广西商用密码协会

密码铸盾八桂行--柳州站 密码科普讲座

密码赋能人工智能安全

广西商用密码协会专家 王高华

2025.04.15

密码保障AI应用安全，AI离不开密码保障

- AI安全包括：本地部署和使用大模型的安全 和 训练大模型所需数据的安全
- 目前存在的安全问题有：

(1) 本地部署后使用不安全的http://明文方式访问，无法保障AI输出数据不会被非法篡改和非法窃取，怎么保障?

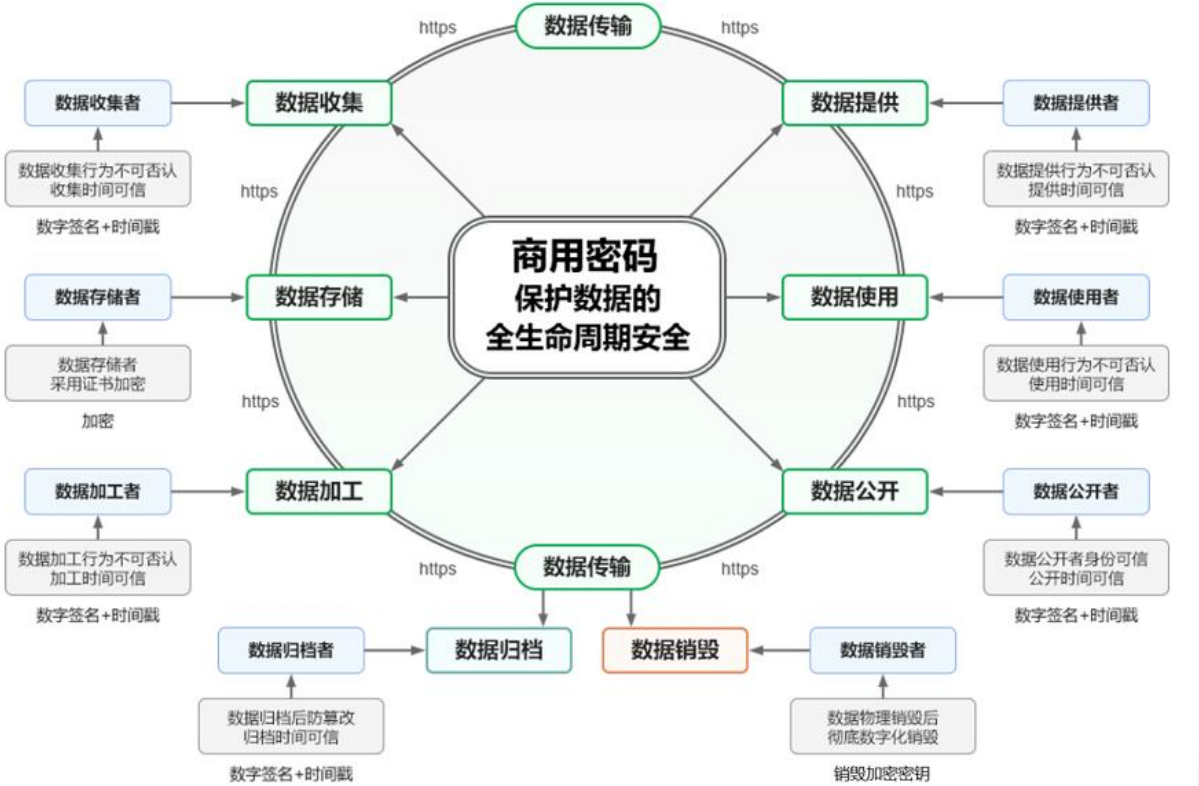
(2) AI应用成功的核心是原始数据的真实性，如何保障大模型所需数据的全生命周期安全?

密码保障AI应用安全，AI离不开密码保障

- 本地部署必须是https加密方式访问，而不能是http明文裸奔方式！
- 如何保障训练AI所需的原始数据的全生命周期安全--https加密
- 电子政务+AI，首先必须保证AI所需的政务数据安全--https加密
- 工业互联网+AI，首先必须保证AI所需的工业数据安全-- https加密

AI应用安全急需HTTPS加密，否则AI会给出灾难性的结果！

密码如何保障AI数据全生命周期安全?



