代码签名证书申请和使用的6大注意事项

代码签名证书（CodeSigning）作为软件发行的身份证明和代码保护的重要工具，已经被软件开发商或者发行商经常使用，使用代码签名证书为您需要发布的软件进行数字签名具有重要意义。但在采购或者使用代码签名证书的时候，其实有很多极易被忽视的看似很小实则很重要的问题。

1，新规则下，代码签名证书的使用方式其实不止一种。

自 2023 年 6 月开始，无论是普通的 OV 代码签名还是 EV 代码签名证书，按照相关要求都需要存储在满足相关标准的硬件设备或者环境里。这样导致很多原来使用 pfx 软证书场景的用户不得不改变策略。但其实，环度网信在 2023 年 6 月也同步上线了一款支持代码签名证书云签名的解决方案，用户无需在本地插入硬件也能多人多地同时使用代码签名证书，方案详见环度网信官网。

2，严格监督您的代码签名证书交付方式，防止证书被盗用。

代码签名证书是由全球可信 CA 机构审核签发。在中国，很多 CA 机构都是通过授权环度网信这种本土企业来为用户提供售前售后服务，常见的代码签名证书详见环度网信官网发布的代码签名证书型号列表。因此，代码签名证书交付过程通常有第三方经销商的参与。为了保障客户证书的交付安全，环度网信通常采用的是将空白的硬件 Token 发给客户，然后将证书一次性的提取链接或者提取验证码交付给客户，由客户亲自在自己或者授权的电脑上把代码签名证书提取到空白的 Token 中。这种方式确保了用户才是代码签名证书的第一时间接触人。

如果您在其他服务商那申请到的代码签名证书，是由服务商直接发给您提取好证书的 Token，那么您的服务商已经比您先一步拿到了可以签名的证书，理论上.....这存在被盗用的风险。可能从主观感情上您是信任这个第三方服务商，或者您忽略了这个证书使用的“盲区”，但不得不说，这其实是一个漏洞。环度网信坚持的是“零信任”模式，即只从客观条件上来满足用户才是证书的第一接触人，而不是对用户说“请放心，我们不会偷偷的使用您的证书”这种苍白的保证。

主观的信任，可能带来的是伤害，只有合理的流程才是安全的保障。

3，牢记密码，防止 Token 锁死自毁。

如果您使用的是本地插入 Token 的方式来使用证书，那么请一定牢记您 Token 的设备密码和管理员密码。环度网信在交付客户硬件 Token 的时候，会设置好默认密码一起交付给用户，并建议用户在收到 Token 之后第一时间修改默认密码。但经常有客户忘记自己重新设置过的新密码，这样导致的最坏结果就是 Token 被锁死报废，如果要继续使用，那将不得不再重新申请一个 Token。

4，驱动文件的签名比较特殊。

如果您需要签名的软件是驱动类文件，那么请注意，您不仅仅需要申请一张 EV 代码签名证书，而且还需要通过 WHQL 的方式来获取微软发布的数字签名，方案详见环度网信 WHQL 服务项目。总之，内核驱动文件不再支持使用 EV 代码签名证书直接签名。

5，代码签名证书并不是恶意或者疑似恶意的软件被杀毒软件放行的“通行证”。

很多用户申请代码签名证书，目的是想避免杀毒软件的误报误杀。环度网信在此郑重提醒：代码签名证书并不能让您的软件直接避免杀软的误报误杀。如果您的软件是合法合规，仅仅是被误报为病毒，我们建议您将软件用代码签名证书签名之后提交给杀软厂商申诉。如果您签名的软件本身就是病毒等恶意程序，一旦发现，我们将联合 CA 机构吊销证书并配合相关部门调查。

6，代码签名证书并没有专门的试用版本

“能否先试用一下，如果没问题再正式申请”，这是我们在与客户具体接触中遇到过很多次数的问题。由于代码签名证书的特殊性，在签发之前，CA 机构需要对申请证书的组织单位进行严格的核验，以确保申请证书的单位目前是真实存在、且该单位对申请证书的人员知情并同意其代表单位申请证书。核验完毕之后方可签发代码签名证书。因此，无论您是想试用一下还是正式申请，所需要的流程都是一样的。当然，如果您因为特殊情况在拿到证书后的几天之内想要退订证书，环度网信一般支持 7-30 天内退款，具体情况根据不同的证书型号有所差异。

最后，代码签名证书是一款专业的产品，其申请和使用还有很多细节需要注意，欢迎您咨询环度网信获取更多细节。

关于环度网信：

上海环度信息科技有限公司成立于 2015 年，是 DigiCert、Entrust、GlobalSign、CFCA、SHECA 等国内外 CA 机构授权过的数字证书服务商。业务涵盖 SSL 证书、代码签名证书、文档签名、邮件证书等众多数字证书产品。