SSL 证书自动化部署，保障业务系统 HTTPS 加密不间断

部署 SSL 证书已经成为各种业务系统的必须，而 SSL 证书是有有效期的，一旦过期则无法使用，一定会影响业务系统的正常运行。大家先看一个发生在 2018 年 12 月的真实案例：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 万客户以及全球其他运营商的客户都无法正常使用移动通信服务，业务被中断了二十多个小时才恢复。为此，O2 向爱立信索赔数百万美元。由此可见，维持关键业务所需的 SSL 证书持续有效是多么重要的事情，但对于需要维护上百台 Web 服务器的大型机构是一个非常大的挑战，面临着 SSL 证书意外过期的巨大风险，以及由此产生的系统故障和这些故障可能会使企业带来的一段时间内系统瘫痪，从而对企业的业务和声誉造成不可挽回的损失。

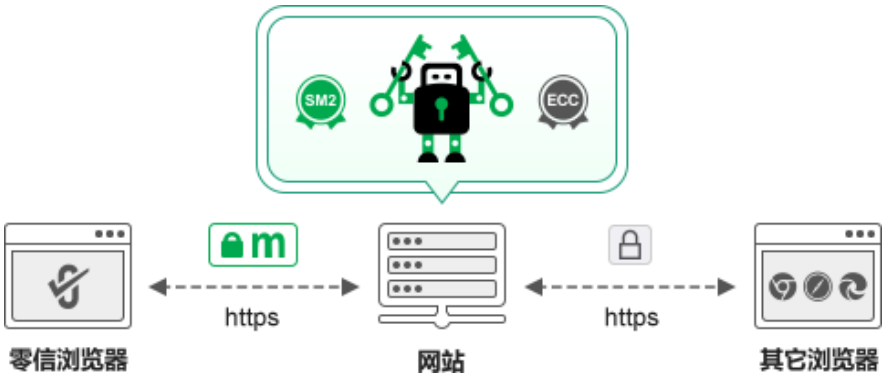
而随着我国《密码法》的深入贯彻落实，关键信息基础设施系统部署国密 SSL 证书已成为必须。这给 IT 管理员带来了新的挑战，因为部署国密 SSL 证书必须先把 Web 服务器改造为支持国密算法。同时为了兼容所有浏览器，还得同时部署全球信任的国际 SSL 证书，国密改造加双证书部署，的确是一个很大的挑战，特别是如果要管理上千甚至上万台 Web 服务器的政务云平台。这就不能理解为何大量的政务网站还没有部署 SSL 证书，因为为成千上万个 Web 网站部署 SSL 证书可不是一个容易的活，特别是还不能影响现有正在运行的系统的正常运行，更不用提证书到期后还需要续期证书和重新部署证书！

怎么办？唯一的办法也只有实现自动化部署了。所幸的是，目前已经有了证书自动化部署国际标准—RFC 8555 (ACME)，目前市场上也已经有了多家支持 ACME 标准的 CA 机构，并且已经大获成功，因为 ACME 自动化部署彻底把 IT 管理员从繁琐的证书申请和部署解决出来了，并且由于实现了自动化，大大降低乃至杜绝了由于人为操作错误和遗忘证书续期带来的业务中断风险。

但是，国际 ACME 不支持自动化部署国密 SSL 证书，只能部署国际 SSL 证书。怎么办？今天上线的证签国密 ACME 服务就是为了解决自动化部署国密 SSL 证书的难题，当然也顺带同时部署了国际 SSL 证书，使得网站能全自动实现 https 加密的自适应加密算法，以支持所有浏览器。支持国密算法和国密证书透明的零信浏览器自动使用国密算法实现国密 https 加密，不支持国密算法和国密证书透明的浏览器则采用 ECC 算法实现 https 加密。

证签国密 ACME 服务由证签技术和零信技术联合鼎力打造，彻底同时解决了国密 SSL 证书和国际 SSL 证书的自动化部署难题，用户只需一次安装国密 ACME 客户端 - SM2cerBot，

就能全自动申请和部署一张全球信任的 ECC SSL 证书、一张国密合规的 SM2 SSL 签名证书和一张国密合规的 SM2 SSL 加密证书一张，同时全自动安装国密算法模块以支持国密算法实现国密 https 加密，一键实现全自动化部署双算法 SSL 证书。不仅支持完全免费的 90 天免费 SSL 证书，也支持有效期为 1 年的扩展验证 EV SSL 证书、单位验证 OV SSL 证书和域名验证 DV SSL 证书，这些 SSL 证书都是自动配置双算法证书。欢迎免费下载 SM2cerBot，享用证签国密 ACME 服务。



王高华

2023 年 1 月 6 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。