《自动化证书管理规范》商密标准与商密证书自动化管理生态

由零信技术牵头制定的商密标准《自动化证书管理规范》已经批准立项制定，本文讲讲这个标准的制定过程，也讲一讲大家关心的与标准相关的一些关键技术，并结合讲一讲零信技术成功打造的商密证书自动化管理生态产品。具体话题有：

(1) 为什么必须制定自动化证书管理商密标准？

(2) 《自动化证书管理规范》与 RFC8555 国际标准有哪些不同？

(3) 零信技术打造的商密证书自动化管理生态产品有哪些？是否符合《自动化证书管理规范》？

(4) 哪些产品厂商应该支持《自动化证书管理规范》商密标准？零信技术能提供哪些支持？

一、 为什么必须制定自动化证书管理商密标准？

2022 年 2 月 24 日发生了俄乌冲突，美国 CA 就开始吊销了俄罗斯政府和银行网站使用的 SSL 证书，20 天内吊销了三千多张，几乎覆盖了所有政府网站和银行网站，并同时不再为这些网站签发新的证书。这个“断供”和“禁用”SSL 证书的恶性互联网安全事件非常值得我国高度警惕，在当前非常不确定的国际局势下，我国政府网站和银行网站部署的 RSA 算法 SSL 证书也极有可能同样遭遇“禁用”和“断供”！所以，我国必须未雨绸缪，把普及应用商密算法 SSL 证书来保障我国互联网安全提到第一紧急处理任务上来，这也是《密码法》合规的迫切要求。

而要想普及应用商密 SSL 证书，我们必须同国际 SSL 证书的普及应用对比分析差距，我们还缺什么？已经有 CA 机构能签发商密 SSL 证书，已经有浏览器支持商密 SSL 证书和商密算法实现商密 HTTPS 加密，那商密 SSL 证书还缺什么？**还缺自动化证书管理标准**，就是如何实现自动化申请和部署 SSL 证书。

SSL 证书从 1994 年诞生以来一直人工手动方式申请和部署，用户需要自己生成密钥对和证书请求文件(CSR)，在 CA 网站上提交 CSR 文件、填写证书身份信息和完成域名验证，然后就是等待 CA 签发证书，CA 在完成必须的验证和鉴证后签发证书给用户，用户拿到证书后把私钥和证书安装到 Web 服务器上，就可以启用 HTTPS 加密服务了。这个繁琐的手动方式，每年都要操作一次，因为 SSL 证书有效期只能是 1 年，现在已经进入普及应用 HTTPS 加密时代，所有浏览器都对未部署 SSL 证书的 http 网站提示“不安全”，但是如果要管理几十个、上百个、

成千上万个网站，由工程师手动申请和部署 SSL 证书几乎成为不可能完成的事情，这就是大家看到的为何各省市还有那么多政府网站没有部署 SSL 证书的主要原因。而谷歌正在推动国际 SSL 证书有效期缩短为 90 天，这就彻底把手动部署 SSL 证书变成了不可能，所以普及实现自动化证书申请和部署已经成为必须项，而不是可选项。

国际上的自动化实现证书申请和部署遵循的国际标准是 RFC8555-自动化证书管理环境(**ACME**)，这个标准定义了一些 API 接口协议实现了由 ACME 客户端软件对接 CA 系统实现自动化证书申请和签发，这是 SSL 证书自发明以来的革命性的创新，让 SSL 证书普及应用成为了可能，用户只需在 Web 服务器上安装一个 ACME 客户端软件即可，一次安装和配置就可以永久自动化实现 HTTPS 加密，当然前提是有 CA 机构提供 SSL 证书，目前一般都是 90 天有效期的免费 DV SSL 证书，这类证书只需自动化完成域名控制权验证就能自动化签发，也就可以做到完全免费。目前有效的全球信任的 114 亿张 SSL 证书中，超过 80%的 SSL 证书都是自动化申请和部署的，这个成绩当然要归功于 RFC8555 国际标准，正是由于有了这个标准，全球业界就可以依据此标准实现了 SSL 证书的自动化管理，包括申请、签发、部署、续期和吊销等，实现了 HTTPS 加密的快速普及应用，由 2016 年的 26%的 HTTPS 加密普及率只用了 3 年时间就提升到 80%。目前，ACME 标准的主要制定者-Let's Encrypt 每日签发 SSL 证书高达 360 多万张，遥遥领先于其他 SSL 证书提供商，位于全球市场第一位。

