沃通身份认证通用证书策略

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《沃通身份认证通用证书策略》正文，明确 CP4 策略边界、证书类型、对象标识符、适用 CPS、用途限制、证书状态服务、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 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 - 3 -
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 - 4 -
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 - 5 -
1.5.3. 决定 CP 符合策略的机构 - 5 -
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 - 8 -
2.1. 信息库 - 8 -
2.2. 认证信息的发布 - 8 -
2.3. 发布时间或频率 - 8 -
2.4. 信息库访问控制 - 9 -
3. 标识与鉴别 - 9 -
3.1. 命名 - 9 -
3.1.1. 名称类型 - 9 -
3.1.2. 名称意义化要求 - 9 -
3.1.3. 匿名或伪名 - 10 -
3.1.4. 名称形式解释规则 - 10 -
3.1.5. 名称唯一性 - 10 -
3.1.6. 商标识别与角色 - 11 -
3.2. 初始身份确认 - 11 -
3.2.1. 证明私钥拥有权的方法 - 11 -
3.2.2. 个人身份认证证书身份鉴别 - 11 -
3.2.3. 机构身份认证证书身份鉴别 - 12 -
3.2.4. 设备身份认证证书身份鉴别 - 12 -
3.2.5. 内网 SSL/TLS 服务器证书身份鉴别 - 13 -

3.2.6. 私域内网 SSL 证书身份鉴别 - 13 -
3.2.7. 测试证书身份鉴别 - 14 -
3.2.8. 订户告知与意愿确认 - 14 -
3.2.9. 未验证的订户信息 - 15 -
3.2.10. 授权确认 - 15 -
3.2.11. 互操作准则 - 15 -
3.3. 密钥更新请求的标识与鉴别 - 16 -
3.4. 撤销请求的标识与鉴别 - 16 -
4.1. 证书申请 - 16 -
4.1.1. 证书申请实体 - 16 -
4.1.2. 注册过程与责任 - 16 -
4.2. 证书申请处理 - 17 -
4.2.1. 识别与鉴别 - 17 -
4.2.2. 批准条件 - 17 -
4.2.3. 拒绝条件 - 17 -
4.2.4. 处理时限 - 18 -
4.3. 证书签发 - 18 -
4.3.1. 签发期间电子认证服务机构的行为 - 18 -
4.3.2. 证书签发后通知订户 - 18 -
4.4. 证书接受 - 18 -
4.5. 密钥对和证书的使用 - 19 -

4.5.1. 订户私钥和证书的使用 - 19 -
4.5.2. 依赖方公钥和证书的使用 - 19 -
4.6. 证书更新 - 19 -
4.6.1. 证书更新情形 - 19 -
4.6.2. 请求证书更新的实体 - 19 -
4.6.3. 证书更新处理 - 19 -
4.6.4. 更新证书通知、接受和发布 - 20 -
4.7. 证书密钥更新 - 20 -
4.7.1. 证书密钥更新情形 - 20 -
4.7.2. 请求证书密钥更新的实体 - 20 -
4.7.3. 证书密钥更新处理 - 20 -
4.7.4. 密钥更新证书通知、接受和发布 - 20 -
4.8. 证书变更 - 21 -
4.8.1. 证书变更情形 - 21 -
4.8.2. 请求证书变更的实体 - 21 -
4.8.3. 证书变更处理 - 21 -
4.8.4. 变更证书通知、接受和发布 - 21 -
4.9. 证书吊销和挂起 - 21 -
4.9.1. 证书吊销情形 - 21 -
4.9.2. 吊销请求实体 - 22 -
4.9.3. 证书吊销请求流程 - 22 -

4.9.4. 证书吊销请求处理时间 - 22 -
4.9.5. 依赖方检查证书吊销的要求 - 23 -
4.9.6. 证书撤销列表发布频率 - 23 -
4.9.7. 证书挂起和恢复 - 23 -
4.10. 证书状态服务 - 24 -
4.11. 订购结束 - 24 -
4.12. 密钥托管和恢复 - 24 -
5.1. 物理控制 - 24 -
5.2. 程序控制 - 25 -
5.3. 人员控制 - 25 -
5.4. 审计日志程序 - 25 -
5.5. 记录归档 - 25 -
5.6. 密钥变更 - 26 -
5.7. 损害与灾难恢复 - 26 -
5.8. CA 或 RA 的终止 - 26 -
6.1. 密钥对的生成和安装 - 27 -
6.1.1. 密钥对生成 - 27 -
6.1.2. 私钥传送 - 27 -
6.1.3. 公钥传送 - 27 -
6.1.4. CA 公钥传送给依赖方 - 27 -
6.1.5. 密钥长度和参数质量 - 27 -

6.2. 私钥保护和密码模块工程控制 - 28 -
6.2.1. 私钥保护要求 - 28 -
6.2.2. 私钥多方控制 - 28 -
6.2.3. 私钥备份与归档 - 28 -
6.2.4. 私钥导入和导出 - 28 -
6.2.5. 私钥销毁 - 28 -
6.3. 密钥对管理的其他方面 - 29 -
6.4. 激活数据 - 29 -
6.4.1. 激活数据生成和安装 - 29 -
6.4.2. 激活数据保护 - 29 -
6.4.3. 激活数据其他方面 - 29 -
6.5. 计算机安全控制 - 29 -
6.6. 生命周期技术控制 - 30 -
6.7. 网络安全控制 - 30 -
6.8. 时间戳 - 30 -
7. 证书、证书撤销列表和在线证书状态协议 - 30 -
7.1. 证书 - 30 -
7.1.1. 版本 - 30 -
7.1.2. 证书链与公开服务地址 - 30 -
7.1.3. 证书类型 - 31 -
7.1.4. 证书主体名称 - 32 -

7.1.5. 算法对象标识符 - 32 -
7.1.6. 密钥用法和扩展密钥用法 - 32 -
7.1.7. 标准扩展项和自定义扩展项 - 33 -
7.1.8. 证书有效期 - 34 -
7.2. 证书撤销列表 - 35 -
7.2.1. 版本 - 35 -
7.2.2. 证书撤销列表和扩展项 - 35 -
7.3. 在线证书状态协议 - 35 -
7.3.1. 版本 - 35 -
7.3.2. 在线证书状态协议扩展项 - 35 -
8. 合规审计和其他评估 - 36 -
8.1. 审计和评估频率 - 36 -
8.2. 审计者身份和资质 - 36 -
8.3. 审计者与被审计者关系 - 36 -
8.4. 审计覆盖主题 - 36 -
8.5. 结果沟通 - 36 -
8.6. 抽样、整改和证据留存 - 37 -
9. 其他业务和法律事项 - 37 -
9.1. 费用 - 37 -
9.2. 财务责任 - 38 -
9.3. 业务信息保密 - 38 -

9.4. 个人信息保护 - 38 -

9.5. 知识产权 - 38 -

9.6. 陈述与保证 - 38 -

9.7. 担保免责 - 39 -

9.8. 责任限制 - 39 -

9.9. 赔偿 - 39 -

9.10. 有效期限和终止 - 40 -

9.11. 对参与者的个别通告与沟通 - 40 -

9.12. 修订 - 40 -

9.13. 争议处理 - 40 -

9.14. 适用法律 - 41 -

9.15. 符合适用法律 - 41 -

9.16. 一般条款 - 41 -

9.17. 其他条款 - 41 -

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《沃通身份认证通用证书策略》（以下简称“本 CP”或“CP4”）规定沃通身份认证通用证书的策略边界、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 适用于沃通签发的个人身份认证证书、机构身份认证证书、设备身份认证证书、内网 SSL/TLS 服务器证书、SM2 私域内网 SSL 证书、RSA 私域内网 SSL 证书和测试证书。上述证书用于身份认证、设备识别、内网通信、私有网络通信、接口联调、验收或演示等限定场景。