《数据安全法》第三条对“数据处理”的定义：数据处理包括：数据收集、数据存储、数据使用、数据加工、**数据传输**、数据提供、数据公开。

密码保障AI应用安全，AI离不开密码保障

AI应用安全急需HTTPS加密，否则AI会给出灾难性的结果！

广西能在AI起步时同步做好密码保障工作，一定会领先全国！

HTTPS加密是全球第一大密码应用，保障全球万物互联(包括AI)安全！

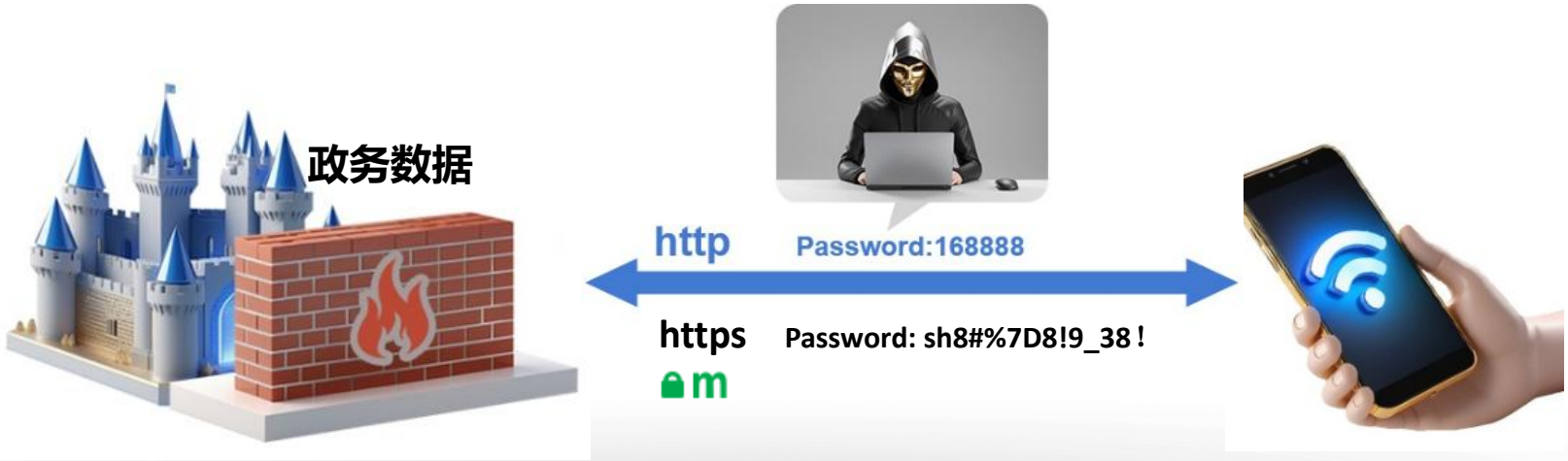
密码保障AI安全

什么是http？为何所有浏览器都提示“不安全”？

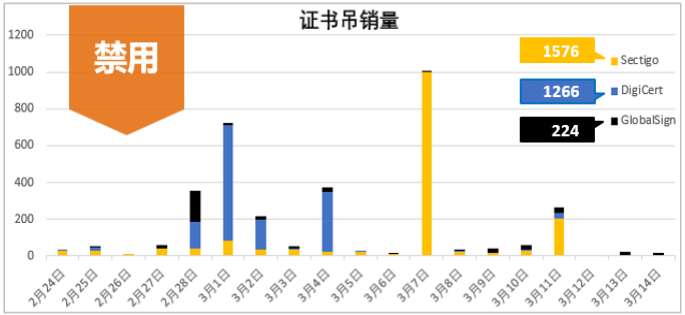
什么是https加密? 什么是商密https加密?

AI时代、万物互联时代、移动互联网时代更需要HTTPS加密

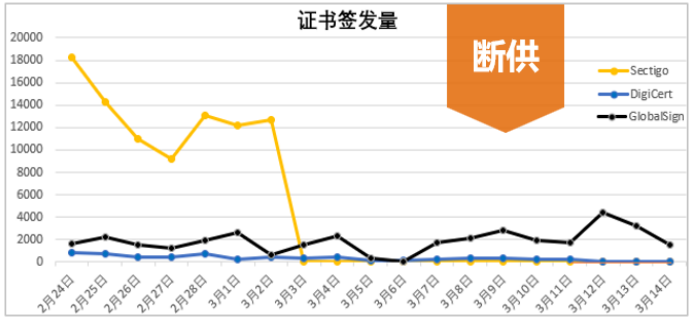
- 传统攻击是攻击服务端，传统安全防护是堡垒防护。
- 现在的万物互联时代和AI时代，是移动互联网时代，数据在流通，让数据跑题。
- 新的攻击方式是直接在数据传输路径上窃取和篡改数据，而不去攻击服务端！
- 所以必须实现**https加密**传输，并且是**商密https**加密！



我国为何必须实现商密HTTPS加密?



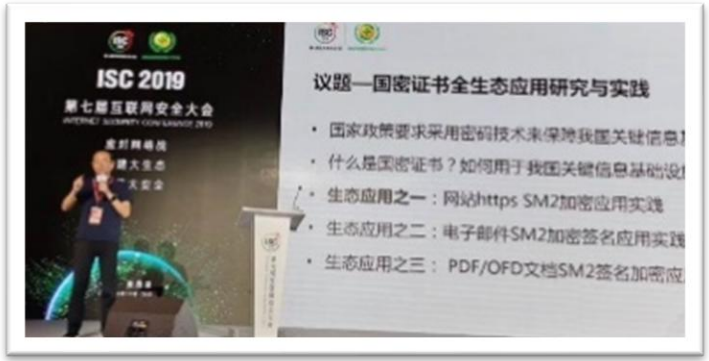
俄乌冲突发生后20天内三千多张RSA证书被非法吊销、10天后被断供、政府和银行网站系统无法访问!