但是,这个完美的通过自动化证书管理实现普及应用 SSL 证书的解决方案不支持商密 SSL 证书的自动化管理，商密 SSL 证书是双证书模式(签名证书和加密证书)，而国际 SSL 证书是单证书模式，我们无法完成套用 ACME 协议实现商密 SSL 证书的自动化管理，所以我国要想实现快速普及应用商密 SSL 证书，也必须实现商密 SSL 证书的自动化管理，这就必须先有商密证书自动化管理标准，有了标准业界才能依据标准来实现自动化证书管理。

也就是说，通过对标分析国际 SSL 证书的自动化管理生态，我们发现商密 SSL 证书的普及应用还缺自动化证书管理生态，那我国就应该建设这个生态，也就必须先制定自动化证书管理商密标准。

二、 《自动化证书管理规范》与 RFC8555 国际标准有哪些不同？

上面分析了我国必须参考自动化证书管理国际标准制定自己的自动化证书管理商密标准，所以，零信技术牵头制定的《自动化证书管理规范》商密标准草案就是完整地参考和采用了国际标准 RFC8555，但把 API 密钥对算法和签名算法由 ECC 算法改为 SM2 算法，把提交 CSR 和下载证书改为同时提交两个 CSR 文件和下载两张 SSL 证书，这是最主要的不同之处，具体

不同之处有如下几点：

(1) RFC8555 在申请证书时仅需提交一个 CSR 内容，商密标准则预留了这个“csr”参数仍然用于国际算法 CSR，同时增加了“csrSign”和“csrEncrypt”参数用于同时提交商密签名证书和商密加密证书 CSR 内容，预留了一个“csrSM2”参数用于将来签发商密单证书使用。这个设计就是为方便用户申请双算法双 SSL 证书，因为目前商密 SSL 证书的部署都是双算法双 SSL 证书模式，用于兼容支持所有浏览器实现自适应算法 HTTPS 加密。

(2) RFC8555 下载已签发的证书也只有一个下载网址，商密标准则不仅预留了下载国际算法 SSL 证书的网址，同时增加了“certificateSign”和“certificateEncrypt”参数用于分别下载商密签名证书和商密加密证书，预留了一个“certificateSM2”参数用于将来下载商密单证书使用。

(3) 增加了证书续订信息(ARI)接口，这是一个计划提交为新的 RFC 标准的新增的 ACME API 接口，直接集成到商密标准中，用于 ACME 服务端通知 ACME 客户端何时续期证书。这个接口不仅可以用于方便通知客户端在某种证书需要吊销之前及时续期新证书，而且可以用于通知客户端来自动申请已经完成身份认证的 OV SSL 证书和 EV SSL 证书。

(4) 增加了扩展标识符类型和挑战类型，如 SIP 号码、VIN 码、IMEI 码等等，适用于电信设备、物联网设备的自动化证书签发。这是由标准制定参与单位之一的华为公司增加的内容。