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，不作为可靠电子签名效力主张的证书来源。任何订户或依赖方不得将本 CP 项下证书作为个人或机构电子签名认证证书使用，也不得据此主张第三方电子认证服务路径下的可靠电子签名效力。

本 CP 属于策略文件。CP 确定证书适用的策略、对象标识符、证书类型、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	《沃通身份认证通用证书策略》
文档简称	CP4
CP 文档对象标识符	1.2.156.150570.6.4
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身份认证通用证书策略。除测试证书外，本 CP 项下用户证书的 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。

测试证书使用独立测试专用策略对象标识符 1.2.156.150570.3.3.1，用于与正式业务证书进行策略隔离。测试证书虽由本 CP 统一规定业务归口、用途边界和责任限制，但不得使用本 CP 正式业务证书对象标识符。

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、主体身份核验、用途确认、订户告知、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 项下证书的个人、机构、设备所属机构、系统运营方、内网服务运营方、私有网络服务运营方、测试项目申请方或其他经授权主体。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 项下证书进行身份识别、设备识别、内网通信验证、私有网络通信验证、接口联调或测试验证的个人、机构或其他实体。依赖方在信赖证书前，验证证书链、证书有效期、证书用途、证书策略、证书状态、主体信息和适用场景，并结合具体业务规则判断是否可以信赖。

1.3.5. 其他参与者

其他参与者包括业务系统、内网服务系统、私有网络系统、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. 个人身份认证证书用于业务系统、服务平台或约定场景中的个人身份识别和客户端身份验证；
2. 机构身份认证证书用于业务系统、服务平台或约定场景中的机构身份识别和客户端身份验证；
3. 设备身份认证证书用于设备、终端、服务节点或系统组件的身份识别和接入控制；
4. 内网 SSL/TLS 服务器证书用于内网服务器、内网服务或专用网络环境中的服务器身份识别、通道加密和访问控制；
5. SM2 私域内网 SSL 证书用于沃通 SM2 私域内网 SSL 体系下的内网或私有网络通信场景；
6. RSA 私域内网 SSL 证书用于沃通 RSA 私域内网 SSL 体系下的内网或私有网络通信场景；
7. 测试证书用于测试、接口联调、验收、演示或内部试运行场景。

本 CP 项下证书只能在其证书类型、证书用途、证书策略、CPS1、服务协议和申请材料约定的范围内使用。

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；
3. 超出身份认证、设备识别、内网通信、私有网络通信或测试联调用途的场景；
4. 私域内网 SSL 证书用于公众互联网、公共信任 SSL/TLS 服务或无约定依赖方的公开服务；
5. 内网 SSL/TLS 服务器证书用于公众互联网公共信任 SSL/TLS 服务；
6. 测试证书用于生产业务、公众服务、对外交易、正式身份认证或法律效力主张；
7. 违反法律法规、监管要求、公序良俗、服务协议或接入协议约定的用途；
8. 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。
身份认证证书	用于个人或机构在约定业务系统中进行身份识别和身份验证的非电子签名认证证书。
设备身份认证证书	用于设备、终端、服务节点或系统组件身份识别和接入控制的非电子签名认证证书。
内网 SSL/TLS 服务器证书	用于内网服务器、内网服务或专用网络环境中服务器身份识别和通道加密的非电子签名认证证书。
私域内网 SSL 证书	由沃通私域内网 SSL 体系签发，仅限内网、私有网络或约定系统环境使用的 SSL/TLS 证书。
测试证书	仅限测试、接口联调、验收、演示或内部试运行使用的非正式业务证书。
订户	申请并持有证书的个人、机构、设备所属机构、系统运营方或其他授权实体。
依赖方	基于证书进行身份识别、设备识别、通信验证或测试验证的实体。
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
SAN	Subject Alternative Name	主体备用名称

TLS	Transport Layer Security	传输层安全协议
SM2	SM2 Elliptic Curve Public Key Cryptography Algorithm	SM2 椭圆曲线公钥密码算法

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。

私域内网 SSL 体系下用户证书撤销列表至少每 7 天发布一次。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。证书实际扩展项、CPS1 或服务协议约定更短发布周期的，从其规定。

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。证书主体名称按照证书类型载明能够识别订户、设备、系统、内网服务或测试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个人、机构、设备、系统、内网服务或测试项目相对应。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。测试证书、设备证书或内网服务证书确需使用设备标识、系统标识、内网地址或测试项目标识的，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责任主体。

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。

个人身份认证证书主体名称体现个人身份识别信息，至少包含 CN、C 等必要字段。涉及证件类型、证件号码、手机号或其他个人识别信息的，按照适用法律法规、个人信息保护要求、CPS1 和服务协议处理。

机构身份认证证书、设备身份认证证书、内网 SSL/TLS 服务器证书和私域内网 SSL 证书主体名称体现机构或责任主体，至少包含 CN、O、C 等必要字段。涉及统一社会信用代码、设备标识、内网域名、内网 IP 地址、系统名称或服务名称的，按照适用标准、申请材料和 CPS1 处理。

测试证书主体名称与正式业务证书相区分。测试证书的主体名称、组织名称、用途标识或申请记录能够表明测试属性，且不得误导依赖方将其用于正式业务场景。

3.1.5. 名称唯一性

沃通在合理范围内确保证书主体名称与订户、设备、系统、内网服务或测试项目之间的对应关系清晰、可回溯。对于同一订户或同一系统在不同场景下申请多个证书的，通过证书序列号、申请记录、证书类型、用途记录或其他可审计信息区分。

3.1.6. 商标识别与角色

订户不得在证书主体名称中使用侵犯他人合法权益的名称、商标、字号、域名、标识或其他信息。沃通在合理范围内对申请信息进行审查；发现存在争议或可能侵权的，可要求订户补充证明材料、修改申请信息、暂停签发或拒绝签发。

3.2. 初始身份确认

3.2.1. 证明私钥拥有权的方法

申请本 CP 项下证书时，订户证明其拥有与证书公钥对应的私钥，或者证明密钥在其授权的受控环境中生成并由其控制。证明方式包括提交符合要求的证书签名请求、通过安全介质生成密钥、在服务器或设备端生成密钥、通过业务系统生成密钥，或 CPS1 认可的其他方式。

沃通不得接收、保存或要求订户提交明文私钥。任何人员不得以明文方式导出、复制、留存或转交订户私钥。

3.2.2. 个人身份认证证书身份鉴别

个人身份认证证书申请人提交能够证明其身份的有效信息。沃通对申请人的身份真实性、申请意愿和证书用途进行核验。

个人身份鉴别至少包括下列要素：

1. 申请人姓名、有效身份证件信息和联系方式；
2. 与申请人身份相关的在线核验、实名核验、证件核验或有效证书签名核验；
3. 申请人对证书用途、非电子签名法律适用性、责任限制和服务协议的主动确认；
4. 与证书签发记录关联保存的身份核验记录、申请记录和意愿确认记录。

