

深圳市电子商务安全证书管理有限公司（简称 SZCA、深圳 CA）作为（电子政务）电子认证服务机构，根据国家相关法律法规，为用户提供数字证书申请、签发、更新、变更、补办、撤销等证书生命周期管理服务。为明确用户（又称证书申请人、证书持有人、订户）、SZCA（含注册机构）在数字证书办理、应用方面的法律权利和责任，双方本着平等、自愿的原则达成本协议。本协议内容源自深圳 CA 的电子认证业务规则（简称 CPS）、证书策略（简称 CP），如出现内容抵触，以深圳 CA 官网（<https://www.szca.com>）公告的 CPS、CP 内容为准。本协议未尽事宜，按照深圳 CA 的 CPS、CP 执行。

一、用户的权利与责任

- 1、用户申请、使用 SZCA 数字证书前，应阅读 SZCA 的 CPS、CP 及本协议了解数字证书的功能、应用范围、使用要求、用户的权利义务及责任范围。
- 2、申请数字证书时，用户须按照 SZCA 的业务办理要求，提供真实准确完整有效的证书申请资料、信息；申请电子印章的，应提供与印章管理有关法律法规规定的印模规格、与公安机关印章管理部门备案的印模信息（含实物印章图像）样式规格一致的印模图像，或授权 SZCA 从公安机关等相关政府部门的公章管理系统获取印模信息；否则，由此造成的法律后果，由用户承担。
- 3、用户及其授权代理人知悉并同意授权：（1）为向用户提供数字证书及/或电子印章（如涉及，下同）制作签发、管理及查询验证服务，SZCA 收集、使用、保存证书申请资料、信息，包括用户、用户委托的授权代理人、法定代表人/负责人（机构用户适用）姓名、身份证件号码、手机号码（和/或银行预留手机号码及银行卡号）、联系地址、身份证件、人脸识别信息，并授权 SZCA 向第三方机构核验、或通过第三方合作机构向具备合法资质或合法数据来源的其他第三方机构核验用户个人信息（含提供个人信息），同意上述第三方机构、第三方合作机构向 SZCA 及用户提供核验服务（含提供核验结果信息）；（2）如通过 SZCA 注册机构、合作机构向 SZCA 申请证书，用户授权并同意其收集及向 SZCA 提供前述用户个人信息，同意 SZCA 向其提供并通过其向用户提供证书申请处理结果信息；（3）为电子认证服务主管部门向用户提供数字证书查询验证服务，用户授权 SZCA 向前述主管部门提供用户的身份信息、联系信息、证书信息，及授权前述主管部门获取使用用户的前述个人信息。
- 4、用户如不同意 SZCA 发布数字证书至信息库、不接受证书，应证书申请或获取交付时向深圳 CA 提出异议；否则视为接受证书、同意发布证书。
- 5、数字证书（含电子印章）可用于标识识别用户身份，用于电子签名具有与手写签名、盖章同等的法律效力。用户应合法正当使用数字证书，用户可在政务办公、公共管理和社会公共服务活动、经济和社会活动等政务、民商事活动中使用数字证书（含电子印章），法律禁止使用数据电文、电子签名的领域除外。用户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，因违法使用或超范围应用造成的后果由用户自行承担。
- 6、实体证书（如 UKEY 证书），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。
- 7、用户应妥善保管数字证书、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、（业务应用系统）账户密码、OTP 短信验证码、指纹或人脸数据相关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，如因用户保管不善，或提供他人使用造成的证书、私钥及其存储设备、密码或其他激活使用数据泄露、毁损、遗失、被篡改、伪造、冒用、盗用的，造成的损失由用户自行承担。如发现任何私钥泄露失密情形的，用户应立即终止证书使用、通知 SZCA 或注册机构。
- 8、用户应使用证书状态查询服务检查证书状态，并应在数字证书有效时（即证书未过期、未冻结或撤销）使用证书，否则由此产生的损失由用户承担。
- 9、证书所含的用户信息（证书主题名称或使用者的用户名称/姓名、单位、部门、地址）发生变更的，应及时通知 SZCA 或注册机构、办理证书变更。
- 10、证书到期如需续用的，须在证书有效期届满前 1 个月内通过在线方式自助续期更新、或向 SZCA、注册机构申请办理证书续期更新。
- 11、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。
- 12、有下列情况之一的，由用户承担责任：（1）用户未提供真实准确完整的申请资料，造成相关各方损失的；（2）因用户转让、出借或出租证书而产生损失的；（3）用户丢失介质，或不慎将证书密钥泄露造成证书被盗用、冒用、伪造或者篡改造成相关各方损失的；（4）因用户信息变化且未通知 SZCA 更新证书信息而造成损失的；（5）用户违反约定的证书范围、用途、条件及期限不当使用或滥用数字证书。