《自动化证书管理规范》标准草案与 RFC8555 国际标准的所有不同之处见下表。

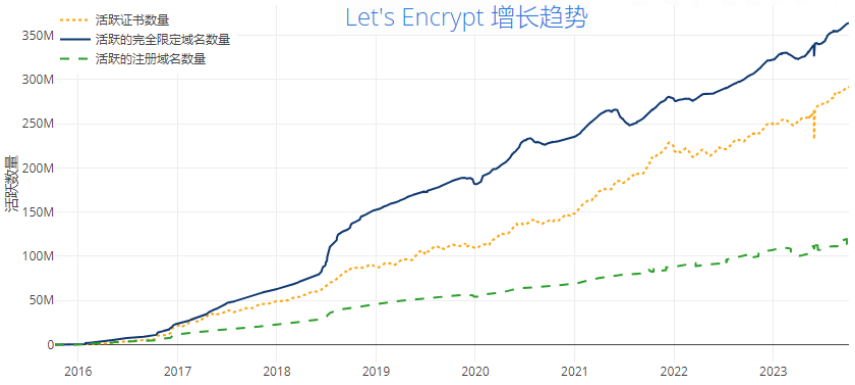
	自动化证书管理规范	**RFC 8555**	**备　　注**
服务端签名算法	8.3 | SM2 算法和 ES256 签名算法	6.2 | ES256 签名算法	是否需要在标准中加入兼容支持 ES256?
订单对象	9.2.3 | 增加 3 个商密 SSL 专用字段	7.1.3 | certificate	原字段仍然用于国际算法证书，新增 3 个用于商密算法证书
CSR 提交	9.5 | 支持同时提交双算法 CSR	7.4 | 提交 1 个 CSR	支持提交 1-3 个 CSR，满足国际和商密证书单独或同时申请需要。
下载证书	9.5.2 | 调 3 次	7.4.2 | 调 1 次	双算法 3 张证书分 3 次取回，因为要叠加证书链。如果一次全部取回，客户端很难分割 3 张证书。
OV/EV 证书支持	9.4.4 | 外部帐户绑定 12.6 | CA 策略注意事项	7.3.4 | 外部帐户绑定 10.5 | CA 策略注意事项	用于绑定 CA 的用户帐户后自动化获取 OV/EV 证书。 CA 必须在签发之前完成网站身份认证，如何验证则不属于本标准制定范围。
增加续订信息	10.8 | 续订信息	没有，计划新增一个	用于服务端通知客户端何时续订证

(ARI)		RFC	书，可用于在 CA 完成身份认证后通过客户端申请 OV/EV SSL 证书
增加其他挑战类型	11.6	扩展挑战符类型 11.7	扩展挑战类型	没有，计划新增多个 RFC	适用于电信设备、物联网设备的自动化证书签发
计划支持	电子邮件证书	没有，其他 RFC 标准	增加邮箱验证方式，支持邮件证书自动化管理
计划支持	代码签名证书、文档签名证书等	没有，其他 RFC 讨论标准	支持其他类型商密证书的自动化管理
其他	Web 服务器如何支持商密算法，不属于本标准制定范围	RFC 勘误表	已更新勘误表内容到商密标准

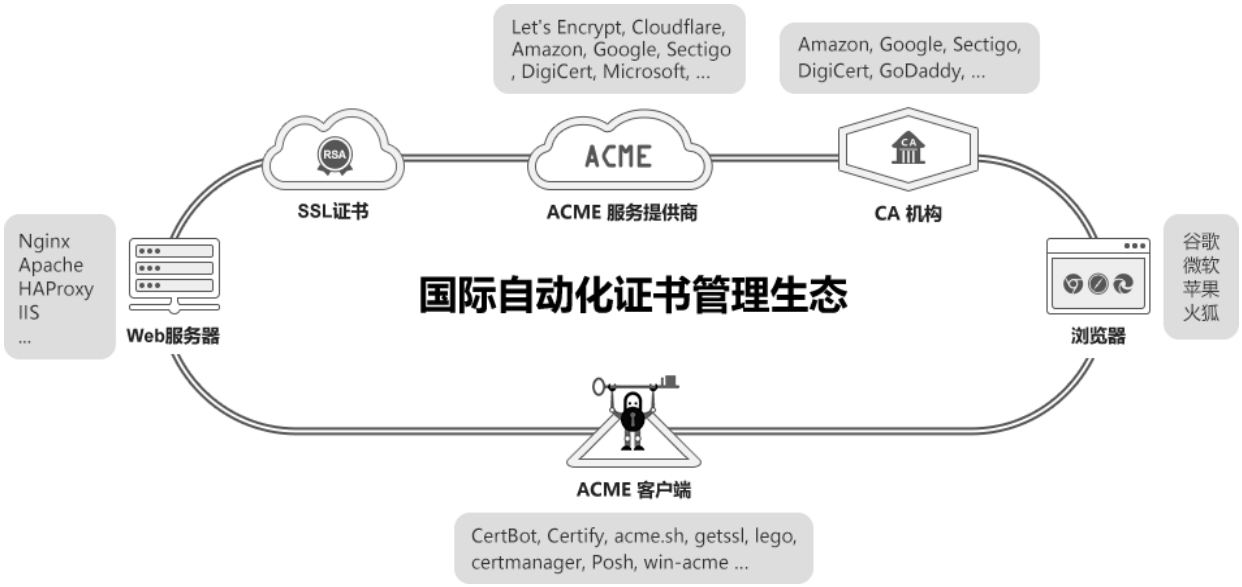
三、 零信技术打造的商密证书自动化管理生态产品有哪些？是否符合《自动化证书管理规范》？

