沃通电子认证服务有限公司

沃通全球信任体系

证书策略（CP5）

版本：V1.0

发布日期：2026 年 11 月 25 日

生效日期：2026 年 11 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	版本发布	建立《沃通全球信任体系证书策略（CP5）》正文，明确 CP5 策略边界、证书类型、对象标识符、适用 CPS、生态信任来源、用途限制、状态服务、生命周期管理、审计评估、法律责任和发布管理要求。	沃通安全策略委员会	2026 年 11 月 25 日

版权声明

本文件所有版权归沃通电子认证服务有限公司所有。未经书面授权，本文件中所有的文字、图表不得以任何形式进行抄袭和出版。

声明

本 CP 全部或者部分支持下列标准、规范和信任计划要求：

- 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》
- 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》
- CA/Browser Forum Baseline Requirements（含 Ballot SC-081 有效期及复用期阶梯要求）
- CA/Browser Forum EV Guidelines
- CA/Browser Forum S/MIME Baseline Requirements
- WebTrust for Certification Authorities
- WebTrust SSL Baseline
- WebTrust Network Security
- Adobe Approved Trust List 相关政策
- 360 信创 SM2 根证书计划相关要求
- 《公共可信证书管理 SSL 服务器证书运营和管理要求》（草案）

目　录

声明 - 3 -
目　录 - 4 -
1. 引言 - 6 -
1.1 概述 - 6 -
1.2 文档名称与标识 - 6 -
1.3 PKI 参与者 - 7 -
1.4 证书应用 - 8 -
1.5 策略管理 - 10 -
1.6 定义和缩写 - 11 -
2. 信息发布与管理 - 12 -
2.1 信息库 - 12 -
2.2 认证信息的发布 - 12 -
2.3 发布时间或频率 - 13 -
2.4 信息库访问控制 - 13 -
3. 标识与鉴别 - 13 -
3.1 命名 - 14 -
3.2 初始身份确认 - 15 -
3.3 密钥更新请求的标识与鉴别 - 18 -
3.4 撤销请求的标识与鉴别 - 18 -
4. 证书生命周期操作要求 - 18 -
4.1 证书申请 - 18 -
4.2 证书申请处理 - 18 -
4.3 证书签发 - 19 -
4.4 证书接受 - 20 -
4.5 密钥对和证书的使用 - 20 -
4.6 证书更新 - 20 -
4.7 证书密钥更新 - 21 -
4.8 证书变更 - 22 -
4.9 证书吊销和挂起 - 22 -
4.10 证书状态服务 - 24 -
4.11 订购结束 - 25 -
4.12 密钥托管和恢复 - 25 -
5. 设施、管理和操作控制 - 25 -
5.1 物理控制 - 25 -
5.2 程序控制 - 25 -
5.3 人员控制 - 26 -
5.4 审计日志程序 - 26 -
5.5 记录归档 - 26 -
5.6 密钥变更 - 26 -
5.7 损害与灾难恢复 - 26 -
5.8 电子认证服务机构或注册机构的终止 - 27 -
6. 技术安全控制 - 27 -

6.1 密钥对的生成和安装 - 27 -
6.2 私钥保护和密码模块工程控制 - 28 -
6.3 密钥对管理的其他方面 - 29 -
6.4 激活数据 - 29 -
6.5 计算机安全控制 - 29 -
6.6 生命周期技术控制 - 29 -
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 -
7.2 证书撤销列表 - 36 -
7.3 在线证书状态协议 - 37 -
8. 合规审计和其他评估 - 37 -
8.1 审计和评估频率 - 37 -
8.2 审计者身份和资质 - 38 -
8.3 审计者与被审计者关系 - 38 -
8.4 审计覆盖主题 - 38 -
8.5 结果沟通 - 38 -
8.6 抽样、整改和证据留存 - 38 -
9. 其他业务和法律事项 - 39 -
9.1 费用 - 39 -
9.2 财务责任 - 39 -
9.3 业务信息保密 - 39 -
9.4 个人信息保护 - 39 -
9.5 知识产权 - 39 -
9.6 陈述与保证 - 39 -
9.7 担保免责 - 40 -
9.8 责任限制 - 40 -
9.9 赔偿 - 40 -
9.10 有效期限和终止 - 41 -
9.11 对参与者的个别通告与沟通 - 41 -
9.12 修订 - 41 -
9.13 争议处理 - 41 -
9.14 适用法律 - 41 -
9.15 符合适用法律 - 42 -
9.16 一般条款 - 42 -
9.17 其他条款 - 42 -