- 我国政务系统(包括智慧城市系统)、电信系统、银行系统目前几乎100%都是RSA算法SSL证书，俄罗斯的遭遇就是前车之鉴，我国也极有可能遭遇断供和禁用，部署的RSA算法SSL证书无法保证我国网络服务包括政务服务和网银服务等的不间断可靠运行!
- 这就是为何《密码法》《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施保护条例》等法律法规都要求关键信息基础设施必须采用商用密码进行保护，实现商密HTTPS加密。

我国做好了防止类似恶性互联网安全事件发生的准备了吗?

2019年8月20日
第七届互联网安全大会



HTTPS加密不仅仅是等保和密评的强制项和加分项

实现商密HTTPS加密困难重重，太难了！

常用浏览器
移动App
不支持商密

Web服务器
不支持商密
加密增加负担

CDN/WAF
不支持商密

证书有效期
将缩短为47天

传统CA系统
不支持签发
商密SSL证书
不支持证书透明

改造工程复杂
无从下手

改造有风险
对业务入侵较大
业务系统不能动

难在整个生态系统安全都是基于RSA密码体系的，全生态商密改造很难！

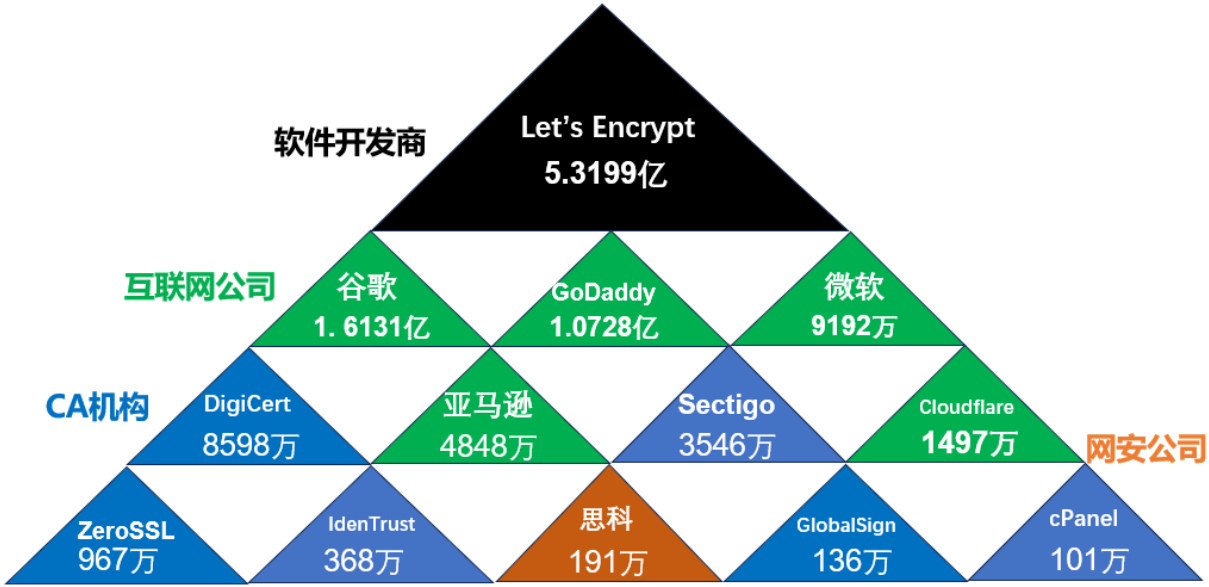
这就是为何全国只有2个省1个部委1个银行官网实现了商密HTTPS加密！

31个省市自治区国际SSL证书申请数据 (2025.03.30)

