

数字证书使用告知书

深圳市电子商务安全证书管理有限公司（简称“SZCA”“深圳CA”）就证书办理及使用的相关风险向用户作如下告知提示：

- 1、办理证书前，请阅读 SZCA 的电子认证业务规则、证书策略，及《电子认证服务协议》，了解证书的用途、应用范围、使用要求及法律风险、法律权利责任。
- 2、申请证书应提供真实准确完整的材料信息。
- 3、如不接受证书或不同意 SZCA 公布证书的，用户应在知悉证书签发或收到证书后当日内向 SZCA 或注册机构提出异议。
- 4、证书有效期内用户信息发生变更应及时通知 SZCA 或注册机构办理证书变更。
- 5、使用证书时请检查证书状态，确保数字证书有效（即证书未过期、未冻结或撤销）。
- 6、证书到期如需使用证书，请在证书有效期届满前 1 个月及时办理证书续期。
- 7、SZCA 签发的数字证书只能用于在网络（Internet/Intranet/Extranet）上标识用户身份、保障电子数据的保密性、完整性和不可抵赖性。数字证书（含电子印章）用于电子签名具有与手写签名、盖章同等的法律效力。数字证书（含电子印章）可在政务办公、公共管理和社会公共服务活动、经济和社会活动等政务、民商事活动中使用，法律禁止使用数据电文、电子签名的领域除外。且不得将证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动，证书策略扩展项含 2.16.156.339.2.1.1.1、或 2.16.156.339.2.1.2.1 的证书不得应用于涉及生命健康、财产权益等高风险活动。
- 8、请安全妥善保管数字证书、私钥及/或其存储设备、密码、或其他激活使用数据，如 UKEY、PIN 码/保护口令、（应用系统）账户密码、OTP 短信验证码、指纹或人脸数据生物特征鉴别数据等，不得以出租、出借、转让、共享等任何方式提供证书给他人使用，否则证书被非法使用或滥用可能会影响您的人身财产安全。如发现前述任何私钥泄露失密情形的，用户应立即终止使用、通知 SZCA 或注册机构。
- 9、证书续期、变更会相应更新证书密钥，旧密钥加密的文件使用新密钥无法解密，用户办理证书续期、变更前，请务必对原证书加密的重要文件进行解密保存。
- 10、实体证书（含 UKEY 证书等），用户在获取实体证书后通过输入 PIN 码可使用数字证书；云证书用户授权同意 SZCA 为用户提供私钥管理服务的，SZCA 将采取必要的验证措施保障数字证书签名密钥由用户控制使用，用户同意通过 PIN 码/保护口令验证、密码验证、手机 OTP 验证、身份证鉴权、银行卡鉴权、电话核身验证、人脸识别或指纹识别等鉴别方式等任一种或几种手段成功鉴别用户身份后在业务应用系统产生的电子签名视为用户实施的电子签名，对用户具有法律约束力，由用户承担相应的法律责任及后果。

- 11、SZCA 承诺按国家法律法规及 CPS 等的规定，采取数据加密、访问控制等信息安全保障措施严格保护用户的个人信息安全，并将依法保存用户数字证书相关信息至证书失效后至少 5 年。除以下情形外，不对外提供用户信息：（1）用户事先同意或授权的；（2）保护国家国防、安全、卫生等国家公共安全及利益所要求的，或紧急情况下为保护自然人的生命健康和财产安全所必需；（3）根据适用的法律法规、法律程序的要求司法机关、政府部门（含监管机构）依程序要求提供的；（4）其他法定应当提供用户信息的。
- 12、如 SZCA 受用户委托提供证书密钥管理服务的，SZCA 应将用户密钥存储在经国家密码管理局批准的密码模块产品，并采取技术措施保证数字证书由用户专有控制使用，否则应承担相应的法律责任，赔偿用户损失。
- 13、如您委托第三方生成、保管、管理证书密钥的，在您授权第三方提供密钥管理服务的同时，请确保第三方通过经国家密码管理部门批准认可的安全密码产品生成与托管您的密钥，且有有效的管理与技术措施保障证书由用户专有控制使用，且应定期检查第三方授权使用证书情况，防范证书非授权使用风险。

SZCA 的电子认证业务规则、证书策略，及《电子认证服务协议》访问地址：
<https://www.szca.com>

SZCA 联系方式：

400-112-3838、kfzz@szca.com.cn

深圳市电子商务安全证书管理有限公司