



广西商用密码协会

密码铸盾八桂行—崇左站 密码科普讲座

解读《关键信息基础设施商用密码使用管理规定》

密码专家 王高华

2025.07.21



国家密码管理局

WWW.SCA.GOV.CN

关键信息基础设施商用密码使用管理规定 (国家密码管理局、国家互联网信息办公室、公安部 令第5号)

《关键信息基础设施商用密码使用管理规定》已经2025年4月21日国家密码管理局局务会议审议通过，并经国家互联网信息办公室、公安部同意，现予公布，自2025年8月1日起施行。

国家密码管理局局长 刘东方

国家互联网信息办公室主任 庄荣文

公安部部长 王小洪

2025年6月11日

解读《关键信息基础设施商用密码使用管理规定》

- **《规定》依据哪些法律法规制定？**
- **《规定》涉及到哪些单位？**
- **《规定》主要内容和核心内容有哪些？**
- **《规定》违反如何处罚？**
- **目前现状是什么样的？存在哪些严重违反的问题？**
- **如何落实《规定》要求？**
- **《规定》是保护关键信息基础设施安全的重要举措**
- **彩蛋：一次技术改造完成两次HTTPS加密技术革命**

《规定》依据哪些法律法规制定？

第一条 为规范关键信息基础设施商用密码使用，保护关键信息基础设施安全，根据《中华人民共和国密码法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《商用密码管理条例》和《关键信息基础设施安全保护条例》、《网络数据安全条例》等有关法律、行政法规，制定本规定。

第二条 本法所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

第八条 商用密码用于保护不属于国家秘密的信息。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

4部国家大法， 3个国务院令

《规定》涉及到哪些单位？

第二条 依据《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》等法律、行政法规和国家有关规定认定的关键信息基础设施的商用密码使用管理，适用本规定。

《关键信息基础设施安全保护条例》

第二条 本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

解读：所有政府官网、政务服务系统、公共服务系统、网银系统、支付系统(包括微信支付和支付宝)、主流电商系统等运营单位都是本《规定》涵盖范围，也可以理解为这是要求全国所有公共服务系统都必须使用商用密码来保护其系统数据安全，范围之广，责任之大，所以大家都称之为重磅规定。

《规定》主要内容有哪些？

共25条。主要包括：

- (一) 总体要求：**规定适用范围、明确管理部门职责、明确保护工作部门职责
- (二) 运营者责任：**明确运营者总体责任；规定制度、人员、经费保障责任
- (三) 商用密码使用具体要求：**明确商用密码技术、产品、服务使用要求；明确数据安全保护、个人信息保护要求；细化规划、建设、运行等阶段商用密码使用要求
- (四) 监督检查及法律责任：**规定商用密码运行安全管理责任、规定密码管理部门和保护工作部门的监督检查职权、规定运营者的违法情形及法律责任、规定监督管理人员的违法情形及法律责任

《规定》核心内容有哪些？

- **第五条**明确运营者总体责任。落实关键信息基础设施商用密码使用“**三同步一评估**”原则，同步规划、同步建设、同步运行商用密码保障系统，并定期开展商用密码应用安全性评估。
- **第九条**明确商用密码技术、产品、服务使用要求。规定关键信息基础设施使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。
- **第十条**明确数据安全保护、个人信息保护要求。强调关键信息基础设施应当使用商用密码对其存储、**使用**、**传输**的核心数据、重要数据和个人信息进行保护。

《规定》违反如何处罚？

- 具体规定见 第十九条、第二十条、第二十一条、第二十二条、第二十三条
- 《规定》共25条，其中处罚有5条！
- 最高处罚：单位处10万元以上**100万元**以下罚款，对直接负责的**主管人员**处1万元以上**10万元**以下罚款：

互联网政务应用安全管理规定

(2024年2月19日中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工业和信息化部、公安部制定 2024年5月15日发布)

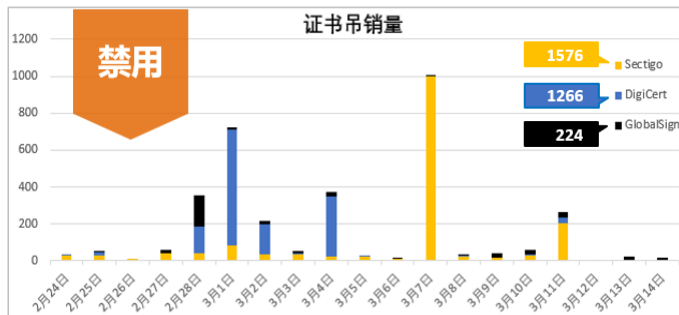
第四十一条 对违反或者未能正确履行本规定相关要求的，按照《党委（党组）网络安全工作责任制实施办法》等文件，依规依纪追究当事人和有关领导的责任。