排名	省市自治区	数量	增长%	占比%	检索域名	默认https	部署国密	WAF防护	安全评级
1	上海市	246	-7.87%	15.06%	shanghai.gov.cn, sh.gov.cn	是	否		B+
2	浙江省	137	-8.05%	8.39%	zj.gov.cn	是	否		B
3	北京市	116	-4.92%	7.10%	beijing.gov.cn	是	否	有	B+
4	海南省	107	-6.14%	6.55%	hainan.gov.cn	是	否		B+
5	广西壮族自治区	80	-12.09%	4.90%	gxzf.gov.cn	否	否		
6	宁夏回族自治区	73	-5.19%	4.47%	nx.gov.cn	是	否	有	B+
7	广东省	69	-4.17%	4.23%	gd.gov.cn	否	否		
8	山东省	64	-7.25%	3.92%	shandong.gov.cn, sd.gov.cn	否	否		
9	云南省	58	-4.92%	3.55%	yn.gov.cn	是	否		B+
10	河南省	56	0.00%	3.43%	henan.gov.cn	是	否		B+
11	甘肃省	54	5.88%	3.31%	gansu.gov.cn	是	否		B+
12	陕西省	54	35.00%	3.31%	shaanxi.gov.cn	是	是		B+
13	天津市	53	-25.35%	3.25%	tj.gov.cn	是	否	有	B+
14	贵州省	45	-11.76%	2.76%	guizhou.gov.cn	是	否		
15	吉林省	42	-10.64%	2.57%	jl.gov.cn	否	否		
16	江西省	42	-8.70%	2.57%	jiangxi.gov.cn	否	是		
17	安徽省	39	2.63%	2.39%	ah.gov.cn				
18	湖南省	38	-11.63%	2.33%	hunan.gov.cn				
19	重庆市	37	-11.90%	2.27%	cq.gov.cn				
20	青海省	32	-11.11%	1.96%	qinghai.gov.cn				
21	黑龙江省	31	-29.55%	1.90%	hlj.gov.cn				
22	新疆维吾尔自治区	29	-9.38%	1.78%	xinjiang.gov.cn				
23	辽宁省	28	-6.67%	1.71%	ln.gov.cn				
24	河北省	23	-36.11%	1.41%	hebei.gov.cn				
25	江苏省	21	0.00%	1.29%	jiangsu.gov.cn, js.gov.cn				
26	西藏自治区	17	-15.00%	1.04%	xizang.gov.cn	否	否		
27	福建省	15	-25.00%	0.92%	fujian.gov.cn, fj.gov.cn	否	否		
28	山西省	10	0.00%	0.61%	shanxi.gov.cn	否	否		
29	内蒙古自治区	9	-18.18%	0.55%	nmg.gov.cn	是	否		B+
30	湖北省	5	-44.44%	0.31%	hubei.gov.cn	否	否		
31	四川省	3	0.00%	0.18%	sc.gov.cn	是	否		B+
	合计	1633	-8.21%			18	3	5	2025Q1

	数量	检索域名
中国大陆	14,856	*.gov.cn
中国台湾省	15,039	*.gov.tw
中国香港特别行政区	2,657	*.gov.hk
中国澳门特别行政区	465	*.gov.mo

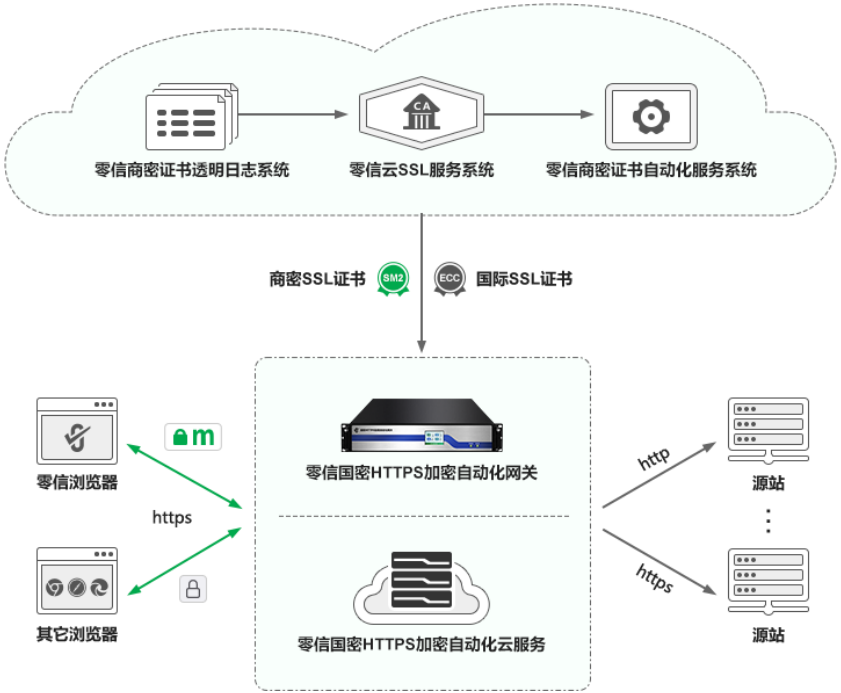
解决方案只有一个：SSL证书自动化管理，HTTPS加密自动化



全球前十三大SSL证书提供商排名和证书签发量(2025.3.30统计)

11.0467亿
自动化部署
比例超过
90%

商密HTTPS加密自动化解决方案—微改造！



微改造，全自动实现商密HTTPS加密！

端云一体，自动配置双算法SSL证书
自动化实现商密HTTPS加密

免费配套商密浏览器—零信浏览器
优先采用商密算法，支持商密证书透明

让商密改造不再难！

学习《密码法》第二条：什么是密码？

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。

- **第一：明确定义了密码的形态**

密码是一项技术，称为密码技术；也可以是一种产品，称为密码产品；也可以是一种服务，称为密码服务。密码以三种形态存在，可以是技术、产品和服务，这为密码从业者指明了发展方向，可以从事密码技术研究，可以从事密码产品研发、生产和销售，也可以提供密码服务，以服务形式来提供密码产品，通常指云密码服务或称密码云服务。

