沃通存证型证书策略

版本：V1.0.0

发布日期：2026 年 10 月 25 日

生效日期：2026 年 10 月 25 日

沃通电子认证服务有限公司

Copyright© WoTrus CA Limited

版本控制表

版本	状态	修订说明	审核/批准人	生效时间
V1.0.0	版本发布	首次建立《沃通存证型证书策略》正文，明确 CP3 策略边界、证书类型、对象标识符、适用 CPS、用途限制、状态服务、法律责任和发布管理要求。	沃通安全策略委员会	2026 年 10 月 25 日

声明

本 CP 全部或者部分支持下列标准和规范：

- GB/T 26855-2011《信息安全技术 公钥基础设施 证书策略与认证业务声明框架》
- GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式》
- GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》
- GB/T 37092-2018《信息安全技术 密码模块安全要求》
- GM/T 0015-2023《数字证书格式》
- GM/T 0033-2014《时间戳接口规范》
- GM/T 0034-2014《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》
- T/CQAE 11034-2025《电子认证业务规则规范》

目 录

1. 引言 - 1 -

1.1. 概述 - 1 -

1.2. 文档名称与标识 - 1 -

1.3. PKI 参与者 - 2 -

1.3.1. 电子认证服务机构 - 2 -

1.3.2. 注册机构 - 2 -

1.3.3. 订户 - 2 -

1.3.4. 依赖方 - 2 -

1.3.5. 其他参与者 - 3 -

1.4. 证书应用 - 3 -

1.4.1. 适合的证书应用 - 3 -

1.4.2. 限制的证书应用 - 3 -

1.5. 策略管理 - 4 -

1.5.1. 策略文档管理机构 - 4 -

1.5.2. 联系方式 - 4 -

1.5.3. 决定 CP 符合策略的机构 - 4 -

1.5.4. CP 批准程序 - 5 -

1.5.5. CP 修订 - 5 -

1.6. 定义和缩写 - 5 -

1.6.1. 定义 - 5 -
1.6.2. 缩写 - 6 -
2. 信息发布与管理 - 7 -
2.1. 信息库 - 7 -
2.2. 认证信息的发布 - 7 -
2.3. 发布时间或频率 - 7 -
2.4. 信息库访问控制 - 8 -
3.1. 命名 - 8 -
3.1.1. 名称类型 - 8 -
3.1.2. 名称意义化要求 - 8 -
3.1.3. 匿名或伪名 - 8 -
3.1.4. 名称形式解释规则 - 8 -
3.1.5. 名称唯一性 - 9 -
3.1.6. 商标识别与角色 - 9 -
3.2. 初始身份确认 - 9 -
3.2.1. 证明持有私钥的方法 - 9 -
3.2.2. 存证证书订户核验 - 9 -
3.2.3. 时间戳证书订户核验 - 10 -
3.2.4. 订户告知与意愿确认 - 10 -
3.2.5. 未验证的订户信息 - 10 -
3.2.6. 授权确认 - 10 -

3.2.7. 互操作准则 - 11 -
3.3. 密钥更新请求的标识与鉴别 - 11 -
3.4. 撤销请求的标识与鉴别 - 11 -
4.1. 证书申请 - 12 -
4.1.1. 证书申请实体 - 12 -
4.1.2. 证书申请过程与责任 - 12 -
4.2. 证书申请处理 - 12 -
4.2.1. 识别与鉴别 - 12 -
4.2.2. 批准条件 - 12 -
4.2.3. 拒绝条件 - 12 -
4.2.4. 处理时限 - 13 -
4.3. 证书签发 - 13 -
4.4. 证书接受 - 13 -
4.5. 密钥对和证书使用 - 13 -
4.5.1. 订户密钥和证书使用 - 13 -
4.5.2. 依赖方证书使用 - 14 -
4.6. 证书更新 - 14 -
4.6.1. 证书更新情形 - 14 -
4.6.2. 请求证书更新的实体 - 14 -
4.6.3. 证书更新处理 - 14 -
4.6.4. 更新证书通知、接受和发布 - 15 -

4.7. 证书密钥更新 - 15 -
4.7.1. 证书密钥更新情形 - 15 -
4.7.2. 请求证书密钥更新的实体 - 15 -
4.7.3. 证书密钥更新处理 - 15 -
4.7.4. 密钥更新证书通知、接受和发布 - 16 -
4.8. 证书变更 - 16 -
4.8.1. 证书变更情形 - 16 -
4.8.2. 请求证书变更的实体 - 16 -
4.8.3. 证书变更处理 - 16 -
4.8.4. 变更证书通知、接受和发布 - 17 -
4.9. 证书吊销和挂起 - 17 -
4.9.1. 吊销情形 - 17 -
4.9.2. 吊销请求实体 - 17 -
4.9.3. 吊销请求流程和宽限期 - 18 -
4.9.4. 吊销处理时限 - 18 -
4.9.5. 依赖方检查要求 - 18 -
4.9.6. 证书撤销列表频率和最长滞后时间 - 18 -
4.9.7. 挂起 - 18 -
4.10. 证书状态服务 - 19 -
4.11. 订购结束 - 19 -
4.12. 密钥托管和恢复 - 20 -

5. 电子认证服务机构设施、管理和操作控制 - 20 -
5.1. 物理控制 - 20 -
5.2. 程序控制 - 20 -
5.3. 人员控制 - 21 -
5.4. 审计日志程序 - 21 -
5.5. 记录归档 - 21 -
5.6. CA 密钥更替 - 22 -
5.7. 损害与灾难恢复 - 22 -
5.8. CA 或 RA 的终止 - 22 -
6. 认证系统技术安全控制 - 23 -
6.1. 密钥对的生成和安装 - 23 -
6.2. 私钥保护和密码模块工程控制 - 23 -
6.3. 密钥对管理其他方面 - 24 -
6.4. 激活数据 - 24 -
6.5. 计算机安全控制 - 24 -
6.6. 生命周期技术控制 - 25 -
6.7. 网络安全控制 - 25 -
6.8. 时间戳 - 25 -
7. 证书、证书撤销列表和在线证书状态协议 - 26 -
7.1. 证书 - 26 -
7.1.1. 证书版本和格式 - 26 -

7.1.2. 证书链 - 26 -
7.1.3. 证书类型 - 27 -
7.1.4. 证书策略扩展 - 27 -
7.1.5. 密钥用法和增强密钥用法 - 27 -
7.1.6. 名称形式和主体信息 - 28 -
7.1.7. 标准扩展项和自定义扩展项 - 28 -
7.1.8. 证书有效期 - 28 -
7.2. 证书撤销列表 - 29 -
7.2.1. 版本 - 29 -
7.2.2. 证书撤销列表和条目扩展项 - 29 -
7.2.3. 发布频率和最大滞后 - 29 -
7.3. 在线证书状态协议 - 30 -
7.3.1. 版本 - 30 -
7.3.2. 在线证书状态协议扩展项 - 30 -
7.3.3. 响应规则和缓存 - 30 -
8. 电子认证服务机构审计和其他评估 - 30 -
8.1. 审计和评估频率 - 30 -
8.2. 审计和评估内容 - 31 -
8.3. 审计人员和机构要求 - 31 -
8.4. 问题整改 - 31 -
8.5. 结果沟通 - 31 -

8.6. 抽样、整改和证据留存 - 31 -
9. 法律责任和其他业务条款 - 32 -
9.1. 费用 - 32 -
9.2. 财务责任 - 32 -
9.3. 业务信息保密 - 33 -
9.4. 个人隐私保护 - 33 -
9.5. 知识产权 - 33 -
9.6. 陈述与担保 - 33 -
9.6.1. 沃通的陈述与担保 - 33 -
9.6.2. 订户的陈述与担保 - 34 -
9.6.3. 依赖方的陈述与担保 - 34 -
9.7. 担保免责 - 34 -
9.8. 有限责任 - 34 -
9.9. 赔偿 - 35 -
9.10. 有效期限与终止 - 35 -
9.11. 个别通告与沟通 - 35 -
9.12. 修订 - 35 -
9.13. 争议处理 - 36 -
9.14. 管辖法律 - 36 -
9.15. 与适用法律的符合性 - 36 -
9.16. 一般条款 - 37 -