3.2.3. 机构身份认证证书身份鉴别

机构身份认证证书申请人提交能够证明机构依法存在、申请人经机构授权、证书用途符合机构真实需求的材料或记录。沃通核验机构主体身份、授权关系、申请意愿和证书用途。

机构身份鉴别至少包括下列要素：

1. 机构名称、统一社会信用代码或依法登记信息；
2. 机构有效登记状态或主体资格证明；
3. 经办人身份信息和机构授权关系；
4. 机构对证书用途、非电子签名法律适用性、责任限制和服务协议的主动确认；
5. 与证书签发记录关联保存的机构核验记录、授权记录、申请记录和意愿确认记录。

3.2.4. 设备身份认证证书身份鉴别

设备身份认证证书申请人为设备所属机构、设备运营方或经授权的系统责任主体。沃通确认申请机构主体身份、设备或服务节点归属、设备标识、使用场景和申请意愿。

设备身份鉴别至少包括下列要素：

1. 设备所属机构或责任主体的身份信息；
2. 设备标识、服务节点标识、系统名称或其他可识别设备的申请信息；
3. 申请机构对设备或服务节点的控制权、管理权或授权使用权声明；
4. 证书用途、接入范围和限制条件；
5. 与证书签发记录关联保存的主体核验、设备归属或控制权确认、授权和意愿确认记录。

3.2.5. 内网 SSL/TLS 服务器证书身份鉴别

内网 SSL/TLS 服务器证书申请人为服务器、服务节点、内网域名、内网 IP 地址或专用网络服务的所属机构或授权运营方。沃通核验申请机构主体身份、经办人授权关系、内网服务用途和申请意愿。

对于内网域名、内网 IP 地址、服务节点归属、部署环境等位于申请机构内网或私有网络、沃通无法独立核实的信息，申请机构在申请材料、服务协议或系统确认记录中承诺其真实性、合法性和使用权。沃通留存该承诺与申请材料。

内网 SSL/TLS 服务器证书不得面向公众互联网信赖使用，不得用于公共信任 SSL/TLS 服务。

3.2.6. 私域内网 SSL 证书身份鉴别

SM2 私域内网 SSL 证书和 RSA 私域内网 SSL 证书申请人为私有网络、内网服务、专用系统或约定业务环境的所属机构或授权运营方。沃通核验申请机构主体身份、经办人授权关系、内网或私有网络用途、证书使用边界和申请意愿。

私域内网 SSL 证书身份鉴别至少包括下列要素：

1. 申请机构主体身份和经办人授权关系；
2. 内网域名、内网 IP 地址、服务节点或系统名称；
3. 申请机构对内网资源、私有网络资源或服务节点的合法使用权声明；
4. 证书仅限内网、私有网络或约定系统环境使用的确认；
5. 证书不作为公共信任 SSL/TLS 证书、不面向公众互联网依赖方使用的确认；
6. 与证书签发记录关联保存的申请材料、主体核验记录、授权记录、用途确认和限制确认记录。

私域内网 SSL 证书申请材料至少包括：证书申请表或线上申请记录、申请机构主体资格材料、经办人身份证明、经办人授权文件、内网域名或内网 IP 地址清单、服务器或服务节点信息、证书签名请求或公钥材料、内网资源合法使用权或控制权声明、内网部署环境说明、仅限内网使用承诺、不得用于公众互联

网信赖场景的风险知情确认、服务协议或接入协议确认记录。申请机构对内网资源、私有网络资源、服务节点和证书用途的真实性、合法性和授权范围负责。

沃通无法通过公共域名系统或公开互联网资源独立验证的内网域名、内网 IP 地址、服务节点和部署环境，以申请机构的书面声明、协议确认、系统申请记录、授权文件和必要的人工审核记录作为核验依据。材料不能证明申请机构对内网资源具有合法使用权、控制权或授权使用权的，不得签发私域内网 SSL 证书。

3.2.7. 测试证书身份鉴别

测试证书仅用于测试、接口联调、验收、演示或内部试运行。沃通确认申请人、测试项目、测试用途、测试期限、审批人、测试环境和禁止正式使用声明。

测试证书身份鉴别至少包括下列要素：

1. 申请人或申请机构信息；
2. 测试项目、测试系统或测试场景说明；
3. 测试期限和测试环境；
4. 审批或授权记录；
5. 禁止用于生产业务、公众服务、对外交易或法律效力主张的确认；
6. 与证书签发记录关联保存的申请、审批、用途说明和测试环境隔离记录。

3.2.8. 订户告知与意愿确认

沃通在证书申请、服务协议、接入协议或业务系统受理流程中向订户明确告知下列事项：

1. 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；
2. 本 CP 项下证书不得用于主张可靠电子签名效力；
3. 内网 SSL/TLS 服务器证书和私域内网 SSL 证书不得用于公共信任 SSL/TLS 服务；

4. 测试证书不得用于生产业务、公众服务、对外交易或法律效力主张；

5. 订户对申请信息真实性、证书使用合规性和私钥安全承担责任。

强制阅读、页面展示或协议展示不得单独构成意愿确认。意愿确认结合短信验证码、勾选确认、电子签名确认、音视频确认、服务协议签署、系统审批、接口调用确认或其他能够体现订户主动确认的方式，并与证书签发记录关联保存。

3.2.9. 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身份信息写入证书。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。

3.2.10. 授权确认

机构订户由经办人申请证书的，沃通查验经办人身份及其代表机构申请、领取、使用或管理证书的授权文件。授权文件与证书申请记录一并保存。

3.2.11. 互操作准则

本 CP 项下证书参与业务系统互认、平台接入、私有网络验证、接口联调或跨系统验证时，遵循下列准则：

1. 沃通负责按照本 CP 和 CPS1 签发、管理、撤销证书并提供证书状态服务；

2. 订户负责向接入系统、平台或依赖方说明证书用途限制、适用范围和法律适用性；

3. 第三方平台或业务系统不得扩大解释本 CP 项下证书的用途，不得将其用于电子签名认证证书或公共信任 SSL/TLS 证书场景；

4. 依赖方在信赖证书前，验证证书链、证书有效期、证书用途、证书策略、证书状态和适用场景；

5. 跨系统验证或互操作结果不改变本 CP 确定的策略边界和责任边界。

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，按照 CPS1 要求重新证明私钥拥有权，并根据证书类型完成必要的身份确认、授权确认、用途确认和意愿确认。测试证书不得通过密钥更新方式转为正式业务证书。

3.4. 撤销请求的标识与鉴别

撤销请求人提交能够证明其身份、授权关系或控制关系的材料或记录。沃通在处理撤销请求前，按照 CPS1 对请求人身份、授权关系、撤销原因和证书信息进行核验。私钥泄露、密钥失控、证书信息错误、订户授权终止、证书被误用或证书用途不符合本 CP 的，及时发起撤销请求。

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个人、机构、设备所属机构、系统运营方、内网服务运营方、私有网络服务运营方、测试项目申请方或经授权代表。申请实体按照证书类型提交申请信息、身份证明、机构证明、授权材料、用途说明、系统或设备信息以及 CPS1 要求的其他材料。

4.1.2. 注册过程与责任

沃通或注册机构在受理申请前告知订户证书用途、使用限制、法律适用性、费用、私钥保护责任、撤销条件、证书状态查询方式和争议处理方式。订户保证申请信息真实、完整、准确，并对证书使用行为承担相应责任。

4.2. 证书申请处理

4.2.1. 识别与鉴别

沃通按照第 3 章和 CPS1 对申请实体身份、授权关系、证书用途、私钥拥有权和意愿确认进行识别与鉴别。对内网 SSL/TLS 服务器证书、私域内网 SSL 证书和测试证书，特别核验证书使用范围、环境限制和禁止用途确认。

