 HTTPS 加密自动化网关，自动化实现 HTTPS 加密</p>	等保 √ 密评 √ 关保 √
通信传输 数据完整性 数据保密性	网络与通信安全 应用和数据安全	 <p>浏览器 / App</p> <p>零信国密HTTPS加密自动化云服务</p> <p>源站</p> <p>启用国密 HTTPS 加密自动化云服务，自动化实现 HTTPS 加密</p>	等保 √ 密评 √ 关保 √

三、内网、外网、公网，等保、关保、密保，都需要 HTTPS 加密

等保和密评共同组成《网络安全法》中要求的“网络安全等级保护制度”，关键信息基础设施是等级保护的重点防护对象，等保是关保的基础。商用密码应用安全是保障网络和信息系统安全的一项重要保护措施，也是保障关键信息基础设施安全的重要技术手段，关键信息基础设施必须按照密评相关标准、规定实现密保合规。

无论是内网、外网、公网都有等保、关保、密保合规要求，都涉及到的 HTTPS 加密改造难题。零信技术提供的内网 HTTPS 加密解决方案简单易用，实施成本非常低；而公网 HTTPS 加密解决方案则是非常省事，完全自动化实现。



零信技术提供完整的内网和公网 HTTPS 加密解决方案，不仅能有效地解决了内网和公网 Web 流量安全隐患，提升内外网信息系统的整体信息安全防护能力，而且能满足用户的等保、关保和密保合规要求，从而有力保障各种内外网重要信息系统的可靠持续安全运行。

有诗为证：

喝酒不开车，开车不喝酒，安全幸福。
 无密码不系统，建系统必密码，安全合规。
 内网安全，用内网证书和零信浏览器，简单。
 公网安全，用零信网关或零信云服务，省事。

王高华

2024 年 4 月 25 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 161 篇(共 43 万 1 千多字)和英文 65 篇(7 万 9 千多单词)。