9.17. 其他条款 ..... - 37 -

1. 引言

1.1. 概述

沃通电子认证服务有限公司（以下简称“沃通”）依法提供电子认证服务。本《沃通存证型证书策略》（以下简称“本 CP”或“CP3”）规定沃通存证型证书的策略边界、适用范围、证书类型、证书用途、法律适用性、依赖方责任、公开发布和版本管理要求。

本 CP 适用于沃通在国家电子认证服务体系下签发的存证证书和时间戳证书。存证证书用于电子数据存证、证据链支撑、业务事件固化和项目接入场景；时间戳证书用于时间戳服务系统签发时间戳响应，以证明数据或签名行为相关时间属性。

本 CP 项下证书不适用《中华人民共和国电子签名法》电子签名认证证书口径，不属于电子签名认证证书，不作为第三方电子认证服务路径下可靠电子签名效力的独立来源。时间戳服务被用于支撑可靠电子签名时间要素时，其法律效力来源于所支撑的电子签名、对应电子签名认证证书、签名行为和时间戳服务证据链，而非时间戳证书本身。

本 CP 属于策略文件。CP 确定证书适用的策略、对象标识符、用途限制和法律责任边界；CPS1《沃通电子认证业务规则》确定本 CP 项下证书的申请受理、主体核验、告知确认、证书签发、撤销、状态查询、记录留存和安全控制等实施要求。

1.2. 文档名称与标识

项目	内容
文档名称	《沃通存证型证书策略》
文档简称	CP3
CP 文档对象标识符	1.2.156.150570.6.3
适用 CPS	CPS1《沃通电子认证业务规则》
CPS 文档对象标识符	1.2.156.150570.7.1
CPS 公开地址	https://www.wotrus.com/ca/cps.html
CP 公开地址	https://www.wotrus.com/ca/cp.html

本 CP 文档对象标识符用于标识沃通存证型证书策略。用户证书的 certificatePolicies 扩展项包含本 CP 文档对象标识符，并以 CPS 公开地址作为策略限定信息。本 CP 项下证书不得包含主管部门电子签名认证证书策略对象标识符。

1.3. PKI 参与者

1.3.1. 电子认证服务机构

沃通作为电子认证服务机构，负责本 CP 项下证书的签发、发布、撤销、证书状态服务、信息发布、记录留存、合规审计和持续运营管理。

1.3.2. 注册机构

注册机构负责证书申请受理、申请材料审查、订户告知、用途确认、授权关系确认和证书生命周期请求处理。注册机构的具体职责、权限和操作要求由 CPS1 规定。

1.3.3. 订户

订户是申请并持有本 CP 项下证书的机构、业务系统运营方、时间戳服务系统运营方、存证平台或经授权的项目接入方。订户提供真实、完整、准确的申请信息，按照证书用途使用证书，并妥善管理私钥、系统访问权限和相关激活数据。

1.3.4. 依赖方

依赖方是基于本 CP 项下证书、时间戳响应、存证签名结果或相关证据链进行验证、审查或业务判断的个人、机构或其他实体。依赖方在信赖相关结果前，验证证书链、证书有效期、证书用途、证书策略、证书状态、时间戳响应或存证数据完整性，并结合具体业务规则判断其证明力。

1.3.5. 其他参与者

其他参与者包括时间戳服务系统、存证平台、项目业务系统、目录服务、证书状态服务、归档系统、审计系统和其他经授权参与服务流程的相关方。相关方的职责和边界以 CPS1、服务协议、接入协议和适用法律法规为准。

1.4. 证书应用

1.4.1. 适合的证书应用

本 CP 项下证书适用于下列场景：

1. 电子数据存证、业务事件固化、证据链支撑和项目接入场景；
2. 存证平台、业务系统或事件发起方对待存证数据进行签名、封存或形成可验证记录的场景；
3. 时间戳服务系统签发时间戳响应，用于证明数据、签名行为或业务事件相关时间属性的场景；
4. 经沃通确认符合本 CP、CPS1 和服务协议要求的其他存证或时间证据支撑场景。

本 CP 项下证书包括存证证书和时间戳证书。项目定制存证证书属于存证证书在特定项目、特定业务系统或特定证书链下的应用形态，不构成独立法律口径。

1.4.2. 限制的证书应用

本 CP 项下证书不得用于下列场景：

1. 作为《中华人民共和国电子签名法》项下电子签名认证证书使用；
2. 对外主张可靠电子签名效力的独立来源；
3. 证明自然人或机构在电子签名行为中的签名主体身份；
4. 超出存证、时间戳、证据链支撑或服务协议约定范围的用途；
5. 违反法律法规、监管要求、公序良俗或服务协议约定的用途；

6. 将证书、私钥、激活数据转让、出租、出借、出售或交由未授权主体使用。

沃通在证书申请、项目接入、服务协议或业务系统受理流程中明确告知订户：本 CP 项下证书不适用《中华人民共和国电子签名法》，不属于电子签名认证证书。订户确认知晓后，相关确认记录随申请或接入资料保存。

1.5. 策略管理

1.5.1. 策略文档管理机构

沃通安全策略委员会负责本 CP 的制定、修订、批准、废止和公开发布管理，并负责审议本 CP 涉及的证书策略对象标识符、证书链、用途边界、重要安全策略和重大例外事项。

1.5.2. 联系方式

项目	内容
机构名称	沃通电子认证服务有限公司
官方网站	https://www.wotrus.com
CP 发布地址	https://www.wotrus.com/ca/cp.html
CPS 发布地址	https://www.wotrus.com/ca/cps.html
客服热线	4006-967-446
客服邮箱	cps@wotrus.com
联系地址	深圳市南山区南海大道 1057 号科技大厦二期 A 座 502

1.5.3. 决定 CP 符合策略的机构

沃通安全策略委员会负责判定本 CP、CPS1、证书签发实践、证书格式、证书状态服务和相关运营活动是否符合本 CP 的策略要求。

1.5.4. CP 批准程序

本 CP 的制定、修订和废止经过起草、合规与技术影响评估、安全策略委员会审议批准、发布和必要的备案或报备程序。涉及订户或依赖方权利义务的重要变更，通过沃通官网或其他合理方式进行公告。

1.5.5. CP 修订

发生法律法规或监管要求变化、适用标准更新、证书策略调整、证书链或证书状态服务变化、重大安全事件、审计发现或安全策略委员会决议等情形时，沃通可启动本 CP 修订。本 CP 至少每年进行一次评审。

1.6. 定义和缩写

1.6.1. 定义

术语	释义
证书策略	指明证书对于具有共同安全要求的特定团体或应用类别的适用性的规则集合。
认证业务规则	电子认证服务机构关于其证书生命周期管理、身份查验、证书签发、状态服务和安全控制实践的具体声明。
存证证书	用于电子数据存证、业务事件固化或证据链支撑的非电子签名认证证书。
时间戳证书	用于时间戳服务系统签发时间戳响应的非电子签名认证证书。
时间戳	对时间和其他待签名数据进行签名得到的、用于表明数据时间属性的数据。
订户	申请并持有证书的机构、系统运营方、平台或其他授权实体。
依赖方	基于证书、时间戳响应、存证签名结果或相关证据链进行验证、审查或业务判断的实体。
证书撤销列表	由电子认证服务机构签发并发布的被撤销证书列表。
在线证书状态协议	用于查询证书撤销状态的在线协议。
证书状态服务	沃通通过证书撤销列表、在线证书状态协议或其他公开渠道提供的证书状态查询服务。
对象标识符	用于无歧义标识对象的全局唯一值。

1.6.2. 缩写

缩写	英文全称	中文含义
CA	Certification Authority	电子认证服务机构
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	认证业务规则
CRL	Certificate Revocation List	证书撤销列表
DN	Distinguished Name	甄别名称
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
OCSP	Online Certificate Status Protocol	在线证书状态协议
OID	Object Identifier	对象标识符
PKI	Public Key Infrastructure	公钥基础设施
TSA	Time Stamping Authority	时间戳服务机构
SM2	SM2 Elliptic Curve Public Key Cryptography Algorithm	SM2 椭圆曲线公钥密码算法
SM3	SM3 Cryptographic Hash Algorithm	SM3 密码杂凑算法

2. 信息发布与管理

2.1. 信息库

沃通建立公开信息库，用于发布与本 CP 项下证书相关的证书策略、认证业务规则、证书链、证书撤销列表、在线证书状态服务信息、业务指南、依赖方信息和其他依法公开的信息。