- **第二：明确定义了密码的用途**

密码用于加密保护和安全认证，准确理解这个用途非常重要，给密码从业者指明了密码到底该用在什么地方。第一个用途是**加密保护**，这是用途最广泛的应用，如**HTTPS加密**、数据加密、邮件加密和数字签名、文档加密和数字签名、软件代码数字签名等。第二个用途是安全认证，用数字签名技术来实现安全可靠的用户身份认证。

- **第三：明确定义了密码的技术路线**

通过特定变换的方法来实现，这个特定变换的方法就是密码算法，用密码算法来实现特定变换。特指商用密码算法，如：SM2、SM3、SM4和SM9等，不包括国外的密码算法，这一点非常重要，一定不能搞错。

- **第四：明确定义了密码的保护对象**

是信息等。信息需要用密码来实现加密保护，信息同时需要密码来实现安全认证后才能获取。等就是所有其他元素都可以用密码来实现加密保护和安全认证。

学习《密码法》第二十七条和第三十七条

第二十七条　法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。

第三十七条　关键信息基础设施的运营者违反本法第二十七条第一款规定，未按照要求使用商用密码，或者未按照要求开展商用密码应用安全性评估的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者违反本法第二十七条第二款规定，使用未经安全审查或者安全审查未通过的产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第三十八条　法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

学习网信办等四部委《互联网政务应用安全管理规定》

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)

第三条 建设运行互联网政务应用应当依照有关法律、行政法规的规定以及国家标准的强制性要求，落实网络安全与互联网政务应用“同步规划、同步建设、同步使用”原则，采取技术措施和其他必要措施，防范内容篡改、攻击致瘫、数据窃取等风险，保障互联网政务应用安全稳定运行和数据安全。

第二十九条 互联网政务应用应当使用安全连接方式访问，涉及的电子认证服务应当由依法设立的电子政务电子认证服务机构提供。

HTTPS加密

用CA签发的商密SSL证书实现商密HTTPS加密

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。

第四十二条 列入关键信息基础设施的互联网门户网站、移动应用程序、公众账号，以及电子邮件系统的安全管理工作，参照本规定有关内容执行。

第四十四条 本规定自2024年7月1日起施行。

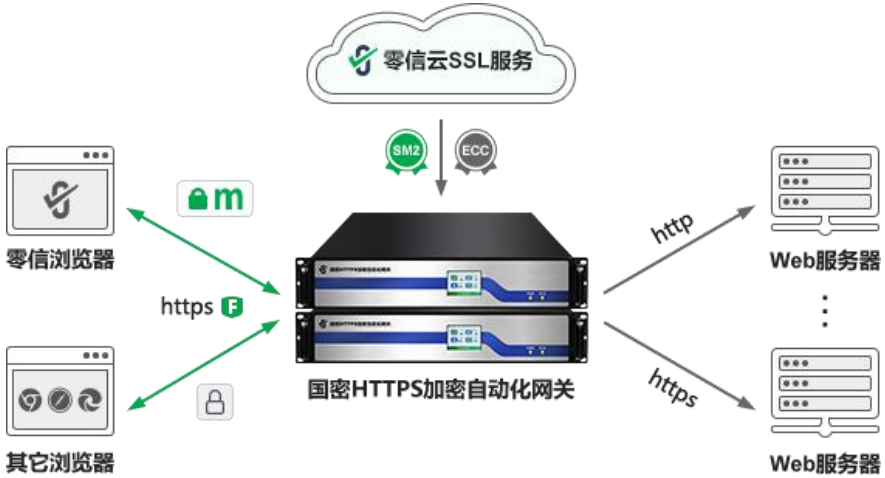
任务很重，怎么办？唯一可行的解决方案只有自动化实现商密HTTPS加密！

学习《商用密码随机抽查事项清单》(2024年7月19日施行)

序号	抽查类别	抽查事项	抽查内容	抽查依据	抽查主体	抽查对象	抽查比例和频次	抽查方式
3	商用密码应用	商用密码应用随机抽查	使用商用密码技术、产品和服务的合规性、正确性、有效性	《中华人民共和国密码法》第二十七条、第三十七条 《商用密码管理条例》（国务院令第760号）第三十八条、第三十九条、第四十一条、第六十条、第六十二条、第六十四条 《商用密码应用安全性评估管理办法》（国家密码管理局令第3号）第六条、第七条、第八条、第九条、第十条、第十一条、第十二条、第十三条、第十四条、第十五条、第十七条、第十八条	密码管理部门	法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统运营者	从法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统运营者中随机抽取。3年内已接受随机抽查、无违法违规行为的，不列入随机抽查范围。对随机抽查不合格的运营者加大抽查频次。	现场、书面、网络检查相结合