与《规定》相关的最近发布的重要文件有哪些？

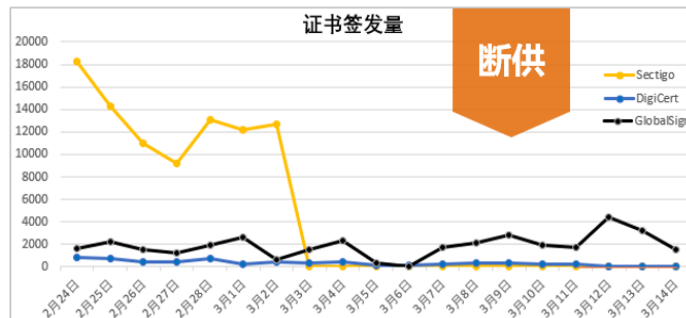
- **2024年5月22日**，网信办官网发布了由网信办、中央编办、工信部和公安部联合发布的[《互联网政务应用安全管理规定》](#)，**2024年7月1日**起施行。此规定明确要求政府官网和政务服务网站系统都必须实现商用密码算法HTTPS加密安全连接，包括列入[关键信息基础设施](#)的网站系统。
- **2024年7月19日**，国家密码管理局发布了[《商用密码随机抽查事项清单（2024年版）》](#)，**发布之日起**施行。这是要执法检查商用密码应用情况，采用抽查的方案巧妙地解决了执法人力不足的难题，不仅能体现被检查对象的公平性，而且能达到法律具备足够威慑力的效果。
- **2025年5月28日**，国务院发布[《政务数据共享条例》](#)，**2025年8月1日**起施行。要求政府部门应当采取技术措施(商用密码)和其他必要措施，防止政务数据被篡改、破坏、泄露或者非法获取、非法利用。
- **2025年6月27日**，国家密码管理局发布[《关键信息基础设施商用密码使用管理规定》](#) (简称《规定》)，**2025年8月1日**起施行。

一年内相关多个权威部门连发4个文件，说明了什么？

- 说明这事很重要，很紧急！问题很多，很严重！
- 不断加码要求全面普及应用**商用密码**来保障我国关键信息基础设施安全！
- 因为已经发生了使用RSA算法**SSL证书**被禁用和断供的前车之鉴！



俄乌冲突发生后20天内
三千多张RSA证书被
非法吊销、10天后被断
供、政府和银行网站系
统无法访问！



目前现状是什么样的？存在哪些严重问题？

⚠ 不安全 | www.chongzuo.gov.cn

chongzuo.gov.cn

×

⚠ 您与此网站之间建立的连接不安全
请勿在此网站上输入任何敏感信息（例如密码
或信用卡信息），因为攻击者可能会盗取这些
信息。 [了解详情](#)



⚠ 不安全 | gxj.chongzuo.gov.cn

广西崇左市 工业和信息化局

⚠ 不安全 | gaj.chongzuo.gov.cn



⚠ 不安全 | www.czsjszq.gov.cn



⚠ 不安全 | www.pxszf.gov.cn



⚠ 不安全 | rsj.chongzuo.gov.cn



⚠ 不安全 | mzj.chongzuo.gov.cn



⚠ 不安全 | www.fusui.gov.cn



⚠ 不安全 | www.czsrmmy.com



崇左市人民政府/各局委办/各区县官网/医院等都没有启用商密HTTPS加密，**不安全！不合规！**

目前现状是什么样的？存在哪些严重问题？

- 国务院84个部门79个有独立官网，其中实现了HTTPS加密的有62个，占比78%，有17个部门官网没有启用HTTPS加密，占比22%。这些启用HTTPS加密的网站中只有1个**公安部**启用了商用密码HTTPS加密，占比仅1.26%，也就是说，除了公安部官网外其他部委官网都是不符合《规定》的——没有采用商用密码算法实现HTTPS加密保护。
- 31个省市自治区政府官网中，只有18个省市自治区启用了HTTPS加密，占比58%。只有4个省（**湖南、海南、江西、陕西**）政府官网实现了商用密码HTTPS加密保护，占比仅12.90%。