2.2. 认证信息的发布

沃通发布下列信息：

本 CP 的现行版本及必要历史版本，发布地址为 https://www.wotrus.com/ca/cp.html；

CPS1《沃通电子认证业务规则》的现行版本及必要历史版本，发布地址为 https://www.wotrus.com/ca/cps.html；

证书链、根证书和中级根证书公开信息，证书链发布地址为 https://www.wotrus.com/ca/chain.html 或证书扩展项载明的公开访问地址；

本 CP 项下证书的证书撤销列表和在线证书状态服务地址；

业务办理指南、订户协议、依赖方协议、投诉处理政策、投诉渠道和争议处理方式；

订户和依赖方需要了解的证书用途、限制、责任、收费和状态查询信息。

2.3. 发布时间或频率

本 CP 经批准后发布，生效日期以版本控制表或发布公告载明日期为准。本 CP 发生修订时，沃通发布修订后的版本，并保留必要的历史版本访问能力。

国家根体系下用户证书撤销列表至少每 24 小时发布一次。吊销生效后，沃通在 24 小时内发布更新的证书撤销列表。在线证书状态服务实时反映证书吊销状态，响应缓存不超过 24 小时。上级根对子 CA 的撤销列表至少每 12 个月更新一次；子 CA 被吊销时，在 24 小时内更新相关状态信息。

2.4. 信息库访问控制

本 CP、CPS1、证书链、证书撤销列表和证书状态查询信息作为公开信息提供只读访问。对信息库内容的新增、修改、删除和发布操作由经授权人员执行，并纳入访问控制、变更审批和审计日志管理。

3. 标识与鉴别

3.1. 命名

3.1.1. 名称类型

本 CP 项下证书采用 X.509 v3 证书格式。证书主体名称使用 X.500 甄别名称，国家代码使用 C=CN。存证证书、时间戳证书按照证书类型载明能够识别订户、系统、平台或业务场景的主体名称信息。

3.1.2. 名称意义化要求

证书主体名称与经核验的订户、系统、平台、项目或业务场景相对应。证书主体信息不得使依赖方误认为本 CP 项下证书属于电子签名认证证书，亦不得误导依赖方将其作为可靠电子签名效力来源。

3.1.3. 匿名或伪名

本 CP 项下证书不支持匿名签发。确因存证业务场景需要使用业务系统标识、项目标识或事件标识的，按照 CPS1 和服务协议进行管理，并确保可回溯至经授权的订户或业务系统。

3.1.4. 名称形式解释规则

证书主体名称的解释规则遵循 X.509、GB/T 20518-2018、GM/T 0015-2023 及 CPS1 的规定。机构类或系统类证书主体名称至少包含 CN、O、C 等必要字段。涉及统一社会信用代码、项目标识、业务系统标识或其他主体识别信息的，按照适用标准和 CPS1 处理。

3.1.5. 名称唯一性

沃通在证书签发和管理过程中保持证书主体名称、证书序列号及必要主体标识信息的可区分性，避免不同订户、系统、平台或业务场景之间发生混淆。

3.1.6. 商标识别与角色

订户申请证书时不得在主体名称中使用其无权使用的商标、字号、名称或其他可能误导依赖方的信息。沃通对证书主体名称的查验不构成对订户商标权、名称权或其他民事权利的最终确认。

3.2. 初始身份确认

3.2.1. 证明持有私钥的方法

订户通过符合 CPS1 要求的证书申请请求、业务系统安全接口、密码模块、服务器密码设备或其他经批准的技术机制证明其与相应密钥的控制关系。存证证书私钥可按业务规则一次性使用并销毁；时间戳证书私钥在时间戳服务系统的受控环境中生成、保存和使用。

3.2.2. 存证证书订户核验

申请存证证书时，沃通核验订户、存证平台、项目接入方、事件发起方或业务系统的主体信息、接入关系和授权关系。核验要素包括但不限于机构登记信息、统一社会信用代码、项目或系统接入协议、业务系统绑定关系、证书用途、证书有效期和证书使用限制。

存证证书用于特定项目、特定平台或特定业务系统的，保存项目接入协议、系统绑定记录、主体核验记录、用途确认记录和业务系统自动记录。存证证书私钥一次性使用的，保存能够证明私钥生成、调用、签名和销毁过程的审计记录。

3.2.3. 时间戳证书订户核验

申请时间戳证书时，沃通核验时间戳服务系统运营方或使用方的主体信息、TSA 系统归属、时间源管理要求、系统用途和授权关系。申请材料证明时间戳服务系统与订户之间的控制或授权关系。

时间戳证书仅用于时间戳服务系统签发时间戳响应，不得用于电子签名认证证书签发、普通身份认证、服务器身份认证或其他超出本 CP 的用途。

3.2.4. 订户告知与意愿确认

沃通在证书申请、项目接入、服务协议或业务系统受理流程中向订户告知证书用途、法律适用性、使用限制、收费、证书服务条件、私钥管理义务、证书撤销条件、订户责任、依赖方验证要求和争议处理方式。

强制阅读仅作为告知方式，不得单独构成订户意愿确认。订户意愿确认结合协议签署、短信验证码、邮件确认、勾选确认、有效证书签名确认、系统日志记录、机构授权文件或其他可追溯的主动确认动作。告知记录和意愿确认记录按 CPS1 保存。

3.2.5. 未验证的订户信息

沃通不得将未经验证且足以影响证书信赖判断的信息作为已验证信息写入证书。确需写入的附加信息，按照 CPS1 和适用标准进行标识，且不得误导依赖方。

3.2.6. 授权确认

机构、平台或系统由经办人申请证书的，沃通查验经办人身份及其代表相应主体申请、领取、使用或管理证书的授权文件。授权文件、接入协议或系统绑定记录与证书申请记录一并保存。

3.2.7. 互操作准则

本 CP 项下证书用于跨系统验证、存证平台、时间戳服务、证据链系统或其他互操作场景时，各参与方以证书载明信息、本 CP、CPS1、证书状态服务、时间戳服务规则、存证服务协议和适用业务规则共同确定信赖边界。沃通负责证书签发、证书状态服务、证书链发布和本 CP 规定范围内的电子认证服务；订户负责按证书用途和授权范围使用证书；依赖方和第三方平台负责在信赖相关结果前验证证书链、证书有效期、证书用途、证书策略对象标识符、证书撤销状态和适用 CPS。

3.3. 密钥更新请求的标识与鉴别

订户申请证书密钥更新时，沃通重新确认订户身份、授权关系、证书主体信息、证书用途和订户意愿。存证证书因短期有效或一次性使用通常不办理常规密钥更新；确需继续使用服务的，按新证书申请或项目接入流程处理。时间戳证书密钥更新重新核验 TSA 系统归属、授权关系和证书用途。

证书因私钥失密、证书信息错误、主体资格变化或其他撤销原因被撤销后，订户申请新证书或密钥更新的，按照初始申请相核验要求重新办理。

3.4. 撤销请求的标识与鉴别

订户、机构授权代表、系统运营方或其他有权主体申请撤销证书时，沃通核验请求方身份、授权关系和撤销理由。因证书信息错误、私钥泄露、主体资格变化、违法违规使用、订户违反协议或其他撤销情形，由沃通主动撤销证书的，沃通按照 CPS1 规定的审批和记录要求执行。

4. 证书生命周期操作要求

4.1. 证书申请

4.1.1. 证书申请实体

本 CP 项下证书申请实体包括存证平台、项目接入方、业务系统运营方、时间戳服务系统运营方以及经合法授权的经办人。证书申请实体按照证书类型提交真实、完整、准确的主体信息、联系方式、授权文件、接入协议、证书用途说明和其他必要材料。

4.1.2. 证书申请过程与责任

证书申请过程包括订户告知、申请资料提交、主体核验、用途确认、意愿确认、协议签署或确认、密钥生成或密钥控制关系确认、证书签发审批等环节。订户对申请信息真实性、完整性、准确性承担责任；沃通对材料审查、签发审批和记录留存承担相应责任。

4.2. 证书申请处理

4.2.1. 识别与鉴别

沃通按照本 CP、CPS1 和适用法律法规对证书申请实体、证书主体、授权关系、接入关系、证书用途、申请材料和密钥控制关系进行识别与鉴别。识别与鉴别完成前，不得签发证书。