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《沃通全球信任体系证书策略（CP5）》（以下简称“本 CP”或“CP5”）规定沃通全球信任体系证书的策略边界、适用范围、证书类型、证书用途、生态信任来源、法律适用性、依赖方责任、公开发布和版本管理要求。

本 CP 适用于沃通全球信任电子认证服务体系下的公开信任 SSL/TLS 服务器证书、国密 SSL/TLS 服务器证书、国密客户端身份证书、国密时间戳证书、Adobe AATL 文档签名证书、S/MIME 电子邮件加密证书和单位身份类证书。上述证书分别服务于浏览器、操作系统、国密信任生态应用、Adobe 产品、邮件客户端或其他第三方生态信任环境。本 CP 不涵盖代码签名证书。

本 CP 项下全部证书（包括 SSL/TLS 服务器证书、国密客户端身份证书、国密时间戳证书、Adobe AATL 文档签名证书、S/MIME 电子邮件证书及单位身份类证书等）均不属于《中华人民共和国电子签名法》规定的电子签名认证证书，**不适用《中华人民共和国电子签名法》及其规定的可靠电子签名法律效力**。其信任效力来源于对应的生态信任计划、适用标准、订户协议、依赖方协议、产品信任库或服务协议。

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、生态信任边界和责任边界；CPS3《沃通全球信任电子认证业务规则》确定本 CP 项下证书的申请受理、主体核验、域名验证、邮箱控制权验证、文档签名验证、证书签发、撤销、状态查询、记录留存、审计评估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	《沃通全球信任体系证书策略（CP5）》
文档简称	CP5
CP 文档对象标识符	1.2.156.150570.6.5
适用 CPS	CPS3《沃通全球信任电子认证业务规则》
CPS 文档对象标识符	1.2.156.150570.7.3
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全球信任体系证书策略。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。

公开信任 SSL/TLS 服务器证书、国密信任生态证书、Adobe AATL 文档签名证书、S/MIME 电子邮件证书或其他生态信任证书，如对应信任计划要求配置特定验证级别对象标识符，同时按照对应信任计划、CPS3 和证书实际用途配置。不得使用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。沃通按照适用信任计划、行业规范和 CPS3 接受必要审计、评估、根计划监督或生态信任计划管理。

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、域名控制权验证、邮箱控制权验证、AATL 身份验证、订户告知、授权关系确认和证书生命周期请求处理。注册机构的职责、权限和操作要求由 CPS3 规定。

1.3.3 订户

订户是申请并持有本 CP 项下证书的域名持有人、网站运营者、服务器运营方、机构、个人、邮箱控制人、文档签名主体、时间戳服务运营方、单位身份主体或其他经授权主体。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 项下证书进行服务器身份验证、加密通信、客户端身份验证、文档签名验证、邮件加密或签名验证、时间戳验证、单位身份验证或其他生态信任判断的个人、机构、软件、系统或服务。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、主体信息和适用生态环境。

1.3.5 其他参与者

其他参与者包括浏览器厂商、操作系统厂商、应用软件厂商、Adobe 产品生态、邮件客户端、国密信任生态相关软件或平台、根计划运营方、WebTrust 审计机构、合作中级根/外部子 CA 运营方、证书状态服务、目录服务、归档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 CPS3、信任计划规则、服务协议、接入协议和适用法律法规为准。

凡处于 360 计划、WebTrust、Adobe AATL 或其他生态信任承诺范围内的根及其内外部子 CA，须在公开 CP 及 CPS 中清晰列明根证书体系、子 CA 范围、版本与生效时间，并每年至少更新一次；外部运营子 CA 仅限非电子签名口径业务，严禁签发《中华人民共和国电子签名法》项下电子签名认证证书，上级根吊销权、审计义务与事件响应边界须写入合作协议。

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. 公开信任 SSL/TLS 服务器证书（支持 RSA 不低于 2048 位、ECC P-256/P-384 及国密 SM2 等主流密码算法）用于网站或服务器的身份验证、TLS 握手和通信加密；

