电子认证服务协议

深圳市电子商务安全证书管理有限公司（简称 SZCA、深圳 CA）作为电子认证服务机构、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、审核、签发和管理等电子认证服务、电子政务电子认证服务。为保障用户（又称证书持有人、数字证书申请人）和 SZCA 各方的合法权益，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，如出现内容抵触，以深圳 CA 的电子认证业务规则（简称 SZCA CPS）为准，有关详情请浏览 https://www.szca.com。

一、用户的权利与责任

1、 用户申请 SZCA 数字证书前，应阅读 SZCA 的 CPS、CP 了解数字证书的功能、应用范围、各方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，提供真实准确完整的证书申请资料、信息；申请制作电子印章的，应提供或授权 SZCA 从公安机关公章治安管理信息系统获取备案的印模信息，并保证提供的印模信息与在公安机关印章管理部门备案的印模信息（包含实物印章图像）样式规格一致；否则，由此造成的法律后果，由用户承担。

3、 **用户知悉并同意授权：（1）为向用户提供数字证书（含电子印章，如涉及，下同）制作签发、管理及查询验证服务，SZCA 收集、使用、保存您的信息，包括姓名、身份证号、手机号、联系地址、身份证件、及人脸图片、营业执照；（2）SZCA 通过第三方机构查询、验证由第三方合作机构合法收集、加工、整理产生且核实您提交的个人信息所必需的信息；（3）SZCA 通过第三方合作机构向其他具备合法资质或合法数据来源的第三方收集、查询、整理本人信息，并同意上述合法资质的第三方向 SZCA、第三方机构、第三方合作机构提供核实和验证本人信息的服务。**

4、 用户获得数字证书后应及时检查确认数字证书的内容（证书主体名称或使用者项）和功能，如有问题应于 2 个工作日内提出异议，如无异议则视为接受证书。

5、 用户如不同意 SZCA 发布数字证书至信息库的，应在申请证书时提出，否则视为同意 SZCA 发布证书。

6、 用户应妥善保管并依法正当安全使用 SZCA 签发的数字证书对应的私钥及其存储设备、激活使用相关数据，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，不得出租、出借、转让、提供他人使用，如因用户保管不善、提供、泄漏或交付他人造成的私钥及其存储设备泄露、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。

7、 **用户应在数字证书有效时（即证书未过期、未被挂起或撤销）使用证书，否则由此产生的损失由用户承担。**

8、 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或向 SZCA 或注册机构申请证书续期、更新。

9、 证书所含的用户信息（证书主体名称或使用者项的用户名称/姓名、单位、部门、地址）发生变更的，应及时通知 SZCA 或注册机构、办理证书变更或撤销。

10、 如发现数字证书密钥或其存储设备、激活使用数据已经或可能已经毁损、泄露、遗失等任何私钥泄露失密情形的，用户应立即终止使用、通知 SZCA、申请撤销证书。

11、 **数字证书（含电子印章）具有与手写签名、实物盖章同等的法律效力，由此产生的电子签名（含电子签章）对用户具有法律约束力。用户可在政务办公、公共管理和社会公共服务活动、经济和社会活动等行政管理、民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。**

12、 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、刷脸认证或指纹识别的生物鉴别方式等任何其中的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。

13、 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的一切损失的；（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）因用户信息发生变化且未及时通知 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 遵照法律法规、深圳 CA 电子认证业务规则及相关管理规范规定的流程签发证书，提供证书更新、变更、补办、挂起、撤销、发布、加密密钥恢复等证书生命周期管理服务，并在数字证书有效期内提供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，可有效防止伪造、篡改、破解。如因法律法规、政策、技术标准变化，SZCA 应及时更新证书版本与格式、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知提醒用户办理证书续期、变更。

5、 SZCA 或注册机构负责受理用户证书申请，审核申请人身份，审查证书申请，并在规定的时间内制作发放证书，处理用户的证书更新、变更、撤销、补办等请求。

6、 SZCA 承诺按国家法律法规，及 CPS 等的规定，严格保护用户的个人信息安全，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。

7、 有下列情形之一的，SZCA 有权撤销用户的数字证书：（1）用户申请证书时提供不真实信息；（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。

8、 因 SZCA 原因造成用户损失的，SZCA 将按照深圳 CA 的电子认证业务规则进行赔偿。以下损失不在赔偿之列：(1)任何直接或间接的收入、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。

9、 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，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。

10、 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、加盖实物印章或网络页面点击确认、勾选等数据电文方式）本协议、同意递交证书申请或实际使用数字证书之时生效，至证书失效终止之日止。**

2、 本协议如有修订，SZCA 会以网站或电子邮件等方式进行公告，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。

3、 本协议未尽事宜，按照深圳 CA 的电子认证业务规则执行。本协议与深圳 CA 的电子认证业务规则、深圳 CA 个人信息保护政策、个人信息授权书等共同组成完整的数字证书服务协议。

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、 双方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，任何一方均可提请深圳仲裁委员会按照仲裁规则进行仲裁。仲裁裁决是终局的，对双方均具有约束力。