4.2.2. 批准条件

符合下列条件的，沃通可以批准证书申请：

申请材料齐备并符合对应证书类型要求；

身份鉴别、授权关系确认、用途确认和意愿确认通过；

证书主体名称、证书用途、证书策略和有效期符合本 CP、CPS1 和适用标准；

未发现虚假申请、冒用身份、越权申请、违规用途或其他不适宜签发情形；

申请人已确认非电子签名法律适用性、用途限制和相关责任。

4.2.3. 拒绝条件

存在下列情形之一的，沃通拒绝或暂停证书申请：

申请材料不真实、不完整或无法核验；

申请人身份、机构主体、授权关系、设备归属、内网资源使用权或测试用途无法确认；

申请用途超出本 CP 允许范围；

申请人拒绝确认非电子签名法律适用性、用途限制或服务协议；

证书主体名称可能误导依赖方或侵犯第三方合法权益；

存在安全风险、合规风险、争议风险或监管要求禁止签发的情形。

4.2.4. 处理时限

沃通在收到完整申请材料并完成必要核验后及时处理证书申请。常规证书申请原则上在 2 个工作日内完成处理；测试证书、项目接入证书或批量申请可按服务协议或业务系统约定执行。因补充材料、授权复核、安全风险排查、合规审查或异常争议导致处理时间延长的，沃通告知申请人延长原因、预计处理时间并保留处理记录。

4.3. 证书签发

4.3.1. 签发期间电子认证服务机构的行为

沃通在证书签发前确认申请已获批准，证书主体信息、证书策略、密钥用法、扩展项、有效期、证书链和证书用途符合本 CP、CPS1 和适用标准。证书签发过程纳入权限控制、操作留痕和审计管理。

4.3.2. 证书签发后通知订户

证书签发后，沃通通过业务系统、申请渠道、邮件、短信、接口回执或其他合理方式通知订户。通知内容包括证书签发结果、证书下载或获取方式、证书用途限制、证书状态查询方式和订户接受或异议处理方式。

4.4. 证书接受

订户在下载、安装、启用、调用或实际使用证书前，核对证书主体名称、证书类型、证书用途、证书有效期、证书策略、证书链和其他重要信息。订户发现证书信息错误、用途不符或不具备签发条件的，在 5 个工作日内或证书首次使用前向沃通提出异议；证书一经启用、调用或用于业务验证，即视为订户接受证书。

对测试证书，订户在使用前确认测试用途、测试期限和禁止正式使用声明。对私域内网 SSL 证书，订户在部署前确认其仅用于内网、私有网络或约定系统环境。

4.5. 密钥对和证书的使用

4.5.1. 订户私钥和证书的使用

订户按照本 CP、CPS1、证书用途、证书扩展项和服务协议使用证书和私钥。订户采取合理措施保护私钥、激活数据、设备、服务器、业务系统和访问权限，防止私钥泄露、丢失、被篡改或被未授权使用。

4.5.2. 依赖方公钥和证书的使用

依赖方在信赖本 CP 项下证书前，验证证书链、证书有效期、证书用途、证书策略、主体信息、撤销状态和适用场景。依赖方不得在本 CP 允许范围之外信赖证书，不得将测试证书、内网 SSL/TLS 服务器证书或私域内网 SSL 证书用于公开信任、正式交易或法律效力主张。

4.6. 证书更新

4.6.1. 证书更新情形

证书即将到期且证书主体信息、证书用途、证书策略、授权关系和密钥仍符合本 CP 要求的，订户可按照 CPS1 申请证书更新。测试证书不得通过更新方式延长为正式业务证书；测试需求持续存在的，按测试审批流程重新申请。

4.6.2. 请求证书更新的实体

证书更新请求可由订户、经授权代表、设备所属机构、系统运营方或 CPS1 认可的其他授权主体提出。沃通核验请求实体的身份、授权关系和证书更新条件。

4.6.3. 证书更新处理

沃通确认原证书未被撤销、未超出允许更新范围、订户信息和用途限制仍然有效，并根据证书类型完成必要的身份复核、授权复核和意愿确认。证书更新后的有效期不得超过本 CP 规定的对应证书类型最长有效期。

4.6.4. 更新证书通知、接受和发布

更新证书签发后，沃通通知订户。订户按照第 4.4 条核对并接受更新证书。更新证书的发布、状态服务和对其他实体的通告按照 CPS1、服务协议和本 CP 第 2 章、第 7 章执行。

4.7. 证书密钥更新

4.7.1. 证书密钥更新情形

证书密钥到期、私钥保护环境变更、密钥算法或长度要求变化、私钥存在疑似风险或订户需要更换密钥的，申请证书密钥更新。发生私钥泄露、密钥失控或存在重大安全风险的，优先申请撤销原证书，并重新申请证书。

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、经授权代表、设备所属机构、系统运营方或 CPS1 认可的其他授权主体提出。沃通核验请求实体身份、授权关系、新密钥私钥拥有权和证书用途。

4.7.3. 证书密钥更新处理

证书密钥更新使用新的密钥对。沃通按照初始申请或 CPS1 规定的复核流程确认订户身份、授权关系、用途限制和意愿确认，并签发包含新公钥的证书。原证书的撤销、保留或到期处理按照 CPS1 和服务协议执行。

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。订户按照第 4.4 条核对并接受证书。密钥更新证书的发布、状态服务和对其他实体的通告按照 CPS1、服务协议和本 CP 第 2 章、第 7 章执行。

4.8. 证书变更

4.8.1. 证书变更情形

订户主体名称、机构信息、设备信息、内网服务信息、证书用途、授权关系或其他证书载明信息发生变化，且变化影响证书真实性、准确性或适用范围的，订户申请证书变更或重新申请证书。

4.8.2. 请求证书变更的实体

证书变更请求可由订户、经授权代表、设备所属机构、系统运营方或 CPS1 认可的其他授权主体提出。沃通核验请求实体身份、授权关系、变更事项和证明材料。

4.8.3. 证书变更处理

证书变更涉及证书主体名称、公钥、证书用途、证书策略、有效期或重要扩展项变化的，重新签发证书。原证书是否撤销由 CPS1 根据变更性质、安全风险和业务影响确定。

4.8.4. 变更证书通知、接受和发布

变更证书签发后，沃通通知订户。订户按照第 4.4 条核对并接受变更证书。变更证书的发布、状态服务和对其他实体的通告按照 CPS1、服务协议和本 CP 第 2 章、第 7 章执行。

4.9. 证书吊销和挂起

4.9.1. 证书吊销情形

发生下列情形之一的，沃通撤销或可撤销本 CP 项下证书：

1. 订户申请撤销证书；
2. 订户私钥泄露、疑似泄露、丢失、被盗、被未授权使用或不再受控；
3. 证书主体信息错误、失实、过期或不再有效；

4. 订户授权关系终止、机构注销、设备退役、系统停止使用或内网服务终止；

5. 证书被用于超出本 CP 允许范围的用途；

6. 私域内网 SSL 证书被用于公众互联网或公共信任 SSL/TLS 服务；

7. 测试证书被用于生产业务、公众服务、对外交易或法律效力主张；

8. 沃通发现证书签发、使用或管理存在安全风险、合规风险或监管要求撤销的情形；

9. 法律法规、监管要求、法院或仲裁机构生效文书、服务协议或 CPS1 规定的其他撤销情形。

4.9.2. 吊销请求实体

证书吊销请求可由订户、经授权代表、设备所属机构、系统运营方、依赖方、监管机构、司法机关、仲裁机构或 CPS1 认可的其他主体提出。沃通也可在发现证书存在撤销情形时主动撤销证书。