2. 国密 SM2 SSL/TLS 服务器证书用于国密信任生态中的服务器身份验证和通信加密；

3. 国密客户端身份证书用于国密信任生态或约定系统中的客户端身份识别、登录和访问控制；

4. 国密时间戳证书用于时间戳服务系统签发时间戳响应；

5. Adobe AATL 文档签名证书用于 Adobe 产品生态中的 PDF 文档签名验证；

6. S/MIME 电子邮件加密证书用于电子邮件加密或邮件相关证书应用；

7. 单位身份类证书用于约定生态中的机构身份识别、登录或访问控制；

8. 经沃通确认符合本 CP、CPS3、适用信任计划和服务协议要求的其他全球信任或生态信任场景。

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. 超出证书类型、证书用途、证书策略、CPS3、信任计划或服务协议约定范围的用途（包括但不限于代码签名用途）；

4. 免费电子邮件加密证书用于主张申请人真实身份已经被验证；

5. Adobe AATL 文档签名证书用于主张中国《中华人民共和国电子签名法》项下第三方电子认证服务效力；

6. 客户端身份证书、单位身份类证书或 Adobe AATL 文档签名证书用于业务签署并对外主张《中华人民共和国电子签名法》项下可靠电子签名效力；

7. SSL/TLS 服务器证书用于申请人无控制权或无授权的域名、IP 地址、服务器或服务；

8. 违反法律法规、监管要求、信任计划、公序良俗、服务协议或接入协议约定的用途；

9. 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、服务协议、产品说明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。

本 CP 项下证书如被实际业务用于对外主张《中华人民共和国电子签名法》项下可靠电子签名效力，须迁移至适用《中华人民共和国电子签名法》的电子签名认证证书管理体系，或采取技术阻断措施防止继续按 CP5 证书签发、使用或宣传。完成迁移或阻断前，不得继续以 CP5 证书作为该类业务签署的证书来源。

1.4.3 生态信任边界

公开信任 SSL/TLS 服务器证书遵循 CA/Browser Forum Baseline Requirements、WebTrust 审计和适用根计划要求。支持 RSA（不低于 2048 位）、ECC（P-256/P-384）及 SM2（256 位）等主流技术算法：其中 RSA 与 ECC 算法证书完全遵循 CA/Browser Forum Baseline Requirements；在签发国密 SM2 SSL/TLS 服务器证书时，存在以下两项与 CA/Browser Forum Baseline Requirements 的固有偏离：

1. 算法偏离：签名/密钥算法采用 SM2/SM3（国密体系），不在 CA/Browser Forum Baseline Requirements 允许算法集（RSA / ECDSA NIST 曲线 / EdDSA）内；

2. 双证书机制偏离：按国密 SSL 协议要求采用签名证书与加密证书成对签发，非 CA/Browser Forum Baseline Requirements 单证书模型。

上述偏离来源于国密算法体系与国际浏览器体系的客观差异，本 CP、CPS3 及对外披露材料如实声明该差异，不得宣称无保留符合与其技术事实不一致的信任计划要求；除上述两项固有偏离外，验证流程、字段约束、有效期及撤销服务均按 CA/Browser Forum Baseline Requirements 当期版本与适用根计划中较严格者执行。

Adobe AATL 文档签名证书的信任来源为 Adobe Approved Trust List 及 Adobe 产品生态。S/MIME 电子邮件证书的信任来源为邮件客户端、S/MIME 生态和对应基线要求。国密信任生态证书的信任来源为国密信任生态相关产品、平台或信任计划。上述生态信任均不改变本 CP 的法律适用性声明。

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、信任计划边界、用途限制、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（WoTrus CA Limited）
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 / +86-755-86008688
客服与问题报告邮箱	cps@wotrus.com / ca@wotrus.com（证书问题报告与吊销请求 7×24 小时受理）
联系地址	深圳市南山区南海大道 1057 号科技大厦二期 A 栋 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、CPS3、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、适用信任计划和审计要求。

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、发布和必要的信任计划通知或披露程序。涉及订户、依赖方、信任计划或根计划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、信任计划要求变化、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与更新发布。

