

西部安全认证中心有限责任公司

电子认证服务协议

尊敬的订户：

感谢您选择西部安全认证中心有限责任公司（以下简称“西部 CA”或“本公司”）提供的电子认证服务。西部 CA 是工业和信息化部批准设立电子认证服务机构和国家密码管理局批准设立电子政务电子认证服务机构，遵照《中华人民共和国电子签名法》为用户提供数字证书相关的电子认证服务。

为明确双方的权利和义务，根据《中华人民共和国电子签名法》《电子认证服务管理办法》《电子认证业务规则规范》等相关法律法规和标准要求，西部 CA 与证书订户（以下简称“订户”或“您”）就数字证书申请、使用等事宜达成如下协议，双方共同遵守执行。

重要提示：

1. 在申请使用西部 CA 签发的数字证书之前，您必须先阅读本《电子认证服务协议》（以下简称“本协议”）及《西部安全认证中心有限责任公司电子认证业务规则》（以下简称“CPS”）。
2. 您根据本公司的业务流程提交数字证书申请信息（无论该信息是通过填写申请单、在线互动操作，还是其他方式形成），须通过可靠的方式（如强制阅读并勾选、短信验证、手写签名/盖章、手写板签名、手机电子签名、数字证书签名等）对信息进行确认，方视为同意全部条款。
3. 本协议将于您向西部 CA 递交申请并获得审核批准后生效；线上电子确认版本、线下纸质签字盖章版本具有同等法律效力。

第一条 定义与解释

除非本协议另有约定，下列词语在本协议中具有以下含义：

- 1.1 数字证书：是西部 CA 签发的包含数字证书使用者身份信息和公开密钥的电子文件，用于在网络活动中标识订户身份并验证其电子签名。
- 1.2 电子认证业务规则（CPS）：是西部 CA 对外公布的、详细说明数字证书签发和管理规则的规范性文件，作为本协议不可分割的组成部分。
- 1.3 订户：指向西部 CA 申请数字证书并被颁发证书的自然、法人或其他组织。
- 1.4 依赖方：指基于对数字证书或者电子签名的信赖从事有关活动的个人或组织。
- 1.5 私钥：非对称密码算法中由订户独有的不公开密钥，用于制作电子签名。
- 1.6 公钥：非对称密码算法中可公开的密钥，用于验证电子签名。

第二条 协议的组成与效力

2.1 本协议由以下文件共同组成，具有同等法律效力：

- （1）本《电子认证服务协议》正文；
- （2）《数字证书订户告知书》；
- （3）《西部安全认证中心有限责任公司电子认证业务规则（CPS）》；
- （4）《数字证书申请单（或申请信息）》及相关身份证明材料。

2.2 上述文件内容如有不一致之处，以本协议正文为准；本协议未约定的事项，以 CPS 为准。

2.3 CPS 已在西部 CA 官方网站（www.cwca.com.cn）公布，订户应在申请证书前仔细阅读。订户申请证书的行为，视为已阅读并同意 CPS 的全部内容。

2.4 西部 CA 有权根据法律法规变化或业务需要修改本协议及 CPS，修改后的内容将在官方网站公告。订户如不接受修改后的协议，可于公告发布之日起十五日内申请吊销证书；逾期未提出异议或继续使用证书的，视为同意接受修订后的协议。

第三条 证书的申请与颁发

3.1 订户应根据自身需求选择适当的证书类型（可向西部 CA 咨询），西部 CA 提供不同种类的数字证书，包括但不限于个人高等级证书、个人基础级证书、机构高等级证书、机构基础级证

书。

3.2 订户在申请数字证书时，应按照西部 CA 的业务规程办理手续，并依法提供真实、完整、准确的身份信息及证明材料。

3.3 订户向西部 CA 提交证书申请后，即成为本协议项下的证书订户。西部 CA 对证书申请进行审核，并有权根据 CPS 及本协议的规定决定是否批准。

3.4 订户在获得数字证书时，应及时验证证书所载信息是否正确。如无异议，视为接受证书；如有异议，应立即通知西部 CA。

第四条 服务内容西部 CA 为订户提供以下电子认证服务：

4.1 证书生命周期管理服务：包括证书申请、签发、接受、续期、密钥更新、变更、冻结、解冻、吊销等。

4.2 证书状态查询服务：通过证书撤销列表（CRL）和在线证书状态协议（OCSP）提供证书状态查询，服务可用率不低于 99%。

4.3 电子签名验证服务：根据订户或依赖方的请求，对电子签名进行验证并出具验证报告（如有需要）。

4.4 其他服务：双方约定的其他电子认证相关服务。

第五条 服务收费

5.1 西部 CA 提供不同种类的证书，订户应根据自身需求自行选择证书种类。

5.2 订户应在申请时向西部 CA 交付相应的数字证书使用服务费用，除非西部 CA 以书面形式予以豁免。

5.3 具体收费标准已在西部 CA 官方网站（www.cwca.com.cn）及服务网点公示。收费项目包括但不限于：证书签发费、证书更新 / 续期费、证书吊销费、介质费、证书状态查询服务费、电子签名验证报告费等。