- **威慑力更大**：一定会查！每个单位都有可能被抽查到！
- **抽查方式灵活**：如：用零信浏览器访问官网看看是否显示 m 标识即可！

怎么应对抽查？自动化实现商密HTTPS加密，一劳永逸！



- **无需**购买和部署商密SSL证书
- **无需**购买商密浏览器
- Web服务器**无需**商密改造

只需：

- 部署商密HTTPS加密自动化网关
- 保5年最多255个网站实现不间断的商密HTTPS加密和WAF防护
- 免费配套商密浏览器—零信浏览器

密评和密改必须与时俱进

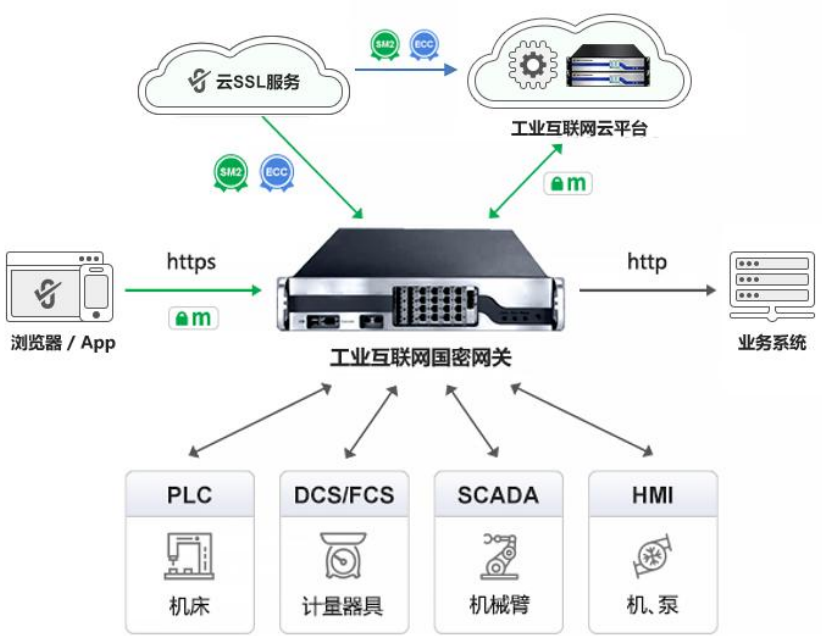
- **密评**就是要评估网络和信息系统的密码应用合规性—是否采用了商用密码算法和相关的商用密码产品，评估是否正确采用，评估采用后是否有效，是否能真正用商用密码来保障网络和信息系统安全。这就是密评三要素—是否采用、是否正确采用、采用后是否有效。
- 《**规定**》第二十九条要求互联网政务应用应当使用CA机构提供的商密SSL证书来实现HTTPS安全连接方式访问，这就是明确了必须采用、必须正确商用密码来实现HTTPS加密连接。这个就需要第三方密评机构来评估是否已经采用，是否正确采用，采用后是否有效。
- **密评**的重点应该是评估用户是否满足《规定》和《抽查》的要求--评估互联网政务应用的网络和通信安全是否正确有效地采用了商用密码技术、产品和服务来保护，那就是检查互联网政务应用是否实现了商密HTTPS加密。
- **密改**的重点应该是帮助用户轻松实现商密HTTPS加密，满足《规定》《抽查》的要求。