4.9.3. 证书吊销请求流程

吊销请求人通过沃通公布的渠道或 CPS1 规定的方式提交吊销请求，并提供证书信息、请求人身份信息、授权证明、吊销原因和必要证明材料。沃通核验请求人身份、授权关系和吊销原因；对私钥泄露、密钥失控、违规使用或重大安全风险情形，优先处理。

订户发现私钥泄露、疑似泄露、丢失、被盗或被未授权使用的，立即停止使用相关证书，并尽快向沃通提交吊销请求。因迟延提交吊销请求导致的损失，由责任方依法承担。

4.9.4. 证书吊销请求处理时间

沃通在完成必要核验后及时处理证书吊销请求。对私钥泄露、密钥失控、证书误用、测试证书违规使用、私域内网 SSL 证书违规对外使用或其他重大安全风险情形，按照紧急流程处理。吊销生效后，沃通在 24 小时内更新证书撤销列表，并通过在线证书状态服务反映撤销状态。

4.9.5. 依赖方检查证书吊销的要求

依赖方在信赖本 CP 项下证书前，查询证书状态，不得信赖已撤销、已过期、挂起、用途不符或证书链无法验证的证书。对内网 SSL/TLS 服务器证书和私域内网 SSL 证书，依赖方同时确认其部署环境和信赖范围符合内网、私有网络或约定系统环境。

4.9.6. 证书撤销列表发布频率

国家根体系下用户证书撤销列表至少每 24 小时发布一次；私域内网 SSL 体系下用户证书撤销列表至少每 7 天发布一次。证书被撤销后，沃通在 24 小时内发布更新的证书撤销列表。具体发布地址见第 7.2 条。

4.9.7. 证书挂起和恢复

本 CP 项下证书可按照 CPS1 提供证书挂起和恢复服务。证书挂起适用于证书使用权、授权关系、私钥控制、设备状态、内网服务状态、测试用途或证书信息存在短期不确定性，但尚未达到必须撤销条件的情形。

证书挂起请求可由订户、经授权代表、设备所属机构、系统运营方、沃通或 CPS1 认可的其他主体提出。挂起期间，订户不得继续使用证书，依赖方不得信赖挂起证书。挂起原因消除并经沃通核验后，按照 CPS1 恢复证书；挂起原因无法消除或证书已不符合本 CP 要求的，撤销证书。

证书挂起最长持续期限不得超过 30 个自然日；CPS1、服务协议或特定业务规则规定更短期限的，从其规定。恢复证书前，沃通重新核验挂起原因已经消除，并根据挂起原因复核订户身份、授权关系、设备状态、内网服务状态、测试用途、私钥控制状态或证书信息。挂起期限届满仍不能满足恢复条件的，撤销证书或按照 CPS1 启动重新申请流程。恢复、撤销或继续处理结果通知订户，并保存处理记录。

4.10. 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证书状态查询服务。证书状态服务支持依赖方查询证书是否处于有效、撤销、挂起、过期或未知状态。

证书状态服务原则上提供 7×24 小时查询能力。国家根体系在线证书状态服务地址为 http://ocsp2.wotrus.com/；私域内网 SSL 体系在线证书状态服务地址为 http://ocsp.wotrus.com。当在线状态服务异常时，依赖方可通过证书撤销列表或沃通公布的备用渠道进行状态验证。服务可用率目标和异常期间处理规则由 CPS1 规定。

4.11. 订购结束

证书到期、撤销、订户终止服务、服务协议终止、测试项目结束、内网服务停用或其他订购结束情形发生时，订户停止使用相关证书和私钥。沃通按照 CPS1 保留证书、申请材料、状态记录和审计记录。

4.12. 密钥托管和恢复

本 CP 项下订户签名私钥、身份认证私钥、设备私钥、服务器私钥和测试证书私钥原则上由订户或其授权系统自行控制，沃通不得托管、恢复或以明文方式接触订户私钥。

如业务场景涉及加密用途密钥、密钥备份、密钥恢复或会话密钥封装，在符合法律法规、密码管理要求、服务协议、CPS1 和安全策略委员会批准规则的前提下实施。签名用途私钥不得以恢复签名能力为目的进行托管或恢复。

5. 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身份认证通用证书服务场所，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。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、证书状态服务、密钥管理、系统运维、策略变更和应急处置执行职责分离、权限审批、双人或多人控制、操作复核、变更管理、发布管理和审计追踪。关键操作纳入授权、审批、记录和审计管理；涉及私域内网 SSL、测试证书或设备身份认证场景的业务，按照 CPS1 留存资源权属、授权、用途确认和审批记录。

5.3. 人员控制

沃通对参与本 CP 项下证书服务的人员实施身份背景核验、岗位授权、保密承诺、培训、权限管理、岗位变更管理和离岗管理。关键岗位人员具备身份认证通用证书服务运行、密码安全管理、主体核验、私域资源权属核验、测试业务隔离和证书状态服务管理所需能力；授权前完成岗位培训，在岗期间接受持续培训和权限复核。

5.4. 审计日志程序

沃通记录申请受理、身份核验、授权确认、证书签发、证书下载、证书撤销、证书挂起、证书恢复、状态查询、系统管理、密钥管理、权限变更、安全事件和异常操作等日志。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，防止未授权访问、修改、删除或覆盖。

5.5. 记录归档

沃通归档证书申请材料、身份核验记录、内网资源权属确认、测试审批记录、授权记录、用途确认、告知确认、证书签发记录、撤销记录、状态服务记录和审计日志。本 CP 项下证书服务记录至少保存至对

应证书失效后 5 年；测试证书审批记录与审计日志保存期限同正式业务证书。法律法规、监管、审计或争议处理要求更长期限的，按更长期限保存。

5.6. 密钥变更

沃通 CA 密钥、证书状态服务密钥和其他关键密钥的变更执行风险评估、审批、生成、启用、公告、迁移、备份、状态服务联动和审计程序。订户密钥变更按照第 4.7 条和 CPS1 执行；涉及私域内网 SSL、测试证书、设备身份认证或证书链变化的，沃通同步完成影响评估、公告或通知以及证书链发布。

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、审计日志和相关支撑系统。发生系统故障、密钥风险、数据损坏、证书误签、状态服务异常、网络攻击或其他重大事件时，沃通按照 CPS1 启动应急处置、影响评估、业务恢复、状态更新、通知报告和记录留存流程。

5.8. CA 或 RA 的终止

沃通终止本 CP 项下身份认证通用证书服务时，按照法律法规、监管要求和 CPS1 处理订户通知、证书撤销或迁移、记录移交、状态服务延续、公告和善后事项。涉及终止电子认证服务的，沃通至少提前 90 日通知有关各方，并至少提前 60 日向主管部门报告。

6. 技术安全控制

6.1. 密钥对的生成和安装

6.1.1. 密钥对生成

本 CP 项下证书密钥对根据证书类型和业务场景在订户安全介质、客户端、服务器、设备、密钥管理系统、密码模块或其他受控环境中生成。CA 密钥和证书状态服务密钥在符合密码管理要求的受控密码设备或等效安全环境中生成，生成过程执行授权审批、多人控制、操作见证和审计记录。

6.1.2. 私钥传送

订户签名私钥原则上不传送。因加密证书、密钥管理或业务系统部署需要进行密钥封装、备份、恢复、导入、导出或迁移的，沃通和订户采用加密、访问控制、操作授权、安全通道和审计记录措施，不以明文方式传送私钥。