5.4 订户不得与其他第三方发生纠纷为理由拒绝支付或未在规定时间内支付应付给西部 CA 的数字证书使用服务费用。对于拒绝支付或逾期支付服务费用的订户，西部 CA 有权停止相关服务，因此造成的任何经济损失，西部 CA 不承担任何责任。

5.5 如订户系通过第三方机构（如电子合同签署平台、应用集成商等）使用本证书，该第三方机构是否另行向订户收费，由订户与第三方机构自行协商确定，与西部 CA 无关。

第六条 订户的权利

6.1 知情权：有权了解本协议、CPS 及告知书所载全部内容。

6.2 使用权利：有权按照 CPS 及本协议的规定，在证书有效期内合法使用所申请的数字证书。

6.3 吊销权利：在证书有效期内，有权向西部 CA 申请吊销数字证书。

6.4 争议处理权利：有权按照本协议约定的争议解决方式，就电子认证服务相关事项提出异议或索赔。

6.5 信息查询权利：有权通过西部 CA 官方网站查询证书状态、证书撤销列表（CRL）及证书相关信息。

第七条 订户的义务

7.1 信息真实义务：申请数字证书时，应当提供真实、完整、准确的身份信息及相关证明材料。上述信息发生变更时，应在变更之日起 2 日内通知西部 CA。如因故意或过失未提供真实、完整、准确的信息，或提供非法获取的相关信息及资料，或发生变更后未在规定时限内通知西部 CA，导致签发证书错误或造成相关各方损失的，由订户承担全部责任。

7.2 私钥保管义务：订户选择自行持有私钥，应当妥善保管数字证书私钥及相关激活数据（如密码、PIN 码等），采取必要的安全措施防止私钥丢失、泄露、被篡改或未经授权使用。西部 CA 不承担因订户私钥保管问题造成损失的赔偿责任，除非订户能够合法、充分地证明该问题产生的全部责任在于西部 CA。

7.3 合法使用义务：不得将所获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。仅限在申请时预定的目的和应用范围内使用证书，否则西部 CA 不承担任何由此产生的责任和义务。

7.4 及时报告义务：一旦发现私钥可能泄露或已泄露、证书信息有误、证书被他人冒用等异常情形，应当立即停止使用证书，并在 24 小时内向西部 CA 报告，申请吊销证书。因未及时报告而给西部 CA、其他订户、依赖方或其他相关方造成损失的，订户应承担相应的赔偿责任。

7.5 接受审查义务：配合西部 CA 在证书申请、续期、变更、吊销等环节依法开展的身份查验和材料审查。

7.6 付费义务：应当按照西部 CA 公布的收费标准，按时足额缴纳证书服务相关费用。

7.7 到期更新义务：为保证安全，西部 CA 所签发证书具有有效期。证书到期后需要继续使用的，订户应在证书有效期到期前 30 日内向西部 CA 提出申请进行证书密钥更新。西部 CA 将对过期证书进行失效处理，对过期证书不承担任何安全保障义务。

7.8 个人信息提供与授权义务：订户同意向西部 CA 提交办理数字证书所必要的身份信息（个人用户包括姓名、身份证号、实名手机号、电子邮箱、住址、所在单位信息；机构用户包括机构名称、统一社会信用代码证号、注册地址、单位电话、法定代表人姓名、法定代表人身份证号及经办人姓名、身份证号、实名手机号），并授权西部 CA 向其第三方合作机构传递前述信息用于核实用户身份。