相信有读者朋友看了第二部分的内容可能会认为，制定证书透明商密标准并没有什么技术含量，不就是翻译国际标准并把标准中的密码算法更换为商用密码算法吗？这个似乎谁都可以做，为何是零信技术牵头做这个？这真的是一个非常好的问题，必须在这一段落好好讲一讲。

笔者在第一部分就讲过：要想普及应用商密算法 SSL 证书来保障我国网络空间安全，必须是自动化证书管理方式来实现证书申请、签发和部署，这就需要一个自动化证书管理标准来统一证书申请和部署接口，这就是由 Let's Encrypt 牵头制定的 RFC8555 国际标准。但是，光有标准是不够的，必须建立一个基于标准的生态系统来支持这个标准落地应用。Let's Encrypt 的做法是自己首先开发一个 SSL 证书自动化管理系统为全球用户免费提供 90 天有效期的 DV SSL 证书，大家应该已经看到了这个自动化申请和部署 SSL 证书是何等的受到全球用户的喜爱，让 Let's Encrypt 只用了 3 年时间就做到了 SSL 证书市场份额全球第一，并且是遥遥领先的第一(是第二名的 5 倍多)。于是 Let's Encrypt 就依据这个自研系统牵头制定了 RFC8555 国际标准(ACME)，让业界都可以依据这个标准协议来为用户提供 SSL 证书自动化申请、签发和部署服务。



自从 2019 年 3 月发布 RFC8555 国际标准后，不仅得到了全球用户的喜爱，也得到业界的认可和大力支持，各家 CA 机构和云服务提供商都纷纷提供 ACME 服务。现在，全球市场已经形成了一个很完善的生态，不仅 CA 机构开始为用户提供 ACME 服务，操作系统和 Web 服务器厂商也开始集成 ACME 服务，物联网设备厂商开始采用 ACME 协议为物联网设备自动化配置 SSL 证书，各大云服务提供商也纷纷在其云服务产品中集成 ACME 服务，为云服务用户提供自动化证书申请和部署服务，彻底把用户从繁琐的人工申请 SSL 证书解放出来。如：全球领先的 CDN 服务提供商 Cloudflare，彻底丢弃了原先的用户必须先从 CA 手动申请到 SSL 证书后手动上传 SSL 证书到 CDN 系统中使用的做法，用户只需把网站的 DNS 服务器指向到 Cloudflare 的 DNS 服务器即可，Cloudflare 会自动完成域名验证和自动化免费为用户 CDN 服务配置 SSL 证书，自动化启用 HTTPS 加密服务。这使得 Cloudflare 成为了全球第二大 SSL 证书提供商。



自动化证书管理是普及 SSL 证书的唯一解决方案，是终极解决方案，这就是为何这个协议的名称为英文单词“acme”(终极、顶峰)的原因。所以，要想普及应用商密 SSL 证书，也只有实现自动化申请和部署这一条路。所以，零信技术决定参考 RFC8555 国际标准自研相关产品来实现商密 SSL 证书的自动化管理。但是，商密 SSL 证书自动化管理不能仅仅只实现自动化申请 SSL 证书和签发证书，在部署 SSL 证书之前必须先完成 Web 服务器的商密算法支持改造，也就是要求 Web 服务器必须支持商密算法和商密 SSL 证书才能成功部署使用。这是同国际证书自动化解决方案的最大不同之处，也是难以实现之处，因为现有的 Web 服务器都不支持商密算法和商密 SSL 证书，并且基本上都是封闭系统无法改造支持商密算法，只有开源的 Nginx 方便改造，研发商密算法支持模块，并重新编译 Nginx 就能改造 Nginx 支持商密算法和商密

SSL 证书，实现自适应加密算法的 HTTPS 加密。所以，零信技术做的第一件事就是研发 Nginx 商密算法支持模块，当然市场也有其他完全免费的 Nginx 商密支持模块，如非常优秀的阿里 Tengine 和铜锁 SSL(BabaSSL)。