⚠ 不安全 | www.gxzf.gov.cn

广西壮族自治区人民政府

🔒 T4 [CN] 中国广西壮族自治区人民政府 | https://tyrz.zwfw.gxzf.gov.cn/am/



广西壮族自治区人民政府

Gvangsih Bouxcuengh Swcigih Yinzminz Cwngfuj

全国一体化在线政务服务平台

广西数字政务一体化平台

🔒 m T4 [CN] 中国公安部 | https://www.mps.gov.cn

m 商密合规, 密保合规

该连接使用 SMSSL (SM2)

该连接是使用 SM4 进行加密的, 同时使用 SM3 进行消息认证并使用 SM2 作为密钥交换机制。

[了解详情](#)

🔒 m T4 [CN] 中国公安部 | https://www.mps.gov.cn

云WAF防护, 等保合规

由 创宇盾云WAF 提供

[了解详情](#)

🔒 m T4 [CN] 中国湖南省人民政府 | https://www.hunan.gov.cn

m 商密合规, 密保合规

该连接使用 SMSSL (SM2)

该连接是使用 SM4 进行加密的, 同时使用 SM3 进行消息认证并使用 SM2 作为密钥交换机制。

[了解详情](#)

不是关键信息基础设施单位不作为，而是密改方案有问题！

- 为何存在这么多严重问题？为何大家都喊国密改造难？因为密改方案就是错的！

1. 名称：IPsec/SSL VPN综合安全网关	错		
2. 功能参数：1、产品具备国家密码管理局商用密码产品认证证书；			
2、支持256位SM2公钥密码算法，支持2048位和4096位私钥密码算法，支持SM4和AES等对称密码算法，支持SM3、SHA256摘要算法；			
3、支持创建SSL VPN服务并支持单双向SSL配置，同时支持国密和国际证书策略，并支持国密与国际SSL算法套件及协议；			
4、具备SM9算法SSL连接建立功能，在50并发用户数时，SM9算法SSL平均吞吐量不低于800Mbps；			

SSL VPN网关是远程接入内网的设备，这是要让互联网用户接入政府内网？

1. 名称：国际算法SSL证书（第三方合规机构颁发）	错		张	11
2. 功能参数：1、基于国际算法为网站提供身份鉴定并保证该网站拥有高强度加密安全；				
4、可安装部署在服务器或网关，实现数据传输加密。				
1. 名称：国密算法SSL证书（第三方合规机构颁发）	错		张	11
2. 功能参数：1、基于国密算法为网站提供身份鉴定并保证该网站拥有高强度加密安全；				

只采购11张证书，一个地级市只有11个网站系统？

1. 名称：国密浏览器	错		套	200
2. 功能参数：1、产品具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书；				
2、支持基于 SM2 算法的数字证书、数字证书撤销列表（CRL）；				
3、同时支持 SSL 单向及双向链接；				
4、支持基于 RSA 算法的数字证书、数字证书撤销列表（CRL）；				
5、双算法支持，同时支持国密算法和国际通用算法；				

只采购200套国密浏览器，一个地级市只有200个政府工作人员？

某政府单位密改招标文件

不是关键信息基础设施单位不作为，而是密改方案有问题！

- 为什么会错的这么离谱？
 - 为什么给用户的方案是十年前的老三样！为何不能与时俱进？
 - 这是所有密改从业者和用户都应该反思的！
-
- 《规定》要求落实“三同步一评估”原则，同步规划、同步建设、同步运行商用密码保障系统，定期评估！第一步产品规划就是错的！
 - 《规定》要求不断改进商用密码应用技术措施，SSL证书国际标准和国密标准都变了，变成47天有效期了，密改方案还在给用户手动申请和部署证书，这是用户需要的密改方案吗？这是在坑用户，在浪费钱！

不是关键信息基础设施单位不作为，而是密改方案有问题！

- 正确的、与时俱进的密改方案是什么？正确的产品选型是什么？

某政府单位密改招标文件

1. 名称：IPsec/SSL VPN综合安全网关
2. 功能参数：1、产品具备国家密码管理局商用密码认证，支持256位SM2公钥密码算法，支持2048位和1024位SM3、SHA256摘要算法；
- 3、支持创建SSL VPN服务并支持单双向SSL配置，同时支持文件及协议；
- 4、具备SM9算法SSL连接建立功能，在50并发用户数时，：