第八条 西部 CA 的权利

8.1 西部 CA 有权根据 CPS 及本协议的规定，对订户的证书申请进行审核，并自主决定是否批准。

8.2 订户拒绝支付或逾期支付服务费用时，西部 CA 有权停止相关服务。

8.3 西部 CA 有权根据法律法规变化或业务需要修改本协议及 CPS，修改后的内容将在官方网站公告。

8.4 西部 CA 对本协议享有最终解释权。

第九条 西部 CA 的义务

9.1 提供服务义务：按照公布的 CPS 和本协议，向订户提供数字证书申请、签发、发布、查询、吊销等生命周期管理服务。

9.2 身份查验义务：对证书申请人的身份进行查验，对申请材料进行审查。身份查验义务未委托给外部机构（非属同一法人主体的机构视为外部机构）。

9.3 保密义务：对证书申请过程中获得的订户信息予以保密，不做超出电子认证业务范围的使用。根据法律法规、强制性的行政执法或司法要求必须提供订户身份信息的情况除外。

9.4 持续服务义务：保证提供的证书状态查询服务连续不间断，服务可用率不低于 99%。

9.5 信息保存义务：妥善保存与电子认证相关的信息，保存期限至少为证书失效后 5 年。

9.6 赔偿责任：在现有的技术条件下，由西部 CA 签发的数字证书能够有效防止被伪造、篡改。如经确认确属西部 CA 责任，西部 CA 按照 CPS 规定的责任范围和赔付标准承担赔偿责任。

9.7 安全告知义务：向订户提供关于签名私钥及激活数据安全使用的指导与建议。

第十条 签名私钥的存储方式及安全要求

10.1 存储方式：订户选择由自行持有私钥。私钥存储在订户持有的符合国家安全标准的密码模块（如智能密码钥匙 UKEY）中。

10.2 订户安全义务：

将私钥存储在符合国家密码管理局要求的硬件密码模块中；

妥善保管硬件密码模块及激活密码，不得告知他人；

初次使用时立即修改初始密码，密码应具备足够复杂度（建议 8 位以上，含数字、字母、特殊符号的组合）；

不得将硬件密码模块转借、转让给他人使用；

如硬件密码模块遗失、损坏或密码泄露，应立即向西部 CA 申请吊销证书。

10.3 西部 CA 责任：西部 CA 不承担因订户私钥保管问题造成损失的赔偿责任，除非订户能够合法、充分地证明该问题产生的全部责任在于西部 CA。

第十一条 电子签名的使用条件与限制

11.1 适用场景：

高等级电子签名认证证书：适用于涉及生命健康、财产权益等高风险场景的电子签名活动。

基础级电子签名认证证书：适用于除高等级证书规定场景外的其他电子签名场景。

11.2 禁止使用的场景：

涉及人身关系的，如婚姻、收养、继承等；

涉及停止公共事业服务的，如停止供水、供热、供气等；

法律、行政法规规定的其他不适用电子签名的应用场景或类型；

国家法律法规禁止的活动。

11.3 级别使用限制：涉及生命健康、财产权益等高风险活动，禁止使用基础级电子签名认证证书。

11.4 电子签名的法律效力：根据《中华人民共和国电子签名法》的规定，可靠的电子签名与手写签名或者盖章具有同等的法律效力。订户使用本证书进行的电子签名，在符合法律规定的条件下，将被视为订户本人的真实意思表示。

第十二条 责任划分与免责条款

12.1 订户的责任：

因提供虚假、不完整、不准确的信息或未及时通知信息变更而造成的损失，由订户承担；

因私钥保管不善导致他人冒用签名而造成的损失，由订户承担；

将证书用于非许可目的或违法违规用途而造成的损失，由订户承担；

未及时报告私钥泄露等安全事件而造成的损失，由订户承担；

因未按时支付服务费用导致服务中断而造成的损失，由订户承担。

12.2 西部 CA 的责任：

经确认确属西部 CA 责任（如因西部 CA 系统安全问题导致证书被伪造、篡改），西部 CA 按照 CPS 规定的责任范围和赔付标准承担赔偿责任。

西部 CA 的赔偿责任以 CPS 之规定为准。

12.3 免责条款：西部 CA 不承担因以下原因造成的损失赔偿责任：

- 订户不合法、不科学、不合理、不规范地使用数字证书；
- 因不可抗力事件（如自然灾害、战争、恐怖袭击等）导致暂停、终止全部或部分证书服务；
- 因订户的网络、主机、操作系统或其他软硬件环境存在安全漏洞导致的安全事故；
- 因黑客攻击或任何第三方的违法犯罪行为等不可归因于西部 CA 自身技术或管理原因造成的损失；
- 证书到期后订户未及时更新，西部 CA 对过期证书不承担任何安全保障义务；
- 西部 CA 已谨慎遵循并履行了国家法律法规及 CPS 之规定，视为西部 CA 不存在过错，无须对因此产生的损失承担赔偿责任。