普及应用密码，保障设备、身份、网络、应用、数据安全

密码五大支柱应用，保障网空安全！

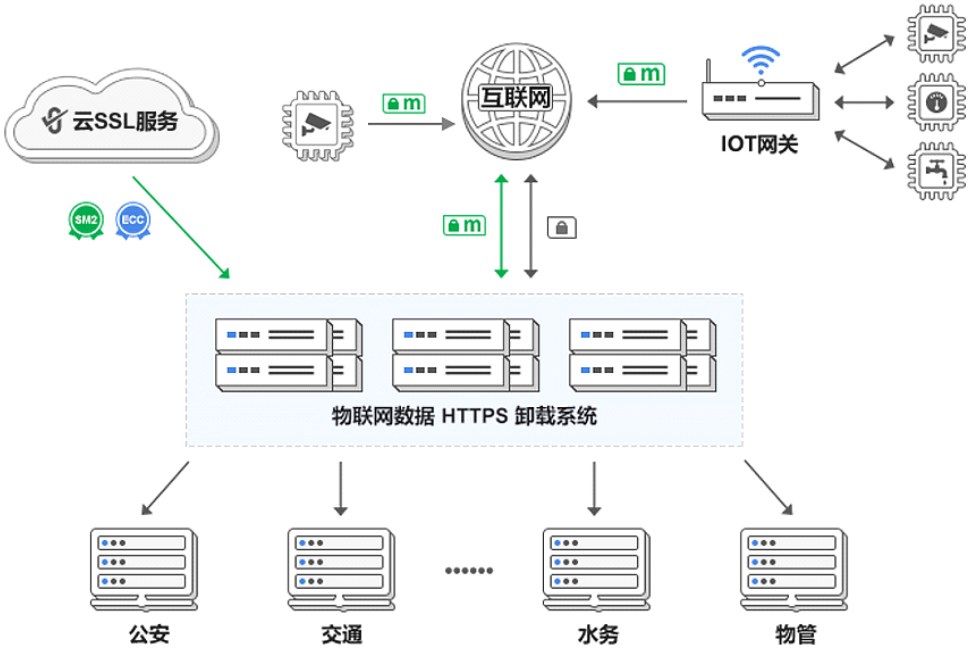
工业互联网的数据安全必须用商用密码来保护

- 目前工业互联网的大量联网数据都是http明文通信，这很不安全！
- 工业互联网商密网关负责把各种工业设备的通信协议转换和指令转化，并统一转换为https协议实现各种工业数据的采集、处理和输出，并对接用户端浏览器/APP和工业互联网云平台
- 由云SSL服务系统自动化为工业互联网商密网关和云平台网关配置双算法双SSL证书，确保不间断的https加密服务
- 现有工厂业务系统零改造实现商密https加密，保障联网工业数据安全

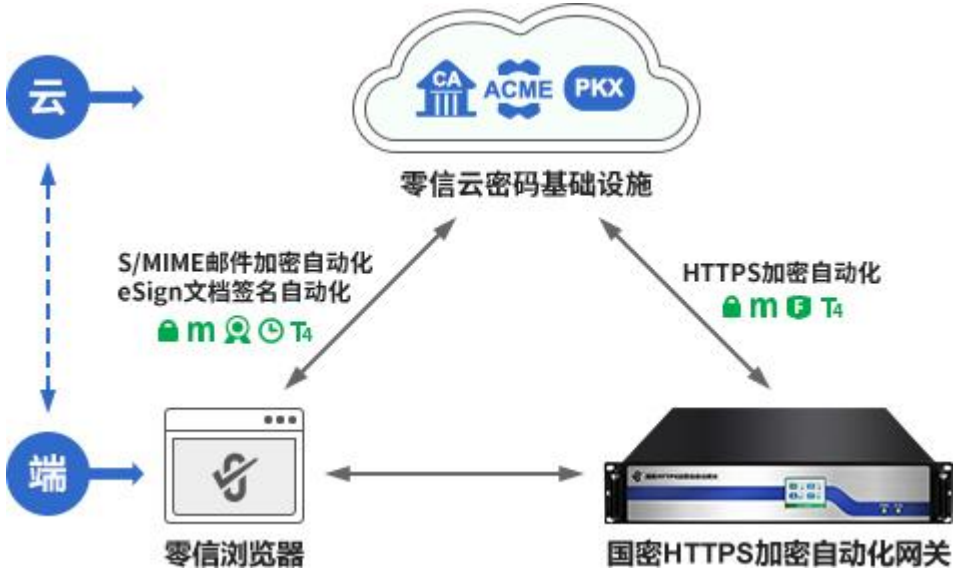


智慧城市的数据安全必须用商用密码来保护

- 目前所有摄像头采集数据到云端都是明文传输，所有智慧灯杆、水利、土地、交通、城管等等数据采集到云端都是明文传输
- 所有数据流通交换都是明文传输，明文传输或简单加密都会导致数据在传输和流通过程被篡改和被非法窃取
- 数据被篡改将导致AI得出错误结果，后果很严重，数据被窃取将导致泄密、系统容易遭遇攻击
- 商密HTTPS加密，保障智慧城市数据安全