6.1.3. 公钥传送

订户公钥通过证书签名请求、业务系统接口、设备接入流程或 CPS1 认可的其他方式提交给沃通。沃通确认公钥格式、算法、长度、参数质量、主体身份和证书用途符合本 CP、CPS1 和适用标准后再签发证书。

6.1.4. CA 公钥传送给依赖方

沃通通过官网、证书链发布地址、证书扩展项载明地址或其他可信渠道向依赖方提供根证书、中级根证书和证书链信息。依赖方从沃通公布或证书载明的可信地址获取证书链并完成路径验证。

6.1.5. 密钥长度和参数质量

本 CP 项下证书使用符合国家密码管理要求、适用标准和 CPS1 的算法、密钥长度和参数。沃通在签发证书前检查公钥算法、密钥长度和参数质量，不符合要求的申请不进入签发环节。

6.2. 私钥保护和密码模块工程控制

6.2.1. 私钥保护要求

订户使用安全介质、安全芯片、服务器密码机、加密存储、访问控制、强口令、多因素认证或其他合理措施保护私钥。任何人员不得以明文方式导出、复制、留存或转交订户签名私钥。

CA 私钥和证书状态服务私钥在符合密码管理要求的密码设备或等效安全环境中生成、保存和使用，并实施分权控制、操作审计和备份保护。

6.2.2. 私钥多方控制

CA 私钥生成、备份、恢复、销毁和重大密钥操作采用多方控制和职责分离机制。单个操作人员不得独立完成影响 CA 私钥安全的关键操作。

6.2.3. 私钥备份与归档

CA 私钥备份采用加密、分权、访问控制和安全介质保护。订户签名用途私钥不由沃通托管或归档。加密用途密钥的备份、归档和恢复按照 CPS1、服务协议和安全策略委员会批准规则执行。

6.2.4. 私钥导入和导出

CA 私钥导入、导出限于安全批准的密钥管理操作，并在受控密码设备或等效安全环境中进行。订户私钥导入、导出由订户按照其安全策略、服务协议和 CPS1 负责管理，不以明文方式导入、导出或传输。

6.2.5. 私钥销毁

证书不再使用、测试项目结束、设备退役、服务器下线或私钥存在安全风险时，订户销毁或停止使用相关私钥。CA 私钥销毁经过审批、见证、记录和审计。

6.3. 密钥对管理的其他方面

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、密钥备份和密钥销毁。订户按照证书类型、服务协议和自身安全策略管理订户密钥生命周期。CA 密钥停用或替换后，沃通继续保存历史验证所需证书链、撤销状态和归档材料。

6.4. 激活数据

6.4.1. 激活数据生成和安装

激活数据包括用于激活私钥、安全介质、服务器密钥、设备密钥或测试环境、业务系统密钥的口令、PIN、密钥份额、令牌或其他认证数据。激活数据由授权人员或受控系统生成，并采用复杂度、随机性、防猜测、防泄露和防未授权使用控制。

6.4.2. 激活数据保护

订户和沃通相关人员保护激活数据，不共享、不明文保存、不通过不安全渠道传输、不交由未授权人员使用。激活数据遗失、泄露或疑似泄露时，立即采取更换、停用、挂起、撤销或其他风险控制措施。

6.4.3. 激活数据其他方面

激活数据在证书、密钥或设备生命周期结束后及时停用、销毁或失效。激活数据的恢复、重置和变更经过授权、身份核验和记录留存。

6.5. 计算机安全控制

沃通对证书服务相关系统实施身份鉴别、访问控制、最小权限、系统加固、漏洞管理、恶意代码防护、日志审计、备份恢复、变更控制和安全监测。测试证书相关系统与正式业务系统保持必要隔离。系统运行期间开展漏洞扫描、必要的渗透测试和安全加固；重大漏洞修复后执行复测并留存证据。

6.6. 生命周期技术控制

沃通对证书服务系统的软件开发、测试、上线、变更、版本发布、配置管理、安全评估、漏洞修复和退役进行全生命周期技术控制。涉及证书策略、证书格式、证书状态服务、安全控制的重要变更经过评估、审批、验证和记录。

6.7. 网络安全控制

沃通对证书服务网络实施网络区域划分、边界防护、访问控制、入侵检测或防护、流量监测、远程访问控制和安全审计。证书签发系统、证书状态服务、目录服务、密钥管理系统和测试环境、私域内网 SSL 支撑系统和管理网络按安全级别实施隔离和访问控制，并采用防火墙、恶意代码防护、漏洞扫描、数据备份和灾难恢复措施。

6.8. 时间戳

沃通证书服务相关系统保持可靠时间源，并记录证书签发、撤销、挂起、恢复、状态服务、日志归档和安全事件的时间。系统时间同步、时间记录和时间审计要求由 CPS1 规定。

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. 版本

本 CP 项下证书采用 X.509 v3 证书格式。

7.1.2. 证书链与公开服务地址

本 CP 项下证书适用下列公开证书链和服务地址：

证书类型	证书链	证书撤销列表地址	在线状态服务地址	CA 证书访问地址
个人身份认证证书、机构身份认证证书、设备身份认证证书、内网 SSL/TLS 服务器证书、测试证书	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
SM2 私域内网 SSL 证书	WoTrus SM2 Private SSL Root → WoTrus SM2 Private SSL CA → 订户证书	http://crl.wotrus.com/sm2_private_ssl_ca.crl	http://ocsp.wotrus.com	http://aia.wotrus.com/sm2_private_ssl_root.cer
RSA 私域内网 SSL 证书	WoTrus RSA Private SSL Root → WoTrus RSA Private SSL CA → 订户证书	http://crl.wotrus.com/rsa_private_ssl_ca.crl	http://ocsp.wotrus.com	http://aia.wotrus.com/rsa_private_ssl_root.cer

私域内网 SSL 中级 CA 证书由相应顶级根签发。上表所列 CA 证书访问地址为当前资料中确认的上级 CA 证书访问地址；订户证书或中级 CA 证书的颁发机构信息访问扩展项另有载明的，以证书实际 AIA 扩展项为准。CPS1 与证书实际配置保持一致；证书扩展项中未明确载明的中级 CA 证书访问地址不得在本 CP 中推定补写。

7.1.3. 证书类型

本 CP 项下证书类型如下：

证书类型	策略对象标识符	适用 CPS	用途边界
个人身份认证证书	1.2.156.150570.6.4	CPS1	个人身份识别和客户端身份验证，不用于电子签名认证证书场景。
机构身份认证证书	1.2.156.150570.6.4	CPS1	机构身份识别和客户端身份验证，不用

			于电子签名认证证书场景。
设备身份认证证书	1.2.156.150570.6.4	CPS1	设备、终端、服务节点或系统组件身份识别和接入控制。
内网 SSL/TLS 服务器证书	1.2.156.150570.6.4	CPS1	内网服务器、内网服务或专用网络环境中的服务器身份识别和通道加密。
SM2 私域内网 SSL 证书	1.2.156.150570.6.4	CPS1	SM2 私域内网 SSL 体系下的内网或私有网络通信。
RSA 私域内网 SSL 证书	1.2.156.150570.6.4	CPS1	RSA 私域内网 SSL 体系下的内网或私有网络通信。
测试证书	1.2.156.150570.3.3.1	CPS1	测试、接口联调、验收、演示或内部试运行，不得用于正式业务。

7.1.4. 证书主体名称

个人身份认证证书主体名称体现个人身份识别信息。机构身份认证证书、设备身份认证证书、内网 SSL/TLS 服务器证书和私域内网 SSL 证书主体名称体现机构或责任主体。测试证书主体名称体现测试属性并与正式业务证书相区分。

