随机抽查，妙！厉害！

2024 年 7 月 19 日，国家密码管理局根据《中华人民共和国密码法》、《商用密码管理条例》及相关商用密码管理规章，发布了《国家密码管理局商用密码随机抽查事项清单（2024 年版）》，自发布之日起施行。这是一件大事，必须好好解读一下这件大事，并给出如何一劳永逸地应对这个随机抽查和其他各种合规检查的建议措施。

一、什么是随机抽查？抽查对象是谁？为何采用随机抽查方式？

随机抽查就是按照随机的原则，即保证总体中每一个对象都有已知的、非零的概率被选入作为检查的对象，保证被抽查的公平性。被调查对象总体中每个个体都有同等被抽中的可能，是一种完全依照机会均等的原则进行的抽样检查，以体现对被检查对象的公平性。

国家密码管理局为何要采用随机抽查方式呢？除了体现公平外，其妙处有二：

一是解决被检查的对象太多而检查不过来的问题。本文仅以抽查清单序号 3 为例，其抽查对象是“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”，这个范围太大了，几乎大家日常用到的所有工作和生活所使用的信息系统都包括在内了，根本检查不过来。

二是解决《密码法》的威慑力难题，也就是解决大众心理的“法不责众”而导致有法不依的难题。《密码法》第二十七条明确要求所有关键信息基础设施运营者应当使用商用密码进行保护，但是有几个关键信息基础设施网站做到了呢？都没有做到就会产生“法不责众”的心理，反正违法不止我一家。而这次出台的抽查就是一个很妙的解决方案，太多了我查不过来，但有可

能抽查到你，因为这是一个已知的、非零的概率，你必须做好准备，如果被查到，那就要依据第三十七条“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”，也就是有可能被罚一百万元，这就使得法律真正具备了可操作性的威慑力。

国家密码管理局商用密码随机抽查事项清单（2024 年版）

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

二、 如何抽查？如果被抽到，会检查什么？

抽查清单序号 3 的抽查类别为商用密码应用，这个是本文解读的重点，因为这个涉及面广，根据《关键信息基础设施安全保护条例》的定义：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。这些单位都是依据《密码法》第二十七条要求使用商用密码技术、产品和服务来保护关键信息设施安全的抽查对象，都会有可能被抽查到。

而抽查的内容是检查使用商用密码技术、产品和服务的合规性、正确性、有效性，这就是密评的内容，检查是否使用、是否正确使用、使用后是否实现了有效保护。如何检查这些待检查的内容呢？采用现场、书面、网络检查相结合的方式抽查。也就是说，不一定有人到你单位现场检查，可以通过网络检查，比如：使用零信浏览器访问一下你的官网，看看地址栏是否有 **m** 标识就知道你的网站是否已经使用商密 SSL 证书实现了商密 HTTPS 加密保护，看到了 **m** 标识就是，看不到就不是。看到了 **m** 标识就是已经正确使用，也就是已经实现了有效保护。看一眼就完成了合规性、正确性和有效性检查，并且这个检查随时随地都可以实现，上网溜一圈，一上午就可以检查完所有部委官网、所有省市政府官网。这就是零信浏览器设计在地址栏增加一个 **m** 标识的目的，方便网站访问者和执法检查者一眼就知道这个网站是否采用了商用密码保护。

检查被抽查对象的官网是否实现了商密 HTTPS 加密，这是一个非常容易实现检查的一个检查项，当然还有其他检查项，密码管理部门会依据《中华人民共和国密码法》第二十七条、第三十七条、新版《商用密码管理条例》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》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，从关键信息基础设施网络与信息系统运营单位中随机抽取，检查到任何一项不符合规定的，都可以认定为有违法违规行为，都有可能依法处罚。

三、如何一劳永逸地从容应对抽查？

这应该是所有可能被抽查到的单位都关心的问题，即使通过了等保和密评，也不是一劳永逸的，因为这些评测只能说明当时某些系统已经通过了测评，但一定还有待整改的部分，一定会有不满足要求的部分。比如说：密评是网站已经部署了商密 SSL 证书实现了商密 HTTPS 加密，但是这张商密 SSL 证书现在已经过期了，所以网站都变成了 HTTP 不安全方式或者变成了国际算法的 HTTPS 加密方式，这些都是无法通过检查的。

那么，应该如何一劳永逸地从容应对随机抽查呢？如何应对随时都有可能发生网络检查方式的抽查呢？就网络通信安全的关键项-商密 HTTPS 加密这一项来讲，笔者的主意就是自动化实现商密 HTTPS 加密，只有自动化采用商密 SSL 证书实现所有信息系统的商密 HTTPS 加密，才是一劳永逸的从容应对方案。原 Web 服务器零改造，无需定期向 CA 申请和部署 SSL 证书，无需关心 SSL 证书是否会过期，只需部署零信国密 HTTPS 加密自动化网关，就可以保证 5 年内每台网关为最多 255 个网站自动化实现商密 HTTPS 加密，不怕随时的检查，随时检查都能在零信浏览器地址栏看到商密加密 **m** 标识。

部署了零信国密 HTTPS 加密自动化网关，实现商密 HTTPS 加密自动化，不仅能一劳永逸从容应对密码管理部门的随机抽查，而且还能从容应对四部委发布的《互联网政务应用安全管理规定》所要求的所有互联网政务应用和关键信息基础设施的互联网门户网站必须实现商密 HTTPS 加密安全连接的规定，以规避《规定》第四十一条“依规依纪追究当事人和有关领导的责任”。

部署了零信国密 HTTPS 加密自动化网关，不仅仅能实现商密 HTTPS 加密自动化，而且还能实现 WAF 防护自动化，自动化以商密 HTTPS 加密方式实现最多 255 个网站系统的 WAF 防护，满足等保合规要求，从容应对《网络安全法》的合规要求。

总之，国家密码管理局发布的商用密码随机抽查事项清单是一个非常高明的执法检查手段，既能解决执法部门执法人力不足的难题，又能体现被检查对象的公平性，还能达到法律具备足够的威慑力的效果。而应对这个随时会落下的执法宝剑，列入抽查对象的所有单位只有自动化这一条康庄大道可走，只有自动化实现商密 HTTPS 加密和 WAF 防护，才能从容应对随时随地的各种合规执法检查，才能真正普及应用商用密码来保证我国关键信息基础设施的安全可靠运行。

有诗为证：

随机抽查，真厉害。
公平维护法律尊严。
自动化，从容应对。
合规使用，真有效。

王高华

2024 年 7 月 24 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 173 篇(共 47 万 5 千多字)和英文 68 篇(8 万 4 千多单词)。。