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。
公开信任 SSL/TLS 服务器证书	面向浏览器、操作系统或公开信任生态的服务器身份验证和通信加密证书。
国密 SSL/TLS 服务器证书	面向支持国密算法的浏览器、应用或信任生态的服务器身份验证和通信加密证书。
文档签名证书	用于特定文档签名生态中验证文档签名主体和签名结果的证书。
电子邮件证书	用于电子邮件加密、签名或相关邮件安全应用的证书。
客户端身份证书	用于客户端身份识别、登录或访问控制的证书。
时间戳证书	用于时间戳服务系统签发时间戳响应的证书。
订户	申请并持有证书的个人、机构、域名控制人、邮箱控制人、服务器运营方、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、通信验证、签名验证、邮件验证或其他信任判断的实体。
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。
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
AATL	Adobe Approved Trust List	Adobe 批准信任列表
BR	Baseline Requirements	基线要求

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
DV	Domain Validated	域名验证型
EV	Extended Validation	扩展验证型
IV	Individual Validated	个人验证型
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
OV	Organization Validated	组织验证型
PKI	Public Key Infrastructure	公钥基础设施
SAN	Subject Alternative Name	主体备用名称
S/MIME	Secure/Multipurpose Internet Mail Extensions	安全多用途互联网邮件扩展
TLS	Transport Layer Security	传输层安全协议
TSA	Time Stamping Authority	时间戳服务机构

2. 信息发布与管理

2.1 信息库

沃通建立 7×24 小时可用的公开信息库，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、审计信息和其他依法、按信任计划或按服务协议公开的信息。

2.2 认证信息的发布

沃通发布下列信息：

1. 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；

2. CPS3《沃通全球信任电子认证业务规则》的现行版本及必要历史版本，发布地址为 https://www.wotrus.com/ca/cps.html；

3. 根证书、中级根证书和证书链公开信息，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；

4. 本 CP 项下证书的证书撤销列表和在线证书状态服务地址；

5. 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；

6. WebTrust 审计、根计划、AATL、S/MIME 或其他生态信任计划要求公开披露的信息。

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。

公开信任 SSL/TLS 服务器证书和国密信任生态证书的证书状态发布频率符合 CA/Browser Forum Baseline Requirements、360 信创 SM2 根证书计划、WebTrust 和 CPS3 中较严格者：

1. 用户证书撤销列表（CRL）：有效期不超过 10 天，至少每 7 天发布一次；吊销生效后，在适用信任计划要求的时限内更新证书撤销列表，且不得晚于 24 小时；

2. 在线证书状态服务（OCSP）：订户证书响应有效期不超过 7 天，至少每 4 天更新一次；吊销生效后及时同步更新状态服务；

3. 机构撤销列表（ARL）：根/中级根 ARL 至少每 12 个月更新一次；子 CA 被吊销时，在 24 小时内更新 ARL 和 OCSP。

其他生态证书的证书撤销列表和在线证书状态服务发布频率按照对应信任计划、CPS3 和服务协议执行；本 CP 基线为用户证书撤销列表至少每 7 天发布一次，吊销生效后在 24 小时内发布更新，在线证书状态服务响应缓存不超过 24 小时。适用信任计划或 CPS3 要求更严格的，从其规定；未在 CPS3 登记状态服务地址和发布周期的证书类型，不得新增对外签发。

2.4 信息库访问控制

本 CP、CPS3、证书链、证书撤销列表、证书状态查询信息和按信任计划要求公开的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，国家代码按照适用标准和证书主体所在地填写。SSL/TLS 服务器证书在主体备用名称扩展项中载明域名或 IP 地址；文档签名证书、客户端身份证书、单位身份类证书和时间戳证书按照证书类型载明能够识别主体、系统或服务的名称信息。

3.1.2 名称意义化要求

证书主体名称与经核验的域名、IP 地址、个人、机构、邮箱、服务器、时间戳服务系统或业务场景相对应。DV 级别 SSL/TLS 服务器证书仅证明域名或 IP 地址控制权，不证明申请人真实身份。OV、EV、IV、AATL、S/MIME 或其他验证级别证书按照对应信任计划和 CPS3 核验证书主体信息。

3.1.3 匿名或伪名

本 CP 项下证书原则上不支持匿名签发。DV 级别 SSL/TLS 服务器证书可仅体现经验证的域名或 IP 地址，不构成匿名或伪名签发。电子邮件证书如仅验证邮箱控制权，在受理流程中明确告知不验证真实身份。

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、RFC 5280、GB/T 20518-2018、GM/T 0015-2023、CA/Browser Forum Baseline Requirements、S/MIME Baseline Requirements、Adobe AATL 要求及 CPS3 的规定。