二、SZCA 的权利与责任

- 1、SZCA 应公布证书对应的电子认证业务规则与证书策略，并保证用户、依赖方可访问、获取电子认证业务规则和证书策略。
- 2、SZCA 提供证书申请、签发、更新、变更、补办、挂起、撤销、发布、加密封恢复等证书生命周期管理服务，及数字证书及其状态的查询、验证服务。
- 3、SZCA 应尽合理努力保证签发的数字证书安全可靠。如因法规政策、技术标准变化，SZCA 应及时更新证书版本格式、密码算法及协议、及升级电子认证服务系统及其配套支持的软硬件设备，并对有效期内的证书提供更新、变更服务。
- 4、为保证数字证书的安全应用，SZCA 在证书即将过期、证书密码算法不安全等情形下将通过短信、邮件或服务消息等方式通知提醒用户办理证书续期、变更。
- 5、SZCA、注册机构应遵照法律法规、CPS 及相关服务规范规定的流程与要求受理处理用户的证书申请，审核申请人身份，并在规定时间内制作发放证书。
- 6、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证书由用户专有控制使用。
- 7、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。
- 8、有下列情形之一的，SZCA 有权撤销用户的数字证书：（1）用户申请证书时未提供真实准确完整有效的信息；（2）用户未按规定缴纳证书服务费用；（3）证书对应的私钥泄露、被盗用冒用或出现其他证书的安全性不能得到保证的情况；（4）用户不能履行或违反相关法律法规、CPS、CP 和本协议所规定的责任和义务；（5）法律、法规规定的其他情形。
- 9、因 SZCA 原因造成用户损失的，SZCA 将按照电子认证业务规则进行赔偿。以下损失不在赔偿之列：（1）任何间接的收入、收益、利润损失、信誉或商誉损害、任何商机或契机损失；（2）由上述损失相应生成或附带引起的损失或损害。若 SZCA 已按照法律法规、CPS 提供服务的仍有损失产生，SZCA 将不承担赔偿责任。
- 10、以下情况造成的数字证书无法签发、签发错误或签发延迟的，或其他证书服务暂停、终止的，SZCA 不承担损害赔偿赔偿责任：（1）不可抗力；（2）计算机、系统、网络、软硬件设备故障等因非 SZCA 原因造成的意外事件，包括但不限于：关联单位如电力、电信、通讯部门而致；黑客、病毒、木马、恶意程序攻击；上游数据源、密钥管理系统、网络故障。
- 11、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。用户将数字证书用于其他用途引起的一切法律后果，SZCA 不承担任何法律责任。

三、协议的生效、变更与终止

- 1、本协议自申请人签署（签署方式含手写签名、盖章或在线点击、勾选等电子方式）本协议、同意递交证书申请或使用数字证书时生效，至证书失效终止之日止。
- 2、本协议如有修订，SZCA 会通过网站或电子邮件等方式进行公告通知，更新后的协议自动替代原协议；如用户不同意更新后的协议，应停止使用数字证书、通知 SZCA 撤销证书；否则，如未提出异议的，视为同意新协议。

四、法律适用与争议解决

- 1、本协议的成立、生效、履行、解释、争议解决，均适用中华人民共和国法律。
- 2、对本协议的生效或履行发生任何争议时，应协商解决。协商不成的，任何一方可向 SZCA 住所地人民法院提起诉讼。