错

SSL VPN网关是远程接入内网的设备，这是要让互联网用户接入政府内网？

1. 名称：国际算法SSL证书（第三方合规机构颁发）
2. 功能参数：1、基于国际算法为网站提供身份认证；
- 4、可安装部署在服务器或网关，实现数据传输加密；

错

只采购11张证书，一个地级市只有11个网站系统？

1. 名称：国密算法SSL证书（第三方合规机构颁发）
2. 功能参数：1、基于国密算法为网站提供身份认证

错

只采购200套国密浏览器，一个地级市只有200个政府工作人员？

1. 名称：国密浏览器
2. 功能参数：1、产品具备国家密码管理局商用密码认证；
- 2、支持基于 SM2 算法的数字证书、数字证书撤销列表；
- 3、同时支持 SSL 单向及双向链接；
- 4、支持基于 RSA 算法的数字证书、数字证书撤销列表；
- 5、双算法支持，同时支持国密算法和国际通用算法

对

应该采购国密HTTPS加密自动化网关

对

采购的网关应该免费包5年双算法SSL证书，并且是自动化配置，支持255个网站

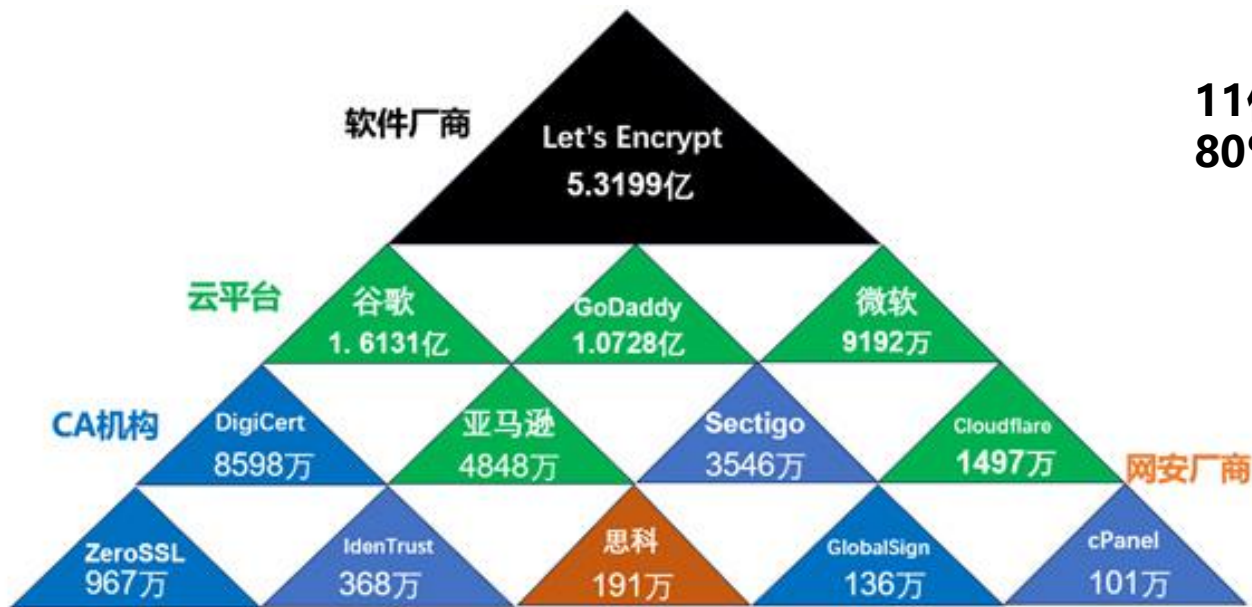
对

市场上已有完全免费干净无广告的满足使用要求的国密浏览器，用户无需花钱采购

什么样的密改方案才是真正能保障关基系统安全的方案？