内网 SSL/TLS 服务器证书和私域内网 SSL 证书在主体名称或主体备用名称扩展项中载明与申请材料一致的内网域名、内网 IP 地址、服务节点或系统名称。证书主体名称不得误导依赖方将本 CP 项下证书理解为电子签名认证证书或公共信任 SSL/TLS 证书。

7.1.5. 算法对象标识符

本 CP 项下 SM2 证书使用符合 GM/T 0003、GM/T 0015、GM/T 0034 和相关国家密码标准的 SM2/SM3 算法对象标识符。RSA 私域内网 SSL 证书使用符合适用标准的 RSA 签名算法对象标识符。具体算法对象标识符以证书实际编码、CPS1 和适用标准为准。

7.1.6. 密钥用法和扩展密钥用法

本 CP 项下证书密钥用法和扩展密钥用法符合证书类型和用途限制：

证书类型	密钥用法	扩展密钥用法
个人身份认证证书	数字签名、密钥加密	客户端身份验证 1.3.6.1.5.5.7.3.2
机构身份认证证书	数字签名、密钥加密	客户端身份验证 1.3.6.1.5.5.7.3.2
设备身份认证证书	数字签名、密钥加密、密钥协商	客户端身份验证 1.3.6.1.5.5.7.3.2，可按用途包含服务器身份验证 1.3.6.1.5.5.7.3.1
内网 SSL/TLS 服务器证书	数字签名、密钥加密、密钥协商	服务器身份验证 1.3.6.1.5.5.7.3.1，可按用途包含客户端身份验证 1.3.6.1.5.5.7.3.2
SM2 私域内网 SSL 证书	数字签名、密钥加密、密钥协商，具体以证书类型和算法要求确定	服务器身份验证 1.3.6.1.5.5.7.3.1，可按用途包含客户端身份验证 1.3.6.1.5.5.7.3.2
RSA 私域内网 SSL 证书	数字签名、密钥加密，具体以证书类型和算法要求确定	服务器身份验证 1.3.6.1.5.5.7.3.1，可按用途包含客户端身份验证 1.3.6.1.5.5.7.3.2
测试证书	数字签名、密钥加密	客户端身份验证 1.3.6.1.5.5.7.3.2，不得用于正式业务

本 CP 项下证书的密钥用法不得使依赖方误认为证书属于电子签名认证证书。私域内网 SSL 证书新签发、更新、密钥更新或重新签发时，使用 CP4 策略对象标识符和目录级 CPS URI，并按非电子签名认证证书口径去除会使依赖方误认为可用于电子签名认证证书场景的密钥用法。历史存量证书按签发时证书实际扩展项和当时服务协议限定用途维护至自然到期；发生证书更新、密钥更新、证书变更或重新签发的，切换至本 CP 的新策略对象标识符、CPS URI 和密钥用法口径。

历史证书与新签发证书密钥用法存在差异的，不得据此扩大历史证书用途，不得将私域内网 SSL 证书宣传或使用为电子签名认证证书。依赖方以证书实际扩展项、证书状态和本 CP 限定用途判断是否信赖证书。

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扩展项：

1. 基本约束；

2. 密钥用法；
3. 扩展密钥用法；
4. 主体密钥标识符；
5. 颁发机构密钥标识符；
6. 主体备用名称；
7. 证书策略；
8. 证书撤销列表分发点；
9. 颁发机构信息访问；
10. 符合适用标准和 CPS1 的其他扩展项。

扩展项的关键性符合 X.509、GB/T 20518-2018、GM/T 0015-2023、CPS1 和证书实际用途要求。自定义扩展项不得改变本 CP 确定的证书用途、法律适用性和责任边界。

7.1.8. 证书有效期

本 CP 项下证书最长有效期如下：

证书类型	最长有效期	说明
个人身份认证证书	1827 天	最长不超过 5 年。
机构身份认证证书	1827 天	最长不超过 5 年。
设备身份认证证书	1827 天	最长不超过 5 年。
内网 SSL/TLS 服务器证书	1827 天	国家根体系下内网服务器证书，最长不超过 5 年。
SM2 私域内网 SSL 证书	1827 天	仅限内网、私有网络或约定系统环境。
RSA 私域内网 SSL 证书	1827 天	仅限内网、私有网络或约定系统环境。
测试证书	30 天	不可延长为正式业务证书。

证书有效期不得超过签发该证书的上级 CA 证书有效期，也不得超过本 CP、CPS1、服务协议或适用标准规定的限制。

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。

7.2.2. 证书撤销列表和扩展项

本 CP 项下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。证书撤销列表扩展项和条目扩展项按照 X.509、GB/T 20518-2018、GM/T 0015-2023 和 CPS1 处理。

国家根体系下证书撤销列表地址为 http://ldap.wotrus.com/crl/wotrussm2uca.crl。SM2 私域内网 SSL 证书撤销列表地址为 http://crl.wotrus.com/sm2_private_ssl_ca.crl。RSA 私域内网 SSL 证书撤销列表地址为 http://crl.wotrus.com/rsa_private_ssl_ca.crl。

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 或适用标准要求。

7.3.2. 在线证书状态协议扩展项

在线证书状态协议响应能够反映证书有效、撤销、挂起、未知或其他适用状态。在线证书状态协议请求和响应扩展项按照适用标准、CPS1 和服务运行规则处理。国家根体系在线状态服务地址为 http://ocsp2.wotrus.com/；私域内网 SSL 体系在线状态服务地址为 http://ocsp.wotrus.com。

8. 合规审计和其他评估

8.1. 审计和评估频率

沃通按照法律法规、监管要求、行业规范、CPS1 和内部制度要求对本 CP 项下证书服务开展合规审计、技术检查和风险评估。本 CP 至少每年进行一次适用性评审；证书服务、证书状态服务、密钥管理、测试证书隔离和私域内网 SSL 使用限制纳入定期审计范围。

8.2. 审计者身份和资质

审计者具备与电子认证服务、密码应用、信息安全、合规管理或相关领域相适应的专业能力和独立性。外部审计或评估机构具备适用法律法规、监管要求或行业规范要求的资质。

8.3. 审计者与被审计者关系

审计者保持客观、公正和独立。负责被审计活动日常操作的人员不得作为该活动的独立审计负责人。

8.4. 审计覆盖主题

审计覆盖主题包括本 CP、CPS1、证书申请受理、身份鉴别、授权确认、告知确认、证书签发、证书撤销、证书挂起、证书状态服务、证书格式、密钥管理、记录留存、访问控制、安全事件、业务连续性、测试证书隔离、私域内网 SSL 使用限制和信息发布等。

8.5. 结果沟通

审计或评估发现的问题形成记录并提交责任部门整改。沃通对整改计划、整改措施、整改期限、整改验证和证据留存进行闭环管理。涉及重大安全风险、重大合规风险、监管要求或依赖方利益的重要事项，按照 CPS1、法律法规和监管要求进行报告或公告。

8.6. 抽样、整改和证据留存

审计抽样覆盖不同证书类型、申请渠道、签发批次、撤销记录、状态服务记录、测试证书记录和私域内网 SSL 证书记录，并重点覆盖私域内网 SSL 的内网资源权属确认、仅限内网使用告知、风险知情确认、历史策略对象标识符切换和密钥用法配置。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。涉及私域内网 SSL 违规对外使用、私钥泄露、证书误用或重大配置变更的记录，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。整改关闭以申请材料补正、配置复核、证书扩展项核验、撤销或重新签发记录、状态服务记录、系统日志或复核结论等证据为基础；未完成整改闭环的，不得作为已关闭事项处理。审计材料、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. 其他业务和法律事项