4.2.2. 批准条件

申请资料真实、完整、准确，主体核验通过，告知与意愿确认完成，接入关系或授权关系清晰，证书用途符合本 CP，签发审批通过，且不存在违法违规或安全风险的，沃通可批准签发证书。

4.2.3. 拒绝条件

申请材料不完整、主体核验未通过、授权关系无法确认、用途与本 CP 不符、订户拒绝确认必要条款、存在违法违规风险、安全风险、主体信息冲突或其他不符合签发条件的，沃通拒绝签发证书，并按 CPS1 保存处理记录。

4.2.4. 处理时限

沃通在申请资料齐备并通过主体核验、意愿确认和签发审批后，按照 CPS1 规定的处理时限完成证书签发或作出拒绝决定。因申请材料补正、人工核验、风险复核、项目接入核验、监管或司法要求导致处理时间延长的，沃通按合理方式通知申请人并保存通知和处理记录。

4.3. 证书签发

沃通签发证书前，确认申请已经通过主体核验、用途确认、订户意愿确认和签发审批，确认拟签发证书的主体信息、证书类型、证书用途、有效期、密钥用法、证书策略对象标识符和 CPS 公开地址符合本 CP 和 CPS1。

证书签发后，沃通向订户通知签发结果，并按照本 CP 和 CPS1 提供证书发布、交付或下载服务。

4.4. 证书接受

订户下载、安装、启用、调用、使用证书，或按照 CPS1、服务协议、接入协议、业务系统提示完成接受确认的，视为接受证书。订户接受证书前核对证书主体信息、有效期、证书用途、证书策略对象标识符和其他关键内容。订户拒绝接受证书或发现证书信息错误的，在证书首次使用前或 CPS1 规定期限内通知沃通处理；沃通核验相关情况，必要时撤销、重新签发或作其他更正处理，并保存处理记录。

4.5. 密钥对和证书使用

4.5.1. 订户密钥和证书使用

订户仅在本 CP、CPS1、服务协议、接入协议和证书载明用途范围内使用证书。订户妥善管理私钥、激活数据、系统访问权限和相关安全介质，不得泄露、转让、出借、出租或授权无关主体使用。订户知悉或有理由知悉私钥已经失密、可能失密或证书信息不再准确时，立即停止使用并通知沃通。

4.5.2. 依赖方证书使用

依赖方信赖相关证据链或时间戳响应前，验证证书链完整性、证书有效期、证书用途、证书策略、证书撤销状态、时间戳响应或存证数据完整性。依赖方未按本 CP 和 CPS1 要求进行合理验证，或超出证书用途和适用范围信赖证书的，自行承担相应风险。

4.6. 证书更新

4.6.1. 证书更新情形

存证证书因短期有效、一次性使用或按项目调用规则签发，通常不办理原证书项下的常规更新。订户需要继续使用存证服务的，按照新证书申请、项目接入或业务调用流程办理。时间戳证书、长期服务支撑证书或 CPS1 明确可更新的证书，在证书到期前且仍符合本 CP 用途边界时，可以办理证书更新。

4.6.2. 请求证书更新的实体

证书更新请求可由订户、项目责任主体、时间戳服务责任主体、经授权代表或 CPS1 认可的其他主体提出。请求实体证明其对原证书、对应系统或对应服务具有控制权或授权关系，并确认继续使用证书服务的用途仍属于本 CP 允许范围。

4.6.3. 证书更新处理

沃通处理证书更新时，重新确认订户身份、授权关系、项目接入关系、证书用途、证书状态、私钥控制状态和申请意愿。存证证书不因历史签发记录自动更新；时间戳证书更新确认时间戳服务系统、时间源、密钥保护措施和证书用途仍符合本 CP 与 CPS1 要求。

更新后签发的新证书使用新的证书序列号，有效期、证书策略对象标识符、密钥用法、扩展密钥用法和用途限制符合本 CP。原证书已经失密、被撤销、信息不准确或不再符合本 CP 要求的，不得作为更新依据继续使用。

4.6.4. 更新证书通知、接受和发布

证书更新完成后，沃通按照 CPS1 通知订户或项目责任主体。订户或项目责任主体核验证书主体信息、证书用途、有效期、证书策略对象标识符和证书链；发现错误的，及时拒绝接受或申请撤销。更新证书是否发布至证书库、目录服务或业务系统，由 CPS1、项目协议或服务规则确定。证书更新原则上不单独向依赖方逐一通知；依赖方通过证书状态服务、证书有效期、证书链和适用 CPS 判断证书状态。

4.7. 证书密钥更新

4.7.1. 证书密钥更新情形

存证证书私钥一次性使用并按业务规则销毁的，不提供原证书项下的密钥更新服务；需要继续使用服务的，重新申请证书。时间戳证书、服务支撑证书或 CPS1 允许密钥更新的证书，在密钥到期、算法或密钥长度调整、私钥保护环境变化、服务系统迁移或存在安全风险时，办理证书密钥更新。

4.7.2. 请求证书密钥更新的实体

证书密钥更新请求可由订户、项目责任主体、时间戳服务责任主体、系统运营方、沃通或 CPS1 认可的其他主体提出。请求实体证明其对原证书和新密钥对具有控制权或授权关系。

4.7.3. 证书密钥更新处理

证书密钥更新生成或确认新的密钥对，并完成私钥拥有权证明、主体核验、授权确认、用途确认、签发审批和必要的安全检查。旧私钥已经失密、疑似失密、被非授权主体控制或不再符合策略要求的，沃通撤销原证书并阻止旧密钥继续用于存证签名、时间戳服务或其他受信操作。

密钥更新后签发的新证书使用新的证书序列号和有效期，证书策略对象标识符、密钥用法、扩展密钥用法和用途限制符合本 CP。不得通过密钥更新扩大证书用途或改变本 CP 确定的法律适用性。

4.7.4. 密钥更新证书通知、接受和发布

密钥更新证书签发后，沃通通知订户、项目责任主体或时间戳服务责任主体进行核验和接受。新证书接受、发布、状态查询和旧证书处置按照 CPS1 执行。旧证书需撤销的，及时更新证书撤销列表和在线证书状态服务。

4.8. 证书变更

4.8.1. 证书变更情形

订户名称、机构名称、统一社会信用代码、授权关系、系统归属、项目接入关系、时间戳服务责任主体、证书用途、证书主体名称或其他影响证书信赖的信息发生变化时，订户及时向沃通申请证书变更或重新签发。

4.8.2. 请求证书变更的实体

证书变更请求可由订户、项目责任主体、时间戳服务责任主体、经授权代表、沃通或 CPS1 认可的其他主体提出。请求实体提交变更原因、变更后信息、授权材料和必要证明。

4.8.3. 证书变更处理

沃通核验变更事项对证书信赖的影响。涉及证书主体信息、系统归属、授权关系、证书用途、证书策略对象标识符、密钥用法或扩展密钥用法变化的，按照初始申请相核验要求处理，并重新签发证书。仅变更联系信息、服务联系人或其他不影响证书内容和信赖判断的信息的，可按照 CPS1 更新业务记录。

证书变更需要重新签发证书的，新证书使用新的证书序列号，证书策略对象标识符、证书用途、密钥用法和有效期符合本 CP。原证书不再准确或不再具备信赖条件的，沃通撤销原证书并更新证书状态服务。

4.8.4. 变更证书通知、接受和发布

证书变更或重新签发完成后，沃通通知订户、项目责任主体或时间戳服务责任主体。订户核验证书内容并按照 CPS1 接受或拒绝接受。变更后的证书发布、旧证书撤销、状态服务更新和对其他参与方的通告按照 CPS1、服务协议或项目接入规则执行。

4.9. 证书吊销和挂起

4.9.1. 吊销情形

发生下列情形之一的，沃通吊销或有权吊销证书：

1. 订户申请吊销证书；
2. 私钥泄露、疑似泄露或不再由授权系统控制；
3. 证书中载明的信息错误、失实或不再准确；
4. 订户违反本 CP、CPS1、服务协议、接入协议或法律法规要求；
5. 订户主体资格终止、授权关系终止、系统归属变化或证书用途不再成立；
6. 沃通发现证书签发、使用或管理存在重大安全风险；
7. 法律法规、监管要求、司法机关或主管机关要求吊销；
8. CPS1 规定的其他吊销情形。