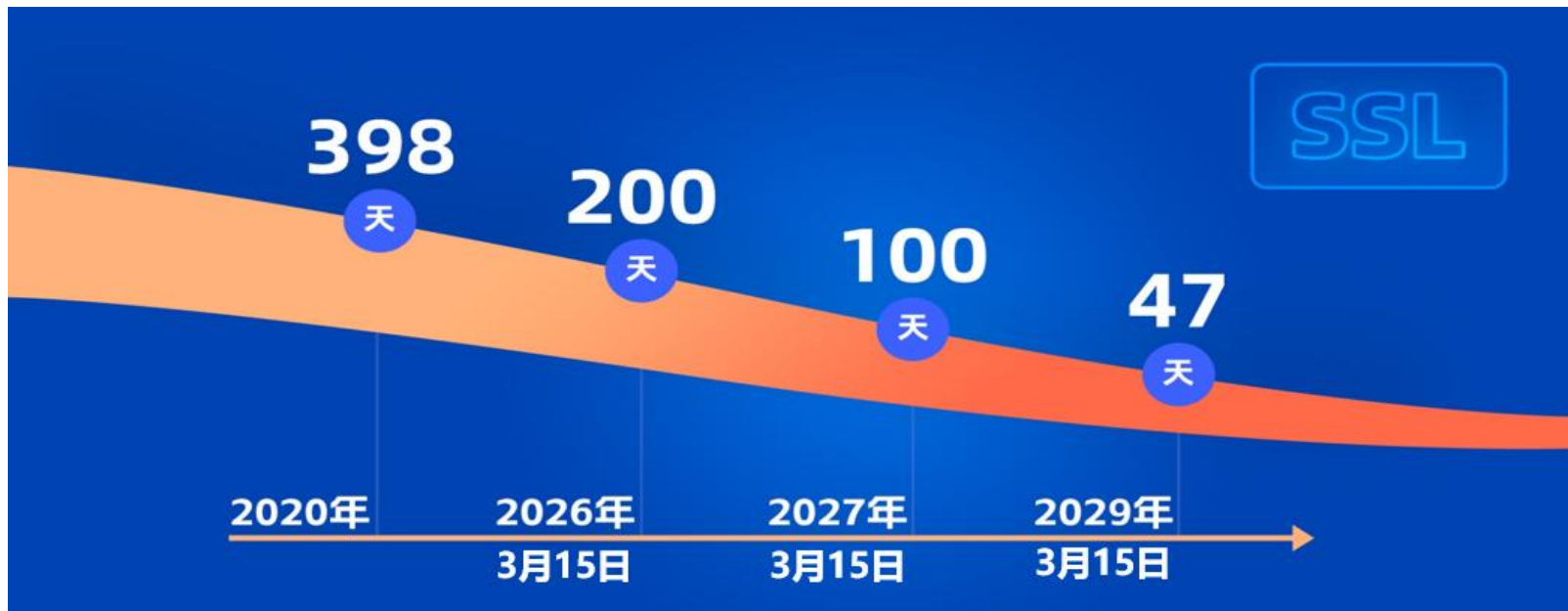
- 系统架构微改造、业务零中断、原Web服务器零改造
- 应该配置 国密HTTPS加密自动化网关，而不是远程接入用的SSL VPN网关
- 网关必须支持自动化配置国密SSL证书和国际SSL证书，自动化实现自适应密码算法的HTTPS加密，自动化实现WAF防护，而不是采购SSL证书和人工安装部署证书，采购的网关必须含双证书，无需另外采购！
- 自从有了互联网，浏览器都是免费的，为何国密改造就要用收费浏览器？这不是趁火打劫？市场上已经有了完全免费的、干净无广告的、满足使用要求的国密浏览器，为何不用而要去采购收费的国密浏览器？

SSL证书自动化管理技术迅速得到了全球普及应用



11亿多张有效SSL证书
80%证书实现了自动化

SSL证书第一次技术革命—证书自动化管理 即将到来



SSL证书从人工管理到自动化管理的技术革命



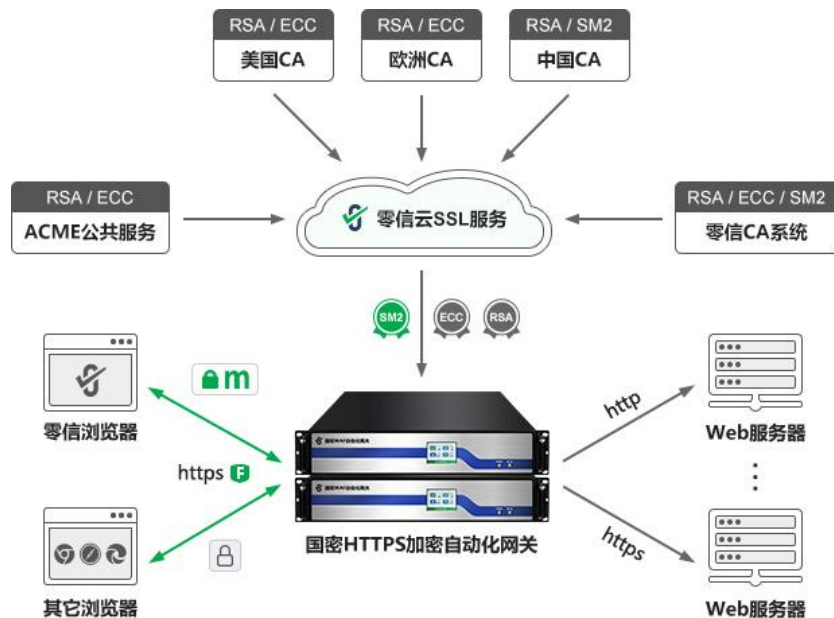
SSL证书有效期将缩短为47天

SSL证书国际标准新政来了，有效期将逐渐缩短为47天，这值得我国业界和用户高度重视，提前做好准备。根据自己的应用系统情况选对技术方案，必须选择原Web服务器零改造的自动化方案。

