

西部安全认证中心有限责任公司

数字证书订户告知书

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。为保障您的合法全文权益，根据《中华人民共和国电子签名法》《电子认证服务管理办法》及《电子认证业务规则规范》等相关法律法规和标准要求，在您申请数字证书前，本公司特向您告知以下重要事项。请您仔细阅读并充分理解本告知书全部内容，确认知晓并同意后，再继续办理证书申请手续。

一、订户的权利和义务

（一）订户的权利

知情权：有权了解本公司电子认证业务规则（CPS）及本告知书所载全部内容。

使用权利：有权按照本公司公布的 CPS 及证书策略的规定，在证书有效期内合法使用所申请的数字证书。

撤销权利：在证书有效期内，有权向本公司（RA）申请撤销数字证书。

争议处理权利：有权按照本公司与订户签订的服务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。

信息查询权利：有权通过本公司官方网站（www.cwca.com.cn）查询证书状态、证书撤销列表（CRL）及本公司相关信息。

（二）订户的义务

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，并在上述信息发生变更时及时通知本公司。

私钥保管义务：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。

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。

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 小时内向本公司报告，申请撤销证书。

接受审查义务：配合本公司在证书申请、续期、变更、撤销等环节依法开展的身份查验和材料审查。

付费义务：应当按照本公司公布的收费标准，按时足额缴纳证书服务相关费用。

知情确认义务：订户在提交证书申请前，已通过官方网站、客服咨询、注册机构公示等途径充分了解本公司的服务项目、收费标准及 CPS 全部内容。订户申请证书的行为，视为对上述内容已知悉并同意接受。

二、服务收费的项目和标准

西部 CA 提供的服务项目包括证书服务费用和证书 KEY 补办费用，其中证书服务包括新办、更新/续期服务，针对证书撤销、证书状态查询服务不进行收费，具体收费标准如下：

首把 KEY：首次新办、续费延期、证书信息变更不进行收费；

多把 KEY：首次新办 300 元/年（含 KEY）、续费延期 150 元/年（含 KEY）；

CA 锁丢失损坏补办 30 元/个。

三、电子签名认证证书、电子签名的使用条件

（一）数字证书的适用场景

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。

（二）数字证书的使用限制

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。

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。

（三）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。您使用本证书进行的电子签名，在符合法律规定的条件下，将被视为您本人的真实意思表示。

四、信息安全保障措施

本公司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：

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。

密码模块安全：使用的密码模块符合现行技术标准。

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，配备温湿度控制、电力保障、消防联动等环境保障措施。

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。

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。

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。

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，保障业务连续性。

五、CA 和订户的责任划分

（一）本公司的责任

按照公布的 CPS 和证书策略，向订户提供数字证书申请、签发、发布、查询、撤销等生命周期管理服务。

对证书申请人的身份进行查验，对申请材料进行审查，确保身份查验义务未委托给外部机构。

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%。

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。

按照本公司在 CPS 中承诺的责任范围和赔付标准，承担相应赔偿责任。

（二）订户的责任

保证在申请数字证书时提供的身份信息及相关证明材料真实、完整、准确，并在信息变更时及时通知本公司。

妥善保管数字证书私钥及相关激活数据，防止丢失、泄露或被未授权使用。

仅在本公司公布的适用场景和使用条件下使用数字证书，不得超范围使用。

不得将数字证书用于任何违法违规、违背公序良俗的用途。

发现私钥泄露、证书信息错误等安全事件时，立即停止使用并及时报告。

因未履行上述义务导致的一切法律后果和损失，由订户自行承担。

六、订户签名私钥的存储方式及安全要求

（一）私钥存储方式

本公司支持以下两种私钥存储方式，具体以您申请证书时选择的类型为准：

存储方式	说明
订户自行持有	私钥存储在订户持有的符合国家安全标准的密码模块（如智能密码匙 UKEY）中
本公司托管	私钥由本公司产生并加密保存，仅在获得订户明确授权后使用

（二）私钥安全要求

如您选择自行持有私钥，请遵守以下安全要求：

将私钥存储在符合国家密码管理局要求的硬件密码模块（如 UKEY）中。

妥善保管 UKEY 及激活密码，不得告知他人。

初次使用 UKEY 时，请立即修改初始密码，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 UKEY 转借、转让给他人使用。

如 UKEY 遗失、损坏或密码泄露，应立即向本公司申请撤销证书。

如您选择由本公司托管私钥，请知悉以下安全保障措施：

本公司仅在获得您书面授权（或同等效力的电子授权）的情况下保存您的签名私钥。签名私钥以加密形式存储，存储条件符合国家相关安全标准。

每次使用签名私钥前，必须获得您的明确授权，并记录授权信息。

所有涉及签名私钥的操作均有完整、可追溯的记录，保存期限不少于证书失效后 5 年。

机构证书签名私钥的使用，须设置法定代表人或受托人作为授权主体。

七、禁止性使用声明

您不得将所获数字证书用于以下任何用途或活动：

任何违反中华人民共和国法律法规的用途或活动；

任何违背公序良俗的用途或活动；

侵害国家利益、社会公共利益的活动；

侵害第三方合法权益（包括但不限于知识产权、商业秘密、个人信息权益等）的活动；

传播病毒、木马或其他恶意代码；

进行任何形式的网络攻击、入侵、干扰；

法律、行政法规及本公司 CPS 中明确禁止的其他用途。因违反上述禁止性声明而产生的一切法律后果和损失，由您自行承担，本公司有权立即撤销相关证书并依法向有关部门报告。

八、其他重要提示

CPS 查阅：本公司的《电子认证业务规则》（CPS）及《电子认证业务规则》已在官方网站（www.cwca.com.cn）公布，详细说明了证书使用的完整规则、各方责任范围、免责条款、赔偿责任等内容，需要您在接受证书前仔细阅读。

服务协议签署：在您确认接受本告知书内容并完成身份查验后，本公司将与您签订正式的《电子认证服务协议》，明确双方的权利义务，该协议将作为双方争议解决的主要依据。

九、订户确认声明

本人/本公司已仔细阅读并充分理解本《数字证书订户告知书》第 1 至第 8 章的全部内容(包括但不限于收费标准、权利义务、责任划分、私钥保管要求及禁止性用途等), 知晓并同意接受上述告知事项, 现自愿向西部 CA 申请办理数字证书。

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