9.1. 费用

本 CP 项下个人身份认证证书、机构身份认证证书、设备身份认证证书、内网 SSL/TLS 服务器证书和私域内网 SSL 证书费用按沃通公布的收费标准、服务协议、项目合同或商务协议执行。测试证书可免费提供或按测试协议约定收费。

本 CP 项下证书链下载、证书撤销列表查询、在线证书状态查询、CP 和 CPS 查阅等公开查询服务原则上免费提供。法律法规、监管要求、服务协议或专项服务另有约定的，从其约定。

9.2. 财务责任

沃通按照法律法规、监管要求、服务协议和 CPS1 建立与其电子认证服务相适应的责任风险保障机制。沃通不通过本 CP 排除或限制依法不得排除或限制的责任。订户和依赖方违反本 CP、CPS1、服务协议或适用法律法规造成损失的，依法承担相应责任。

9.3. 业务信息保密

沃通、注册机构、订户和其他参与者对在本 CP 项下证书服务中获知的非公开业务信息、技术信息、身份信息、授权信息、系统信息、内网信息、测试信息和安全信息承担保密义务，法律法规、监管要求或协议另有规定的除外。

9.4. 个人信息保护

沃通处理个人信息遵循合法、正当、必要、诚信原则，并按照适用个人信息保护法律法规、CPS1、隐私政策和服务协议处理。沃通采取合理安全措施保护个人信息，防止未经授权访问、泄露、篡改或丢失。

9.5. 知识产权

本 CP、CPS1、证书、证书撤销列表、证书状态服务、软件、系统、文档、商标、标识和相关资料的知识产权归属依法律法规、合同约定和权利归属规则确定。未经权利人授权，任何主体不得擅自复制、发布、篡改、冒用或用于超出授权范围的用途。

9.6. 陈述与保证

沃通承诺按照本 CP、CPS1、适用法律法规和监管要求提供证书服务。订户承诺其申请信息真实、完整、准确，证书用途合法合规，私钥和激活数据受到妥善保护。依赖方承诺在信赖证书前进行必要验证，并仅在本 CP 允许范围内信赖证书。

9.7. 担保免责

除法律法规、监管要求、本 CP、CPS1 或服务协议明确规定外，沃通不对超出本 CP 允许用途的证书使用、订户提供虚假信息、订户私钥管理不当、依赖方未履行验证义务、测试证书用于正式业务、私域内网 SSL 证书用于公众互联网或第三方违规使用证书所造成的损失承担责任。

本 CP 项下证书不属于电子签名认证证书，不作为可靠电子签名效力主张的证书来源。任何主体将本 CP 项下证书用于电子签名认证证书场景、公共信任 SSL/TLS 场景或其他超出本 CP 限定用途的，相关风险和责任由责任方依法承担。

9.8. 责任限制

沃通对本 CP 项下证书服务承担的责任范围、责任限额和赔偿程序按照法律法规、监管要求、CPS1、服务协议或项目合同执行。法律法规规定不得限制的责任，不因本 CP、CPS1 或服务协议而排除或减轻。

9.9. 赔偿

因沃通违反法律法规、本 CP、CPS1 或服务协议造成订户或依赖方损失的，沃通依法承担相应责任。因订户、依赖方或第三方违反本 CP、CPS1、服务协议、接入协议或适用法律法规造成沃通或其他主体损失的，责任方依法承担赔偿责任。

赔偿申请方提交赔偿申请、主体身份证明、证书信息、损失说明、损失证明、因果关系说明和联系方式。沃通收到材料后，在 5 个工作日内确认材料是否齐备；材料不齐备的，一次性告知补正事项。材料齐备后，沃通组织对证书签发、用途告知、状态服务、依赖方验证行为、损失事实和因果关系进行审核，并按照内部审批程序形成赔偿处理意见。

赔偿处理流程包括申请受理、材料完整性确认、事实核查、责任和因果关系认定、赔偿审批、赔付执行、归档复核和争议处理。赔付方式、责任限额、免赔情形和更细处理时限按照法律法规、CPS1、服务协议或项目合同执行；法律法规规定不得排除或限制的责任，不因服务协议或责任限额而排除或减轻。

9.10. 有效期限和终止

本 CP 自生效日期起实施，至被新版本替代或被沃通依法废止时终止。本 CP 终止不影响终止前已经产生的证书、记录、保密、责任、争议处理和法律义务。

9.11. 对参与者的个别通告与沟通

沃通可通过官网公告、业务系统通知、邮件、短信、接口回执、服务协议约定渠道或其他合理方式向订户、依赖方和相关参与者发布与本 CP 项下证书服务有关的通知。

9.12. 修订

本 CP 的修订由沃通安全策略委员会管理。涉及证书用途、法律适用性、证书策略对象标识符、证书链、证书状态服务、订户或依赖方重要权利义务的重大修订，经过评估、批准和发布程序。必要时，沃通按照法律法规或监管要求履行备案、报备或通知义务。

9.13. 争议处理

与本 CP 项下证书申请、签发、使用、撤销、状态查询、费用、责任或赔偿有关的争议，相关方可按照 CPS1、服务协议、接入协议或适用法律法规提交处理。

争议申请方提交争议事项说明、证书信息、主体身份证明、授权证明、相关证据材料和联系方式。沃通收到争议材料后，在合理期限内确认受理或告知补正。争议处理可通过协商、调解、投诉处理、监管机关处理、仲裁或诉讼方式进行。举证材料提供期限、协商期限、调解路径、收费或免费规则由 CPS1、服务协议或争议处理规则规定。

沃通收到争议申请材料后，在 5 个工作日内确认受理或告知补正。争议进入协商处理的，原则上自受理之日起 30 日内完成协商；因事实复杂、外部机构协查或监管程序需要延长的，向相关方说明原因。相关方收到补正或举证通知后，原则上在 10 个工作日内提交材料；逾期未提交且无正当理由的，按现有材

料处理。争议处理不收取争议受理费用；鉴定、第三方评估、仲裁、诉讼或服务协议另有约定的费用，按相应规则承担。

9.14. 适用法律

本 CP 的解释、适用和争议处理适用中华人民共和国法律法规。法律法规、监管要求、强制性标准或主管部门要求另有规定的，从其规定。

9.15. 符合适用法律

沃通、注册机构、订户、依赖方和其他参与者遵守与本 CP 项下证书服务相关的法律法规、监管要求、密码管理要求、个人信息保护要求、网络安全要求和合同义务。

9.16. 一般条款

本 CP 与 CPS1 共同构成本 CP 项下证书服务的策略和实施文件。CP 确定策略边界、证书用途、法律适用性和责任限制；CPS1 承担实施细则，不得改变本 CP 的策略结论。

如 CPS1、服务协议、业务规则或其他文件与本 CP 的策略边界不一致，提交沃通安全策略委员会处理。在安全策略委员会作出裁定前，不得以 CPS1 或其他实施文件扩大本 CP 项下证书用途、法律效力或信赖范围。

9.17. 其他条款

本 CP 未尽事项，按照 CPS1、服务协议、接入协议、适用法律法规、监管要求和沃通安全策略委员会批准的规则执行。涉及证书类型新增、证书链调整、用途边界变化、证书状态服务重大变化或重要例外事项的，经过评估、审批和发布程序。