- 这次的技术革命到来时间是**明年3月15日**，其目的是要实现SSL证书自动化管理，从传统的人工管理革命为自动化管理。
- 这就要求SSL证书用户采取合适的技术措施完成系统升级改造，实现SSL证书自动化管理。
- 我国则需要实现双算法(RSA/SM2)SSL证书的自动化管理，同时完成系统国密改造以支持SM2国密算法，实现自适应密码算法的HTTPS加密自动化。

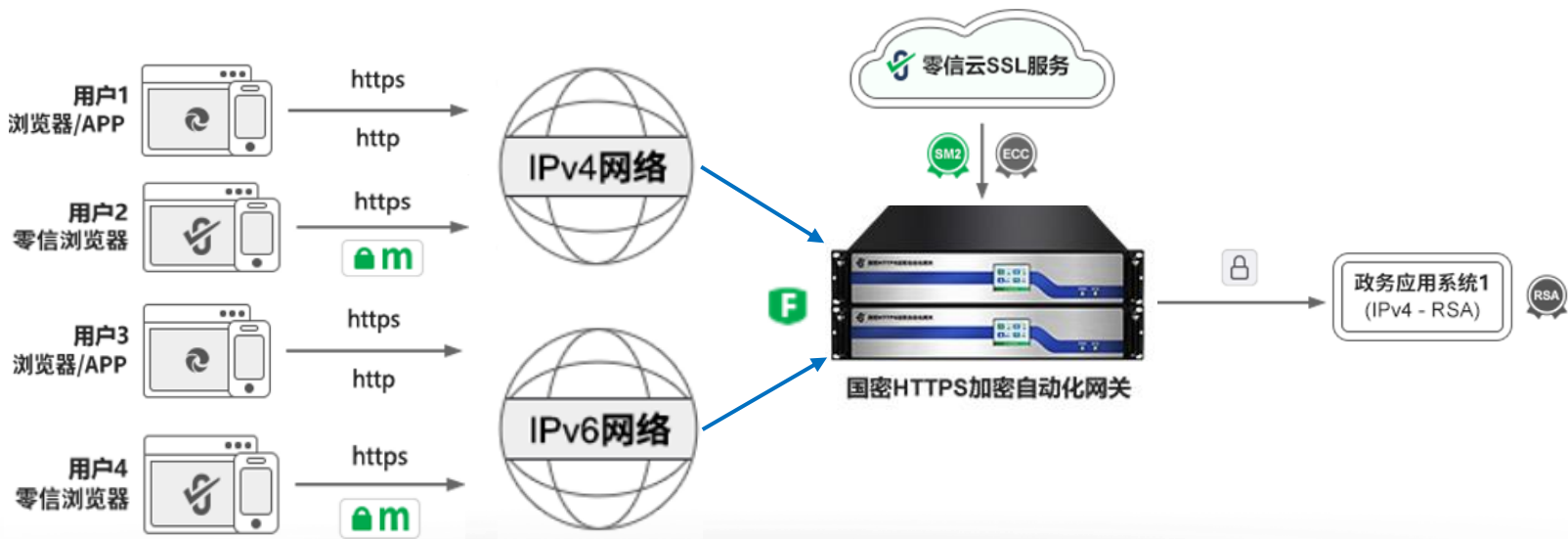
如何落实《规定》要求？微改造、自动化、零中断

- 零信技术独家创新方案满足3要求
- 只需在原Web服务器前部署零信国密HTTPS加密自动化网关即可
- 网关自动化对接零信云SSL服务系统，为最多255个网站自动化配置双算法SSL证书，自动化实现国密HTTPS加密和WAF防护
- 零信云SSL服务系统自动对接多家国际CA和国密CA，自动切换证书签发通道，确保双算法证书的自动化签发万无一失。
- 免费配套国密浏览器—零信浏览器