自动化实现所有密码应用，才是唯一出路！

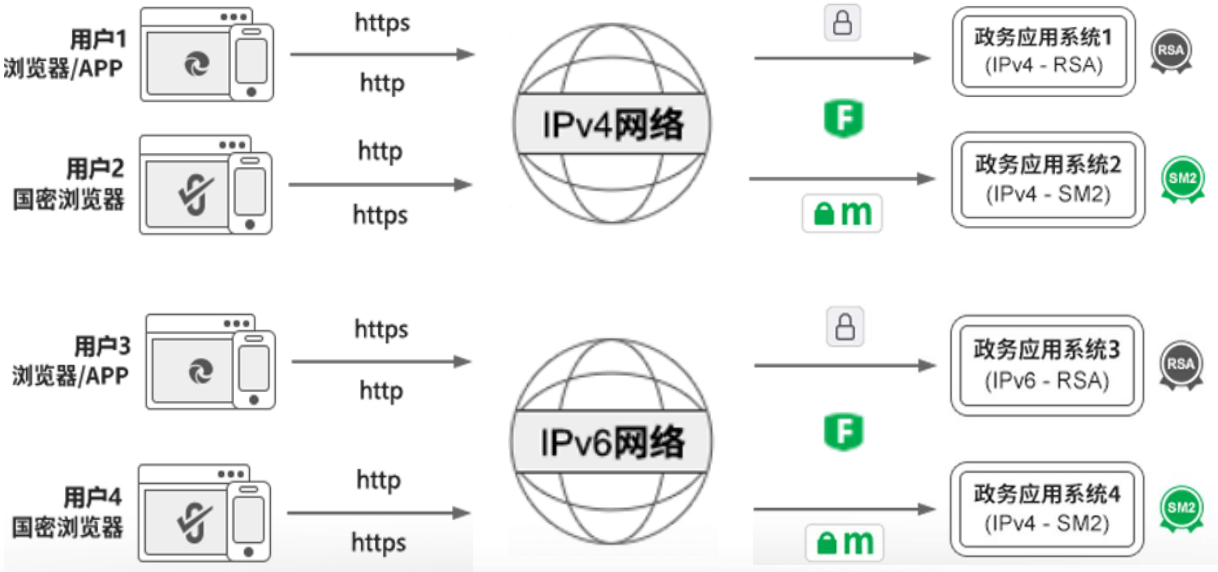


- 自动化配置SSL证书实现HTTPS加密自动化
- 自动化配置邮件证书实现S/MIME邮件加密自动化
- 自动化配置文档证书实现eSign文档签名自动化

- 端云一体实现自动化！算力在云，关键应用在端。

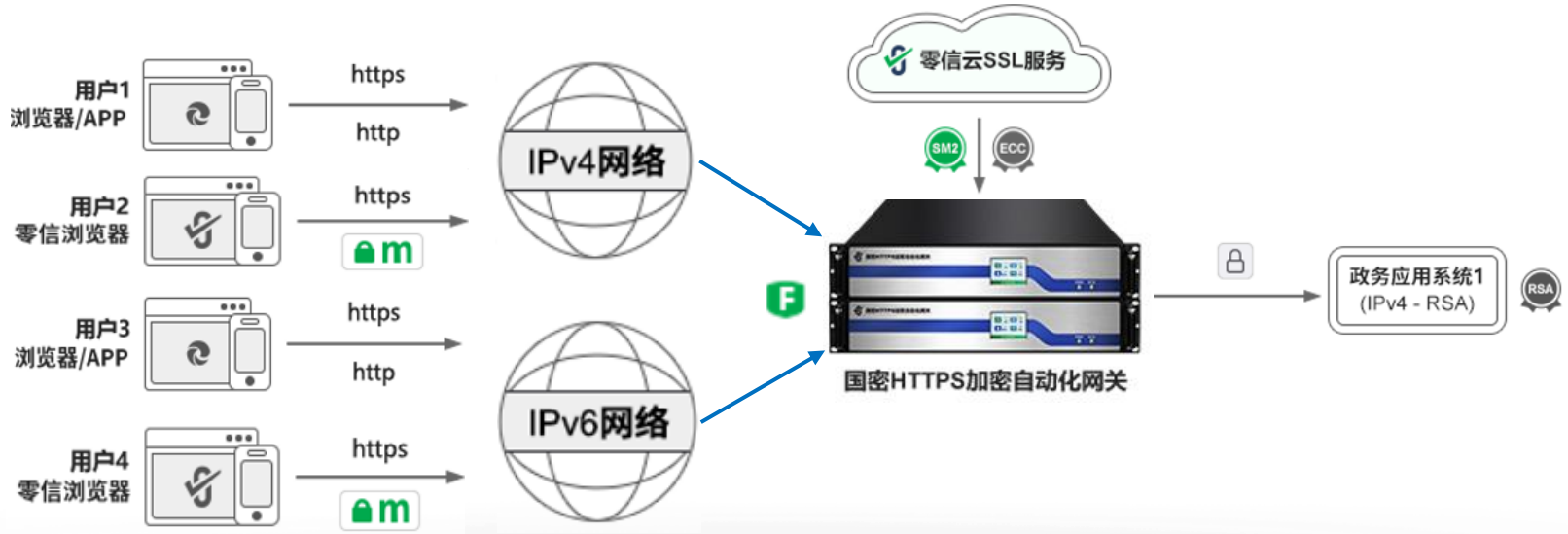
针对密改用户：传统方案，费钱费力不安全，不合理

- 传统方案需要投资建设**4**套系统，分别满足RSA/SM2和IPv4/IPv6的HTTPS加密和WAF防护需求
- 不合理，浪费投资，降低了系统可靠性，提升了系统管理难度！



针对密改用户：推荐零改造的商密改造/IPv6改造/WAF防护方案

- 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！



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

推荐订阅公众号—密码讲堂

CEO博客已累计发表中文 208 篇(共 61 万 1 千多字)和英文 90 篇(11 万 9 千多单词)

第2讲 什么是密码?

密码讲堂 | 赛迪密码专稿 | 密码是信创的根基

密码讲堂 | 阿里云谷创新谈 | 零信任 + 密码，云时代下的网络安全之路

密码讲堂 | 深商密协会讲座 | 深圳商用密码产业升级与发展思路探讨

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！