零信技术打造的第一个商密证书自动化管理生态产品就是商密 ACME 客户端软件-SM2cerBot，这是一个类似了国际证书自动化管理生态产品中的 ACME 客户端软件-CertBot，但不同的是，CertBot 只负责申请和部署单张国际 SSL 证书，而 SM2cerBot 不仅负责申请两张商密 SSL 证书和一张国际 SSL 证书，而且还负责安装自带的支持商密算法模块的新的 Nginx Web 服务器，因为原 Nginx 不支持商密算法。安装好支持商密算法的 Nginx 后才部署已经取回的 3 张 SSL 证书，支持自适应加密算法实现 HTTPS 加密。为何需要部署双算法 SSL 证书？因为我们不能强制要求用户使用何种浏览器，正在大量使用的浏览器和移动 APP 都不支持商密 HTTPS 加密，所以必须同时部署国际 SSL 证书兼容所有浏览器和手机 APP。

但是，这个改造 Web 服务器的解决方案对 Web 服务器是有伤害的，无法像 CertBot 一样做到无缝部署 SSL 证书。所以，对于不能改造 Web 服务器的用户，我们又研发了一个硬件网关产品—零信国密 HTTPS 加密自动化网关，把商密 ACME 客户端集成到 SSL 网关中去，直接由网关来实现双 SSL 证书的自动化申请和部署，由网关实现 HTTPS 加密和卸载转发，这样只需在 Web 服务器前面部署网关即可实现 Web 服务器零改造的商密 HTTPS 加密自动化。而对于有些用户既不想在 Web 服务器上安装商密 ACME 客户端软件，也不想部署硬件网关，我们就把零信国密 HTTPS 加密自动化网关部署到云上为用户提供商密 HTTPS 加密自动化云服务—零信国密 HTTPS 加密自动化服务，这个服务类似于 Cloudflare 的 CDN 服务自动化配置 SSL 证书，用户只需做域名解析即可自动化实现 HTTPS 加密，一样实现自动化配置双 SSL 证书，实现自适应加密算法的 HTTPS 加密。商密 ACME 服务系统负责对接零信云 SSL 系统(CA 系统)，同时为商密 ACME 客户端、商密 HTTPS 加密自动化网关和商密 HTTPS 加密自动化云服务提供 ACME 接口服务，为其自动化签发双算法 SSL 证书。

也就是说，零信技术是先依据国际标准 RFC8555 采用商密算法实现了商密证书自动化管理生态中的所有相关产品，证明了自动化证书管理标准是可以改用商密算法来实现商密 SSL 证书的自动化管理的，并且可以同时实现国际 SSL 证书的自动化管理，实现双算法 SSL 证书自动化部署。为了能尽快证明这个生态的是可行的，我们不是仅仅提出这个概念去求各个相关厂商来支持，而是全部自研产品验证其可行性，验证整个生态相关的产品的可行性。当然，零信技术自己打造的商密自动化证书管理生态产品只是一个自研生态，所以笔者非常感激密标委能在我们完成了自研生态产品后及时批准立项制定自动化证书管理密码行业标准，使得商密自动化证书管理能在我国尽快落地应用，而不是一个企业在自研自用！这必将加快商密 SSL 证书的快速部署应用，使得我国能早日实现普及商密 SSL 证书应用来保障我国网络空间安全。

那么，零信技术自研的商密证书透明生态产品是否全部遵循了《自动化证书管理规范》商密标准草案呢？答案当然是肯定遵循的。但是，我们是自研产品在先，制定标准在后，所以，目前的产品应该属于仅遵循企业标准，是商密标准草案的简化版，标准草案还需要在各参与单位和业界的共同努力下尽快定稿，零信技术所有产品第一时间更新为遵循《自动化证书管理规范》商密标准的产品。目前正在使用的零信商密证书自动化管理生态产品是基于零信云 SSL 系统打造，同零信技术提交的商密标准草案唯一不同的是一次提交 3 张证书的 CSR 和一次取回 3 张证书，因为我们自己知道如何分割收到的 3 张证书，但是作为商密标准，需要对接各家的 CA 系统，我们还是考虑改为 3 个 CSR 分开提交和分开取回证书。我们计划尽快修改现在的产品实现全部遵循商密标准。