证书自然到期自动失效，不因自然到期列入证书撤销列表。

4.9.2. 吊销请求实体

吊销请求可由订户、机构授权代表、系统运营方、沃通、监管机关、司法机关或其他依法有权主体提出。沃通对吊销请求主体身份、授权关系和吊销理由进行核验。

4.9.3. 吊销请求流程和宽限期

订户知悉或有理由知悉私钥泄露、疑似泄露、证书信息错误、授权关系终止或证书不再继续使用时，立即停止使用相关证书并及时向沃通提交吊销请求。沃通提供客服热线、电子邮件、在线服务渠道或现场渠道受理吊销请求，核验请求主体身份与权限，记录吊销理由、受理时间、审核结论和执行结果。对私钥泄露、疑似泄露或重大安全风险情形，不设置请求宽限期；沃通优先处理。

4.9.4. 吊销处理时限

沃通受理有效吊销请求后，在 24 小时内完成吊销处理，并将吊销信息纳入下一次证书撤销列表发布和在线证书状态服务。

4.9.5. 依赖方检查要求

依赖方信赖相关证据链或时间戳响应前，检查证书链、证书有效期、证书用途、证书策略对象标识符和证书撤销状态。证书状态为撤销、挂起、未知、过期或状态查询无法完成的，依赖方不得继续信赖该证书。

4.9.6. 证书撤销列表频率和最长滞后时间

国家根体系下用户证书撤销列表至少每 24 小时发布一次。吊销生效后，沃通在 24 小时内发布更新的证书撤销列表；在线证书状态服务实时反映证书吊销状态，响应缓存不超过 24 小时。上级根对子 CA 的撤销列表至少每 12 个月更新一次；子 CA 被吊销时，在 24 小时内更新相关状态信息。

4.9.7. 挂起

本 CP 项下证书提供挂起和恢复服务。挂起适用于私钥疑似泄露但尚待核实、证书主体信息或授权关系存在争议、司法或监管要求临时中止、订户申请临时中止使用、系统归属争议等情形。挂起请求可由订户、机构授权代表、系统运营方、沃通、监管机关、司法机关或 CPS1 规定的其他有权主体提出。沃通核

验请求主体身份与权限后，可将证书状态更新为挂起并纳入证书状态服务，挂起状态在 24 小时内反映至证书撤销列表或在线证书状态服务。

订户申请恢复证书的，在挂起期内提交恢复申请并通过身份、授权和恢复条件核验。恢复条件包括私钥安全风险排除、争议解决、授权关系恢复、系统归属确认或其他 CPS1 规定条件。恢复审核通过后，沃通在 24 小时内更新证书状态。挂起期限、超过期限后的处置方式和不予恢复情形由 CPS1、服务协议和沃通冻结/恢复制度规定；不满足恢复条件的，沃通依法或依约撤销证书。

4.10. 证书状态服务

沃通通过证书撤销列表和在线证书状态协议提供证书状态查询服务。国家根体系下在线证书状态服务地址为 http://ocsp2.wotrus.com/。

依赖方在信赖相关证据链或时间戳响应前查询证书状态。证书状态服务中显示为撤销、挂起、过期、未知或无法完成有效验证的，依赖方不得继续信赖该证书。

沃通为证书撤销列表、在线证书状态协议和证书目录查询服务建立连续运行保障机制，证书状态查询服务可用率目标不低于 99%。发生计划维护、网络异常、系统故障或其他影响查询服务连续性的情形时，沃通通过备用查询服务、备用发布节点、官网公告、客户服务渠道或其他合理方式提供证书状态查询或状态信息说明。证书状态服务异常期间，沃通优先保障证书撤销状态的及时发布和可验证性，并保留故障、切换、恢复、公告和客户响记录。

4.11. 订购结束

证书服务期届满、证书被吊销、订户终止服务、服务协议终止、项目接入关系终止或其他 CPS1 规定的情形发生时，证书订购关系终止。订购结束不影响终止前已签发证书、时间戳响应、存证记录、证书状态记录、业务记录和审计记录的保存义务。

4.12. 密钥托管和恢复

存证证书私钥可按业务规则一次性使用并销毁，不进行长期托管。时间戳证书私钥在时间戳服务系统的服务器侧密码设备或等效受控环境中生成、保存和使用，并纳入权限控制和审计记录。

本 CP 项下证书涉及密钥备份、恢复、封装、交付和销毁的，执行 CPS1、密钥管理制度和适用密码管理要求。密钥恢复由订户或授权人员提出申请，经身份核验、授权审批和双人控制后执行，并记录恢复日志和归档材料。

5. 电子认证服务机构设施、管理和操作控制

5.1. 物理控制

沃通采用分区分级的物理安全控制措施管理电子认证服务场所，覆盖机房、核心区、管理区、服务区、设备存放区、档案区、备份介质保管区和其他相关场所。核心场所通过门禁、入侵报警、视频监控、出入登记、授权陪同和访问复核控制人员进出，并通过环境监测、消防、防水、防雷、电力保障、防盗、防破坏和介质交接管理保障系统连续运行。

备份介质、档案介质和含敏感信息的载体采用授权领用、封装标识、登记交接、受控存放和销毁留痕管理。CPS1 对各物理区域的访问条件、审批流程、陪同要求、环境指标和异常处置作出实施细化。

5.2. 程序控制

沃通对证书签发、证书撤销、证书挂起与恢复、密钥管理、系统配置、策略变更、审计日志调阅、证书状态服务发布和应急处置执行职责分离、授权审批、双人或多人控制、操作复核、过程记录和审计追踪。根证书和中级根证书密钥相关操作纳入安全策略委员会授权范围，并按照 CPS1 的密钥仪式、变更审批和见证记录流程执行。

5.3. 人员控制

沃通设置与存证型证书服务相匹配的可信角色，明确岗位职责、权限边界、任职条件、背景核验、保密承诺、岗位培训、权限复核、岗位变更和离岗处置。可信人员在授权前完成法律法规、岗位职责、内部制度、PKI 与密码技术、本 CP、CPS1、主体核验、存证业务运行、系统安全和灾难恢复培训；在岗期间接受持续培训和权限复核，离岗或岗位调整时完成权限回收、交接确认和保密义务重申。

5.4. 审计日志程序

沃通记录证书申请、资料审核、身份查验、意愿确认、证书签发、更新、变更、吊销、挂起、恢复、状态服务发布、密钥操作、系统访问、权限变更、配置变更、安全事件、异常操作和物理访问等事件。审计日志包含时间、事件类型、操作人员或系统标识、操作对象、操作结果、来源地址或设备标识以及必要关联编号。

审计日志采用访问控制、防篡改、备份、定期审查和异常告警措施保护。证书签发系统、注册系统、目录服务、状态服务、密钥管理系统、网络安全设备和业务系统日志纳入统一审计范围；发现异常访问、越权操作、重复失败、策略绕行或状态服务异常时，沃通启动调查、处置和留痕流程。

5.5. 记录归档

沃通归档证书申请受理资料、身份查验记录、主体核验记录、订户意愿确认记录、服务协议、接入协议、授权文件、时间戳签发日志、存证签名记录、证书签发审批、证书交付、证书更新、证书密钥更新、证书变更、吊销、挂起、恢复、状态服务发布、争议处理和相关审计日志。上述记录至少保存至对应证书失效后五年；法律法规、监管要求、审计要求、司法协查或服务协议规定更长期限的，按更长期限保存。

归档记录同时采用物理安全和逻辑访问控制保护，授权人员按照审批流程调阅。涉及电子签名效力、证书状态、身份核验和订户意愿的关键证据保持可检索、可核验、可追溯。

5.6. CA 密钥更替

沃通对根证书和中级根证书密钥更替实施计划管理。密钥更替先完成风险评估、算法与密钥长度评估、证书链连续性评估、依赖方影响评估和状态服务影响评估，再提交安全策略委员会审议批准。密钥生成、启用、停用、备份、销毁、公告披露、证书链发布和归档保存按照 CPS1 执行。

旧密钥签发证书的证书链、证书撤销状态、证书撤销列表、在线证书状态服务记录和业务档案保留至覆盖最后一张证书或最后一个时间戳的预期验证期。发生密钥疑似失控、算法不再适用或监管要求变更时，沃通启动专项评估和应急更替流程。