12.4 本协议的签署效力：本协议通过强制阅读并勾选确认、短信验证签署、手写签名/盖章任一方式签署，均与手写签名或盖章具有同等法律效力。

第十三条 信息安全保障

西部 CA 采取以下安全保障措施，保障电子认证服务的安全性、可靠性和连续性：

13.1 系统安全：电子认证服务系统通过国家密码管理局审查，符合 GB/T 25056《信息安全技术 证书认证系统密码及其相关安全技术规范》的要求。

13.2 密码模块安全：使用的密码模块符合 GB/T 37092《信息安全技术 密码模块安全要求》。

13.3 物理环境安全：机房实施分区管理与访问控制，部署门禁、视频监控、入侵检测等安防

系统。

13.4 网络安全：配置防火墙、Web 应用防火墙、入侵检测系统等网络安全防护措施，实施网络访问白名单机制。

13.5 人员管理：建立可信角色管理制度，实施职责分离，关键操作实行双人控制。

13.6 审计与监控：对系统操作、证书生命周期关键过程、物理访问等进行全面日志记录，定期审计。

13.7 灾备与业务连续性：实施异地备份，制定灾难恢复预案，定期开展应急演练。

第十四条 个人信息保护

14.1 西部 CA 承诺对证书申请过程中获得的订户个人信息予以保密，不做超出电子认证业务范围的使用。

14.2 西部 CA 将按照《中华人民共和国个人信息保护法》及 GB/T 35273《信息安全技术 个人信息安全规范》的要求，采取有效措施保护订户个人信息安全。

14.3 根据法律法规、强制性的行政执法或司法要求必须提供订户身份信息的情况下，西部 CA 将依据要求对外共享、转让、公开披露相关信息。

14.4 经办人授权西部 CA 采集个人信息用于身份验证、数字证书办理以及监管部门的数据收集或验证。

第十五条 协议的期限与终止

15.1 线上版本自订户在线点击确认之日生效；线下纸质版本自双方签字盖章完成之日生效。

15.2 本协议在数字证书有效期内持续有效。证书到期后未续期的，本协议自动终止。

15.3 订户申请吊销证书并经西部 CA 处理后，本协议终止。

15.4 西部 CA 根据本协议约定停止服务的，本协议终止。

15.5 协议终止后，西部 CA 对过期证书或已吊销证书不承担任何安全保障义务。

第十六条 争议解决

16.1 本协议之效力、解释、变更、执行与争议解决均适用中华人民共和国法律。

16.2 因本协议产生之争议，双方应首先友好协商解决。

16.3 协商不成的，双方同意将争议提交银川仲裁委员会，按照该会申请仲裁时现行有效的仲裁规则在银川进行仲裁。仲裁裁决是终局的，对双方均有约束力。

第十七条 其他条款

17.1 如本协议中的任何条款无论因何种原因完全或部分无效或不可执行，本协议的其余条款仍应有效并具有约束力。

17.2 本协议中的标题仅为方便阅读而设，不影响本协议条款的解释。

17.3 西部 CA 对本协议享有最终解释权。

17.4 本协议一式两份，西部 CA 与订户各执一份，线上电子协议留存电子档案，具有同等法律效力。

第十八条 订户确认声明本人/本公司确认：

1.已仔细阅读并充分理解本《电子认证服务协议》及《数字证书订户告知书》的全部内容，知晓并同意接受上述约定。

2.已仔细阅读并充分理解《西部安全认证中心有限责任公司电子认证业务规则（CPS）》，知晓 CPS 作为本协议不可分割的组成部分。

3.本证书系直接向西部 CA 申请取得。

4.本人/本公司使用第三方服务（如电子合同签署）时涉及的数字证书费用及约定，与西部 CA 无关，由本人/本公司与第三方自行确定。

5.自愿向西部 CA 申请办理数字证书，并承诺遵守本协议及 CPS 的全部约定。

订户签署区（按需勾选对应类型填写）

☐ 机构单位证书（二选一签署）

1.法定代表人直接签署

机构全称（加盖公章）：_____

法定代表人姓名/手写签名：_____

申请办理日期：____年____月____日

2.经办人代办签署

机构全称（加盖公章）：_____

经办人身份证号：_____

经办人姓名/手写签名：_____

申请办理日期：____年____月____日

☐ 个人自然人证书

姓名/手写签名：_____

联系电话：_____

申请办理日期：____年____月____日

二、西部安全认证中心有限公司

公司盖章：

受理日期：____年____月____日