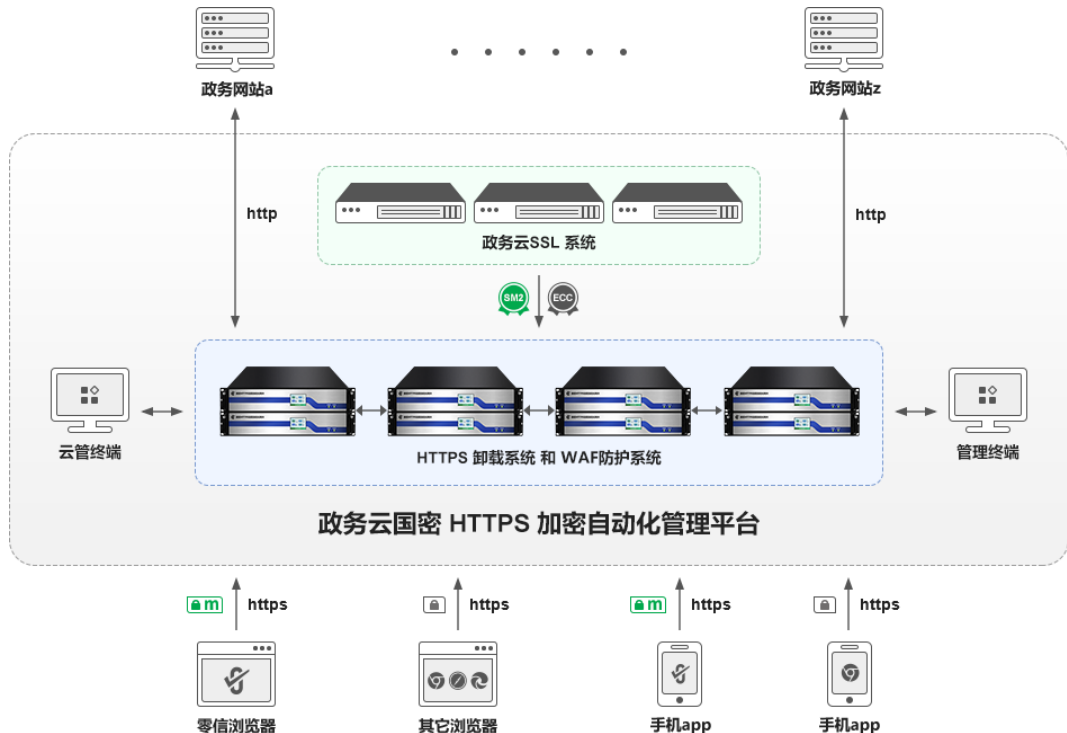


微改造，一个网关搞定商密改造/IPv6改造/WAF防护

- 微改造方案是用户只建一套系统，部署一个网关，就能满足RSA/SM2和IPv4/IPv6的HTTPS加密和WAF防护需求，端云一体
- 更合理，更省事，节省投资，大大提升了系统可靠性，降低了系统管理难度！