5.7. 损害与灾难恢复

沃通建立安全事件响应、业务连续性和灾难恢复机制，覆盖证书签发、证书库、证书撤销列表、在线证书状态服务、目录服务、密钥管理、业务受理、主体核验、时间戳服务、存证业务支撑、审计日志、备份系统和相关支撑系统。发生重大安全事件、系统故障、数据损坏、密钥损害、证书误签、状态服务异常、网络攻击或灾难情形时，沃通按照 CPS1 启动影响评估、业务切换、数据恢复、证书状态更新、通知报告、复盘整改和证据留存流程。

沃通定期测试、审查和更新应急处理预案与灾难恢复计划。涉及 CA 私钥疑似失控、需要作废或其他影响信赖基础的事件，沃通按照密钥风险处置流程完成暂停签发、状态更新、依赖方通知、监管报告、证书链处置和后续恢复安排。

5.8. CA 或 RA 的终止

沃通拟暂停或者终止电子认证服务时，至少九十日前通知订户、依赖方等有关各方，至少六十日前向主管部门报告，并完成业务承接、证书撤销或迁移、密钥和数据移交、证书状态服务延续、档案封存、敏感数据处理、公告发布和后续验证安排。终止不影响终止前已签发证书在法定期限内的验证、撤销记录和业务档案可追溯性。

6. 认证系统技术安全控制

6.1. 密钥对的生成和安装

沃通按照国家密码管理要求、商用密码标准、本 CP 和 CPS1 生成、安装、交付和管理密钥对。CA 密钥和关键系统密钥在受控安全环境中使用经认可的密码设备生成和保护，生成、备份、恢复、启用、停用和销毁过程执行授权审批、多人控制、操作见证和审计记录。

存证证书密钥可在业务系统、服务器侧密码设备或等效受控环境中生成和使用，一次性使用的私钥在使用后按业务规则销毁。时间戳证书密钥在 TSA 服务器、服务器密码设备或等效受控环境中生成和保护。密钥算法、密钥长度、公钥参数质量、公钥与主体身份的绑定关系符合 GM/T 0015-2023、GM/T 0034-2014、GB/T 25056-2018 和 CPS1。

订户公钥通过证书申请请求、密码模块输出、业务系统安全接口或 CPS1 规定的其他方式提交并绑定至证书申请。沃通在签发前验证公钥格式、算法参数、密钥用途、主体身份和申请材料的一致性。私钥不以明文形式传送；加密密钥或相关密钥材料通过加密通道、密码信封、安全介质或其他符合密码管理要求的方式交付。

6.2. 私钥保护和密码模块工程控制

沃通使用符合国家密码管理要求的密码产品和密码模块保护 CA 私钥。CA 私钥不以明文形式导出；密钥生成、备份、恢复、使用、停用和销毁执行严格授权、多人控制、审计记录和安全保管。密码设备具备物理防护和访问控制能力，密钥管理操作在受控环境和授权流程内完成。

存证证书私钥和时间戳证书私钥在受控环境中加密存储或受控使用，使用过程保留调用记录、审计记录和权限控制记录。任何人员不得以明文方式导出、复制、留存或转交证书私钥。

CA 私钥备份材料采用分片、加密、离线或异地安全保存。存证证书私钥和时间戳证书私钥的备份、恢复、销毁和停用按照 CPS1、服务协议和安全策略委员会批准规则执行。

6.3. 密钥对管理其他方面

沃通按照 CPS1 管理 CA 公钥归档、证书链发布、密钥有效期、密钥轮换、密钥备份、密钥恢复和密钥销毁。已签发证书的公钥证书定期归档，归档间隔不超过 12 个月。存证证书最大有效期为 90 天；时间戳证书最大有效期为 1827 天且不超过五年。证书到期后，私钥不再用于存证签名或时间戳服务。

CA 密钥停用、替换或销毁后，沃通继续保存足以验证历史证书状态和历史签名的证书链、证书撤销状态和归档材料。订户密钥发生损害或疑似损害的，按 4.9 节执行撤销或挂起处理，并按 4.7 节完成密钥更新或重新申请。

6.4. 激活数据

沃通和订户保护口令、个人识别码、设备口令、生物特征、令牌口令、密钥份额等激活数据。激活数据生成采用复杂度、随机性、防猜测和防泄露控制，不使用默认口令、弱口令或与个人身份明显相关的信息。初始激活数据通过安全渠道传输，首次使用时完成修改或重新设定。

激活数据不共享、不明文记录在非受控载体中、不交由无关主体使用。连续输入错误达到 CPS1 或内部制度规定阈值时，系统执行锁定和重置流程；关键岗位和高风险操作采用更严格的认证与更换周期。激活数据的变更、重置、锁定、解锁、销毁等操作记录至审计日志。

6.5. 计算机安全控制

沃通对证书签发系统、注册系统、密钥管理系统、目录服务、证书状态服务、日志系统和相关业务系统实施身份鉴别、访问控制、最小权限、系统加固、补丁管理、漏洞扫描、恶意代码防护、数据备份、安全监测和日志审计。系统运行期间开展漏洞扫描、必要的渗透测试和安全加固，发现重大漏洞或高风险配置时启动修复、复测和留痕流程。

6.6. 生命周期技术控制

沃通对电子认证服务系统实施开发、测试、上线、变更、运行、维护和退役全过程安全控制。系统变更、配置调整、补丁升级、关键参数调整和证书策略变更经过影响评估、审批、测试、实施、验证和记录归档；生产发布与回退计划同步管理，避免策略边界、证书格式、状态服务或密钥保护控制被未授权改变。

6.7. 网络安全控制

沃通按照 GB/T 25056-2018 附录 A 及 CPS1 进行网络分区、边界防护、访问控制、白名单管理、安全监控和入侵防护。证书签发系统、注册系统、数据库、密钥管理系统、目录服务和证书状态服务按照安全等级隔离；网络边界部署防火墙、入侵检测或防护、安全审计、恶意代码防护、漏洞扫描、数据备份和灾难恢复措施，并持续更新安全策略和监测规则。

6.8. 时间戳

本 CP 项下时间戳证书用于 TSA 时间戳服务。时间戳服务采用可信、可审计、可校验的时间源，并按照 CPS1 进行同步、偏差监测和异常处理。时间戳服务系统记录时间源同步、时间偏差监测、时间戳签发、系统调用、异常处理和状态服务查询等信息。

时间戳证书私钥在受控密码设备或等效受控环境中生成、保存和使用，不以明文形式导出、复制或转交非授权主体。时间戳签发日志、时间源同步记录、系统调用记录、异常处理记录和证书状态记录至少保存至覆盖最后一个时间戳的预期验证期；法律法规、监管要求、审计要求或服务协议要求更长期限的，按更长期限保存。时间戳证书被撤销、密钥失控、时间源异常或时间戳服务系统发生重大安全事件时，沃通按照 CPS1 启动应急处理、状态更新、通知和记录归档流程。

7. 证书、证书撤销列表和在线证书状态协议

7.1. 证书

7.1.1. 证书版本和格式

本 CP 项下证书采用 X.509 v3 格式，符合 GB/T 20518-2018、GM/T 0015-2023 和相关证书格式规范。证书至少包含版本、序列号、签名算法、颁发者、有效期、主体、主体公钥信息、扩展项和颁发者签名等内容。证书签名算法、主体公钥算法和相关算法对象标识符按 GM/T 0015-2023、GM/T 0006-2023 及证书实际载明信息执行。

7.1.2. 证书链

本 CP 项下证书可使用下列证书链：

证书类型或场景	证书链	证书撤销列表	在线证书状态服务	CA 证书访问地址
时间戳证书	国家电子认证根 ROOTCA → WoTrus SM2 CA → WoTrus SM2 UCA → 订户证书	http://ldap.wotrus.com/crl/wotrussm2uca.crl	http://ocsp2.wotrus.com/	http://ldap.wotrus.com/subca/wotrussm2uca.crt
存证证书	国家电子认证根 ROOTCA → WoTrus SM2 CA → WoTrus SM2 E-Sign CA → 订户证书	http://ldap.wotrus.com/crl/wotrussm2esignca.crl	http://ocsp2.wotrus.com/	http://ldap.wotrus.com/subca/wotrussm2esignca.crt
项目定制存证证书	国家电子认证根 ROOTCA → WoTrus SM2 CA → WoTrus SM2 E-Sign CA → WoTrus SM2 E-Sign CA 000181 → 订户证书	http://ldap.wotrus.com/crl/wotrussm2esignca000181.crl	http://ocsp2.wotrus.com/	http://ldap.wotrus.com/subca/wotrussm2esignca000181.crt