四、 哪些产品厂商应该支持《自动化证书管理规范》商密标准？零信技术能提供哪些支持？

《自动化证书管理规范》既然已经批准立项，我们就当现在的标准草案就是将来发布的正式标准，因为这个发布过程将耗时两年，我们没有时间等到那个时候才去实施商密 SSL 证书的自动化管理，我们相信即使商密证书自动化管理标准还没有正式发布，但只要大家都用起来，一样能实现商密 SSL 证书的自动化管理和快速部署应用，因为此商密标准参考的国际标准 RFC8555 已经成功自动化管理了超过 114 亿张国际算法 SSL 证书，是一个非常成熟的协议，大家从第二部分内容也能看到商密标准修改很少，一样可以安全可靠地实现商密 SSL 证书的自动化管理，并同时实现国际 SSL 证书的自动化管理。

笔者在此诚邀商密证书自动化管理生态相关的厂商现在就积极加入到商密证书自动化管理生态建设中来，而不是等到发布正式标准时，现在参与制定和完善标准草案就有机会增加满足自己的产品的应用需求的内容，如华为提出增加的内容就是为了满足电信设备的自动化证书

管理。本标准相关的厂商包括但不限于：签发商密 SSL 证书的 CA 机构、云服务提供商、SSL 网关生产商、SSL VPN 生产商、国产操作系统厂商、Web 服务器软件厂商、各种需要证书的设备生产商等等。《自动化证书管理规范》有一个最大的亮点是支持双算法双 SSL 证书的自动化管理，可以同时自动申请和部署商密 SSL 证书和国际 SSL 证书，满足用户商密合规和全球信任的应用需求。

由于零信技术已经自研了商密证书自动化管理生态的主要产品，所以，零信技术有能力为生态厂商提供如下但不限于的最有力的支持：

(1) 为广大用户提供完全免费的商密 ACME 客户端-SM2cerBot，用户可以在各种 Linux 系统上一次安装此客户端软件，免费配置 90 天有效期的商密 SSL 证书和国际 SSL 证书，证书到期后自动续期，实现永久完全免费自动化 HTTPS 加密。欢迎访问 SM2cerBot 实现的自动化申请和部署双 SSL 证书测试网站：https://sm2test.cersign.cn，此网站证书每天重新申请一张新证书，使用零信浏览器查看部署的是商密 SM2 SSL 证书，使用谷歌浏览器或其他浏览器查看则部署的是国际 ECC SSL 证书，自动化双 SSL 证书部署，自适应加密算法实现 HTTPS 加密。我们之所以设置演示网站为每天自动化申请和部署一次(不排除以后可能会改为不同的证书有效期测试)，也是为了验证 SSL 证书有效期无论是缩短到 90 天还是 1 天，只要实现了自动化管理都不是问题！

(2) 为 CA 机构提供各种商密证书自动化管理解决方案，指导 CA 机构升级 CA 系统为商密 ACME 客户端提供商密证书自动化服务，实现自动化签发双算法双 SSL 证书。

(3) 欢迎各大云服务提供商、国产操作系统厂商、国产 Web 服务器软件厂商、SSL 网关厂商、SSL VPN 厂商支持《自动化证书管理规范》，对接零信商密 ACME 服务，为其产品和云服务自动配置双 SSL 证书，实现开机即用和即买即用的 HTTPS 加密服务，提升其产品核心竞争力！

(4) 在《自动化证书管理规范》商密标准草案不断完善和商密 ACME 客户端-SM2cerBot 不断完善的情况下，零信技术将在合适的时候开源 SM2cerBot 软件，让更多的开发者能基于开源的商密 ACME 客户端软件开发支持更多的操作系统和更多应用的商密 ACME 客户端软件，特别是各种物联网应用，共同为用户提供更多的选择来普及应用商密 SSL 证书实现 HTTPS 加密。

商密证书自动化生态需要各方的积极参与，只有大家一起齐努力，才能真正让商密证书自动化管理标准发挥最大的作用，保障我国能快速实现普及商密 HTTPS 加密的宏伟目标，快速实现商密 HTTPS 加密泛在，共同为商用密码保障我国网空安全做贡献。

有诗为证：

网站加密要普及，自动实现是关键。

商密加密自动化，标准先行生态建。

王高华

2023 年 12 月 12 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。