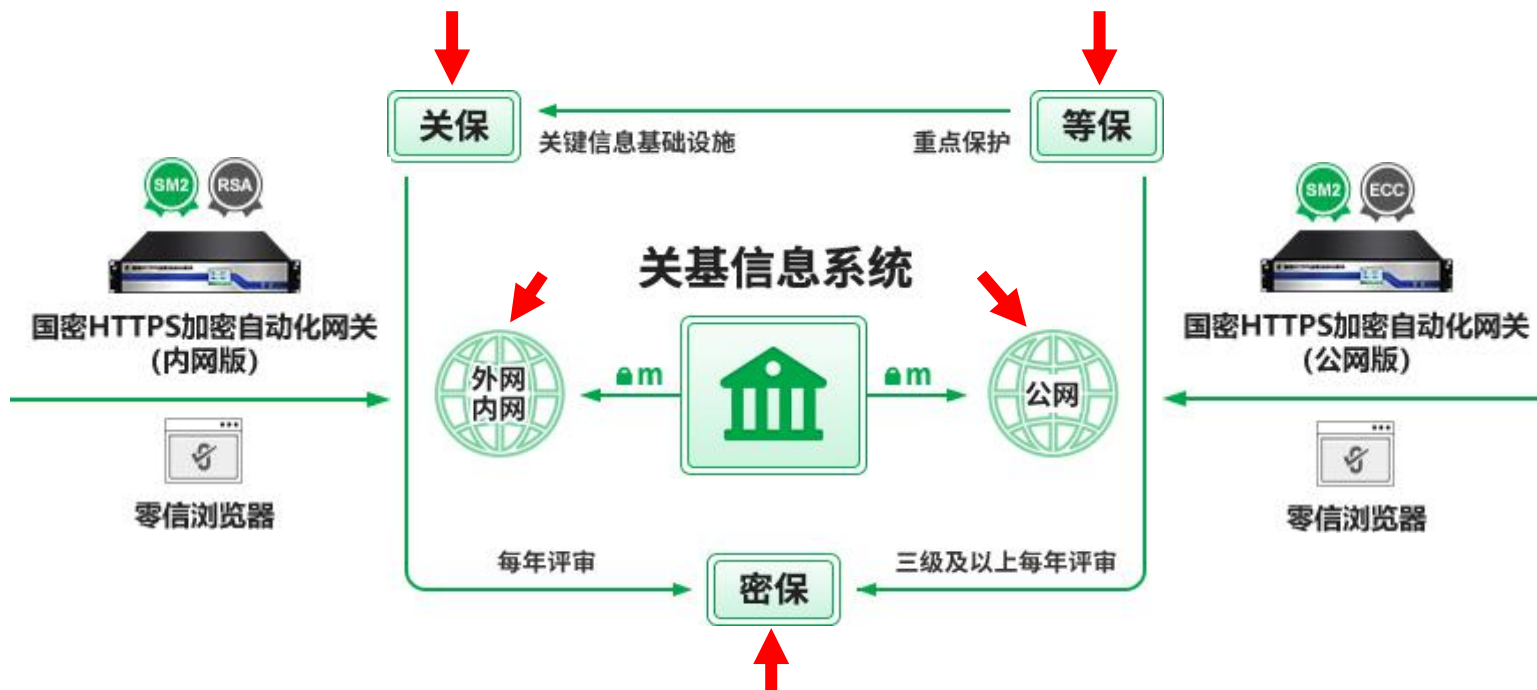


政务云商密HTTPS加密自动化管理解决方案



- 只需在原政务网站服务器群之前增加部署国密HTTPS加密自动化网关阵列组成HTTPS卸载系统和WAF防护系统即可
- 一次部署、全政务云实现https加速、https卸载、WAF防护
- 本地部署政务云SSL系统实现双SSL证书自主签发、到期自动续期
- 自适应加密，不限制用户使用何种浏览器

等保-关保-密保，一站式微改造国密HTTPS加密解决方案



《规定》是保护关键信息基础设施安全的重要举措

- SSL证书有效期即将缩短为47天，这给所有关基运营者带来了巨大的技术改造压力，而《规定》的出台需要关基运营者做好双合规规划，及时落实经费预算，一步到位实现双算法SSL证书的自动化管理，而不是采用SSL证书人工部署的老方案。
- 只有实现SSL证书自动化管理，才能真正实现用好用对密码产品来保障我国关键信息基础设施的安全，真正实现普及应用商用密码来保障业务系统的不间断的持续可靠运行。

重磅关基规定，重任重责重罚，轻改方案是首选！

彩蛋：一次技术改造完成两次HTTPS加密技术革命

- SSL证书从人工管理到自动化管理的技術革命，必须升级改造系统
- HTTPS加密从传统密码到抗量子密码的技术革命，必须升级改造系统
- 零信技术创新实现一次微改造完成两次技术革命必须的技术改造，不仅完成自动化证书管理技术革命，而且可以无缝免费升级系统完成抗量子密码技术革命
- 正如谷歌推动缩短SSL证书有效期是为了轻松过渡到抗量子密码所言，既然完成两次HTTPS加密技术革命是必须的，那就应该在规划第一次技术革命时想到第二次技术革命，把两次技术革命所需要的技术改造一起规划，选择一次完成的先进技术方案，只有这样才是最节省投资和减轻升级改造负担的最佳解决方案。

主讲老师王高华简介

- 中国国产SSL证书开创者
- 中国商密SSL证书开创者
- 中国商密证书透明开创者，商密标准制定牵头人
- 中国商密证书自动化管理开创者，商密标准制定牵头人
- 国际标准组织—CA/浏览器论坛 委员
- 国际组织—PKI联盟 委员
- 深圳市大数据资源管理中心 前 总工程师
- 沃通CA(360安全集团收购)创始人、前 CEO&CTO
- 零信技术（深圳）有限公司 创始人、CEO&CTO
- 广西商用密码协会 特聘专家



推荐订阅公众号—密码讲堂



CEO博客已累计发表中文 219 篇(共 65 万 2 千多字)
和英文 96 篇(13 万 1 千多单词)

关键信息基础设施 商用密码使用管理规定

(国家密码管理局、国家互联网信息办公室、公安部令第5号)

重磅关基规定，重任重责重罚，轻改方案是首选

本文分析了目前国密HTTPS加密应用的现状，为关基运营者提供了一个轻松搞定《规定》合规要求的解决方案，零信技术历时4年创新打造，真正实现商用密码保障业务系统的不间断的持续可靠运行。

2025年06月30日

[阅读全文](#)

祝本次研讨会圆满成功！祝广西壮族自治区密码事业蒸蒸日上！

谢谢大家！