7.1.3. 证书类型

本 CP 覆盖下列公开证书类型：

证书类型	用途	CP 文档对象标识符	CPS 公开地址
存证证书	电子数据存证、业务事件固化、证据链支撑和项目接入	1.2.156.150570.6.3	https://www.wotrus.com/ca/cps.html
时间戳证书	时间戳服务系统签发时间戳响应	1.2.156.150570.6.3	https://www.wotrus.com/ca/cps.html

本 CP 项下证书不得包含主管部门电子签名认证证书策略对象标识符。

7.1.4. 证书策略扩展

本 CP 项下证书的 certificatePolicies 扩展项包含：

本 CP 文档对象标识符 1.2.156.150570.6.3；

CPS 公开地址 https://www.wotrus.com/ca/cps.html，作为本 CP 文档对象标识符对应的策略限定信息。

7.1.5. 密钥用法和增强密钥用法

证书类型	密钥用法	增强密钥用法
存证证书	数字签名	不设置，存证验签链路不依赖第三方增强密钥用法语义
时间戳证书	数字签名	时间戳 1.3.6.1.5.5.7.3.8，且为唯一增强密钥用法

本 CP 项下证书不使用认可签名位作为电子签名认证证书法律效力声明。

7.1.6. 名称形式和主体信息

存证证书和时间戳证书主体名称至少包含 CN、O、C 等必要字段，并与经核验的订户、系统、平台、项目或业务场景相对应。涉及统一社会信用代码、项目标识、业务系统标识或其他主体识别信息的，按照适用标准和 CPS1 处理。

7.1.7. 标准扩展项和自定义扩展项

本 CP 项下证书可包含下列标准扩展项，关键性按证书格式标准和 CPS1 执行：

扩展项	关键性	说明
Authority Key Identifier	非关键	标识签发者公钥
Subject Key Identifier	非关键	标识主体公钥
Key Usage	关键	标识证书密钥用途
Extended Key Usage	非关键或按时间戳证书要求	时间戳证书使用时间戳用途
Basic Constraints	关键	订户证书路径长度约束为 0
Certificate Policies	非关键	标识本 CP 文档对象标识符和 CPS 公开地址
CRL Distribution Points	非关键	标识证书撤销列表发布点
Authority Information Access	非关键	标识在线证书状态服务和 CA 证书访问地址

本 CP 项下证书可按证书类型和业务需要使用国家或行业标准扩展项，以及项目唯一识别号、订单流水号、业务渠道标识、证书产品代码、申请受理日期等业务管理和举证用途的自定义扩展项。自定义扩展项不得向依赖方披露非公开运营留存信息。

7.1.8. 证书有效期

存证证书最大有效期为 90 天。时间戳证书最大有效期为 1827 天，且不超过五年。具体证书有效期以证书载明信息为准。

7.2. 证书撤销列表

7.2.1. 版本

本 CP 项下证书撤销列表采用 X.509 v2 CRL 格式，并符合 GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式》第 5.3 节、GM/T 0015-2023《数字证书格式》和 CPS1 的要求。证书撤销列表由签发 CA 签名，并通过公开信息库发布。

7.2.2. 证书撤销列表和条目扩展项

证书撤销列表包含颁发机构、发布时间、下次更新时间、被撤销证书序列号、撤销时间以及适用标准要求的扩展项。证书撤销列表可包含 Authority Key Identifier、CRL Number、thisUpdate、nextUpdate 等字段或扩展项；撤销条目可包含撤销日期、撤销原因等条目扩展项。具体 CRL 和条目扩展项以证书撤销列表实际载明信息、GB/T 20518-2018 第 5.3 节、GM/T 0015-2023 和 CPS1 为准。

7.2.3. 发布频率和最大滞后

服务项	国家根体系
用户证书撤销列表发布周期	至少每 24 小时发布一次
吊销后更新时限	吊销生效后 24 小时内发布更新
上级根对子 CA 的撤销列表	至少每 12 个月更新；子 CA 被吊销时 24 小时内更新

对时间戳证书、项目支撑证书或其他长期验证依赖的证书，证书撤销列表发布和归档保证依赖方能够在最后一个时间戳或最后一条存证记录的预期验证期内验证证书状态。证书撤销列表的 nextUpdate 不得超出 CPS1 规定的发布周期。

7.3. 在线证书状态协议

7.3.1. 版本

本 CP 项下在线证书状态协议服务符合 RFC 6960、GB/T 19713-2025《信息安全技术 公钥基础设施在线证书状态协议》第 7 章和 CPS1 的要求。国家根体系下服务地址为 http://ocsp2.wotrus.com/。

7.3.2. 在线证书状态协议扩展项

在线证书状态协议响应版本、响应签名、证书状态值、响应时间、响应缓存和扩展项处理规则按 GB/T 19713-2025 第 7 章及 CPS1 执行。在线证书状态协议可返回有效、撤销、挂起、未知等状态；依赖方结合证书链、证书有效期、证书用途和本 CP 判断是否信赖证书。

7.3.3. 响应规则和缓存

在线证书状态服务实时反映证书吊销状态，响应缓存不超过 24 小时。对时间戳证书或长期验证依赖的证书，OCSP 响应、证书撤销列表或可替代状态验证信息在最后一个时间戳或最后一条存证记录的预期验证期内保持可验证。在线状态服务异常时，依赖方可使用证书撤销列表或 CPS1 公布的备用状态查询机制进行验证。

8. 电子认证服务机构审计和其他评估

8.1. 审计和评估频率

沃通建立覆盖本 CP 项下证书服务的审计和评估制度。认证业务审计至少每年一次，内部运营审计至少每季度一次，全面符合性评估至少每年一次。发生重大安全事件、监管要求、重大系统变更或证书策略重大变更时，沃通启动专项审计或评估。认证业务审计可采用全面审计或抽样审计方式；采用抽样方式

的，在审计方案中明确抽样范围、抽样方法和最低抽样率，抽样率不得低于内部审计制度和监管要求规定的最低比例。

8.2. 审计和评估内容

审计和评估内容包括证书申请、主体核验、告知确认、签发审批、证书交付、证书使用、证书更新、密钥更新、证书变更、证书吊销、挂起恢复、证书状态服务、信息发布、记录留存、存证私钥一次性使用、时间戳服务支撑、物理安全、人员控制、技术安全控制、密码应用、业务连续性和法律责任履行情况。

8.3. 审计人员和机构要求

审计和评估人员具备 PKI、电子认证、信息安全、密码应用或合规审计专业能力。由外部机构执行审计或评估的，外部机构具备相应资质，并与沃通不存在影响独立性的利益冲突。

8.4. 问题整改

沃通对审计和评估发现的问题进行分级、整改、验证和闭环管理。重大问题立即停止相关风险操作，启动整改并向安全策略委员会报告；依法或按监管要求需要报告主管部门的，按规定报告。整改完成后，由合规、审计或指定责任部门进行验证，保存整改方案、整改证据、复核结论和闭环记录。

8.5. 结果沟通

认证业务审计报告提交安全策略委员会审议并归档，监管检查时依法提供。全面符合性评估报告按照监管要求在每年 1 月底前报送主管部门。

8.6. 抽样、整改和证据留存

审计抽样覆盖存证证书、项目定制存证证书、时间戳证书、不同申请渠道、签发批次、撤销记录、状态服务记录、时间戳签发日志、时间源同步记录和长期验证支撑记录。内部审计抽样率原则上不得低于当

期同类业务记录的 1%，且每类证书不少于 5 件；当期记录不足 5 件的，全量抽查。涉及时间戳服务、私钥保护、证书状态服务、证据链完整性或重大项目接入的，纳入重点抽样。

审计发现问题形成整改清单，明确责任部门、整改措施、完成期限、复核人员和验证证据。整改关闭以主体核验材料、授权文件、系统日志、签发记录、撤销记录、时间源同步记录、状态服务记录、配置复核记录或整改复核结论等证据为基础。审计报告、抽样底稿、整改证据和复核结论按照 CPS1 的记录留存要求保存。

9. 法律责任和其他业务条款

9.1. 费用

本 CP 项下可能收费的服务类别包括存证证书签发、时间戳证书签发、项目接入、平台接入、调用量服务、批量服务、定制服务和其他服务协议约定项目。具体收费项目、收费标准、批量或定制价格、退款条件和调整机制，以沃通官网公开收费规则、订户协议、服务协议或商务合同约定为准。

本 CP 项下证书状态查询、证书撤销列表访问、在线证书状态查询、证书链下载和 CP/CPS 文本访问等依赖方验证所需公开信息访问服务免费提供。

9.2. 财务责任

沃通按照法律法规、监管要求、服务协议和本 CP 承担相应财务责任，并按监管要求建立电子认证服务责任风险保障机制。责任风险保障机制用于保障因电子认证服务相关问题给订户或依赖方造成损失时的赔付能力，其保障额度、资金来源、管理方式和动用审批按法律法规、监管要求、CPS1 和沃通内部管理制度执行。本 CP 项下证书不属于电子签名认证证书，不适用《中华人民共和国电子签名法》项下可靠电子签名认证证书赔偿口径；但沃通仍应依法承担其过错导致的相应责任。

9.3. 业务信息保密

沃通对订户身份信息、主体核验记录、授权文件、申请与意愿记录、私钥及激活数据、审计底稿、审批记录、运维与安全配置信息、密钥管理资料、存证记录、时间戳服务记录以及其他未公开的业务信息承担保密义务。法律法规、监管要求、司法程序、审计要求、订户授权或安全事件处置需要披露的除外。

9.4. 个人隐私保护

沃通按照《中华人民共和国个人信息保护法》、GB/T 35273《信息安全技术 个人信息安全规范》和其他适用法律法规处理个人信息。沃通收集、使用、保存、共享、提供、删除或匿名化个人信息，遵循合法、正当、必要和诚信原则，并采取访问控制、加密、去标识化、日志审计和最小授权等安全措施。

9.5. 知识产权

本 CP、CPS1、证书格式规范、证书服务文档、系统软件和相关资料的知识产权归沃通或相关权利人所有。订户取得证书使用权，不因此取得沃通相关知识产权。证书中的公钥属于订户，证书本身及 CA 数字签名属于沃通签发的电子文件。

9.6. 陈述与担保

9.6.1. 沃通的陈述与担保

沃通陈述并保证：依法提供电子认证服务；按照本 CP 和 CPS1 签发、管理和撤销证书；对证书申请材料进行必要核验和审查；保持证书状态服务的准确性和及时性；按照法律法规和 CPS1 保存认证相关信息。

9.6.2. 订户的陈述与担保

订户陈述并保证：向沃通提供真实、完整、准确的信息；按本 CP、CPS1、服务协议和接入协议使用证书；妥善管理私钥、激活数据、系统访问权限和安全介质；证书信息变化或私钥失密时及时通知沃通；不将证书用于超出允许范围、对外主张电子签名认证证书效力或违法违规的用途。

9.6.3. 依赖方的陈述与担保

依赖方陈述并保证：在信赖相关证据链或时间戳响应前验证证书链、证书有效期、证书用途、证书策略、证书撤销状态和适用 CPS；根据业务场景、证据规则和法律要求判断相关结果是否适合被信赖；不将本 CP 项下证书作为电子签名认证证书信赖。

9.7. 担保免责

除本 CP、CPS1、服务协议和法律法规明确规定外，沃通不对证书、时间戳响应、存证结果及电子认证服务作出其他明示或默示担保。在法律允许范围内，沃通不承担适销性、特定用途适用性等默示担保责任。本 CP 项下证书不适用《中华人民共和国电子签名法》电子签名认证证书口径，沃通不就本 CP 项下证书主张可靠电子签名效力承担保证责任。

9.8. 有限责任

沃通、订户和依赖方的责任范围，根据法律法规、本 CP、CPS1、服务协议、接入协议和具体业务规则确定。任何责任限制不得排除法律强制性规定。订户或依赖方将本 CP 项下证书用于对外主张电子签名认证证书效力、超出证书用途使用、未验证证书状态或未遵守服务协议约定的，自行承担相应风险。

9.9. 赔偿

订户因提供虚假、不完整、不准确的信息，未妥善管理私钥、系统访问权限或激活数据，超出证书用途使用证书，未及时申请撤销证书，或违反本 CP、CPS1、服务协议、接入协议和法律法规，给沃通、依赖方或其他第三方造成损失的，依法承担赔偿责任。

沃通因证书信息错误、未按规定核验主体信息、未及时撤销证书、证书状态服务错误、密钥管理缺陷、系统故障、人为错误或其他沃通过错导致订户或依赖方遭受损失的，依法承担相应责任。赔偿申请、材料齐备确认、材料核验、因果关系审核、赔偿审批、赔偿支付、归档备案和监督复核流程由 CPS1 明确。

9.10. 有效期限与终止

本 CP 自生效日期起生效，至被新版本替代或被安全策略委员会依法废止之日终止。本 CP 的终止不影响终止前已签发证书、时间戳响应、存证记录、证书状态记录、争议处理和法律责任承担。

沃通暂停或者终止电子认证服务的，按照适用法律法规和 CPS1 的规定，至少九十日前通知有关各方，至少六十日前向主管部门报告，并作出业务承接和数据归档安排。

9.11. 个别通告与沟通

沃通可通过官网公告、注册邮箱、注册手机号、业务系统通知、书面通知或服务协议约定方式向订户和依赖方发送通知。订户保持联系方式准确有效，并及时查阅与证书服务相关的通知。

9.12. 修订

本 CP 的修订条件、修订程序、审批程序、公告机制和历史版本保留要求按照 1.5 节和 CPS1 执行。涉及订户、依赖方权利义务的重要变更，通过合理方式通知相关方。

9.13. 争议处理

订户、依赖方与沃通因本 CP 项下证书服务发生争议的，可向沃通投诉与争议处理部门提出。受理范围包括证书申请、主体核验、告知确认、证书签发、证书交付、证书使用、证书更新、密钥更新、证书变更、证书撤销、挂起和恢复、证书状态服务、收费、赔偿、存证记录、时间戳响应和证书使用效力等相关争议。

争议申请人提交身份证明、争议事项说明、相关证据材料、联系方式以及沃通合理要求的其他材料。沃通自收到完整材料起 5 个工作日内确认是否受理并告知申请人。争议首先通过协商解决，协商期为 30 天；协商不成的，可提请行业调解，或按照服务协议约定和法律规定处理。

沃通建立覆盖证书全生命周期的举证能力，可在法定范围内提供证书状态证明、业务流程说明、时间戳服务记录、存证业务记录和相关证据材料。举证材料自收到合法请求起 10 个工作日内提供；复杂情形可适当延长并告知申请人。依法免费提供的不收费，其他费用按沃通公开收费规则、服务协议、司法机关或监管要求执行。协商、调解不成的，任何一方可按照服务协议约定或法律规定向有管辖权的人民法院提起诉讼，或按双方另行达成的仲裁协议提交仲裁。

9.14. 管辖法律

本 CP 的制定、解释、执行和争议解决适用中华人民共和国法律。与本 CP 相关的证书服务适用《中华人民共和国民法典》《中华人民共和国密码法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《商用密码管理条例》《电子认证服务管理办法》等法律、行政法规、部门规章和主管部门监管要求。

9.15. 与适用法律的符合性

本 CP 的任何条款与适用法律法规的强制性规定不一致的，以适用法律法规的强制性规定为准。若本 CP 的某一条款被认定为无效或不可执行，不影响其他条款的效力。

9.16. 一般条款

本 CP 与 CPS1、服务协议、接入协议、订户协议、依赖方协议和相关业务规则共同构成沃通存证型证书服务规则体系。CPS1 是本 CP 的实施文件，用于规定本 CP 项下证书的实施细则，不得改变本 CP 的策略边界、证书类型、对象标识符、法律适用性、用途限制和责任边界。CP 与 CPS1 对同一事项规定不一致且无法协调时，以安全策略委员会批准的现行策略基线、本 CP 的策略边界和安全策略委员会裁定为准；涉及法律法规或监管强制性规定的，从其规定。

9.17. 其他条款

本 CP 未尽事宜，按照法律法规、监管要求、CPS1、服务协议、安全策略委员会决议和沃通公开发布的相关规则执行。