SSL/TLS 服务器证书的 CN 值来自主体备用名称扩展项，主体备用名称包含经验证的 dNSName 或 ipAddress。公开信任 SSL/TLS 服务器证书禁止填写组织单元（OU）字段（按 CA/Browser Forum Baseline Requirements 规定执行）。

3.1.5 名称唯一性

沃通在证书签发和生命周期管理中保持证书主体名称与订户、域名、邮箱、服务器、系统或生态场景之间的对应关系清晰、可回溯。对于同一订户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 商标的承认、鉴别和角色

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。沃通按照适用信任计划和 CPS3 对申请信息进行审查；发现存在争议或可能侵权的，要求订户补充证明材料、修改申请信息，并根据审查结果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 CPS3 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 SSL/TLS 服务器证书身份鉴别

SSL/TLS 服务器证书申请按照 CA/Browser Forum Baseline Requirements、适用根计划、360 信创 SM2 根证书计划和 CPS3 进行域名控制权、IP 地址控制权、机构身份和授权关系核验。

SSL/TLS 服务器证书身份鉴别至少包括下列要素：

1. 对证书中每个域名或 IP 地址的控制权验证（不向本地主机名或私有 IP 地址颁发公开信任证书）；

2. 对 CAA 记录或等效授权限制的检查，适用标准另有规定的从其规定；

3. DV 证书按域名或 IP 地址控制权验证执行；

4. IV（个人验证型）证书在域名或 IP 地址控制权验证基础上核验个人有效身份证件、地址及可靠通信方式；

5. OV 证书在域名或 IP 地址控制权验证基础上核验机构合法存在、第三方渠道核验经办人身份与授权事实；

6. EV 证书按照 EV Guidelines 及国密 SSL 标准要求核验机构合法存在、业务类别、行政管辖级别、运营存在、经办人身份与授权；EV 证书不得颁发通配符域名且不得包含 IP 地址；

7. 域名或 IP 验证随机值唯一且有效期不超过 30 天，文件目录校验不得用于通配符域

名；

8. 与证书签发记录关联保存的验证方法编号、验证时间、验证证据、授权记录和意愿确认记录；历史验证数据复用遵循适用信任计划与国密 SSL 标准中较严格者（国内标准为域名/IP 398 天、身份 825 天、DV 不复用；CA/B Forum BR 按 Ballot SC-081 阶梯收紧）。

3.2.3 国密客户端身份证书身份鉴别

国密客户端身份证书申请人为经核验的机构或经授权的系统责任主体。沃通核验机构合法存在、申请授权、证书用途、服务场景和申请意愿。

国密客户端身份证书用于身份标识、登录或访问控制时，属于生态信任口径。若被用于业务签署并对外主张《中华人民共和国电子签名法》项下可靠电子签名效力，须迁移至适用《中华人民共和国电子签名法》的电子签名认证证书管理体系，或采取技术阻断措施。完成迁移或阻断前，不继续按本 CP 签发、使用或宣传该类证书用于对外业务签署。

3.2.4 Adobe AATL 文档签名证书身份鉴别

Adobe AATL 文档签名证书申请按照 Adobe AATL 相关政策、CPS3 和服务协议进行身份鉴别。

个人文档签名证书核验个人身份真实性、申请意愿和证书用途。企业文档签名证书核验机构合法存在、授权关系、申请意愿和证书用途。沃通在受理流程中明确告知订户：该证书属于 Adobe AATL 国际信任生态文档签名证书，不属于《中华人民共和国电子签名法》项下电子签名认证证书。

3.2.5 S/MIME 电子邮件证书身份鉴别

S/MIME 电子邮件证书申请按照 CA/Browser Forum S/MIME Baseline Requirements、CPS3 和服务协议进行邮箱控制权、个人身份或机构身份核验。

仅验证邮箱控制权的电子邮件证书，明确告知订户和依赖方：该证书仅证明申请人控制相应邮箱地址，不证明申请人真实身份，不适用《中华人民共和国电子签名法》。如证书类型要求个人或机构身份核验，按照对应验证级别执行。

3.2.6 单位身份类证书身份鉴别

单位身份类证书申请人为经核验的机构或经授权主体。沃通核验机构合法存在、申请授权、证书用途和申请意愿。单位身份类证书用于身份标识、登录或访问控制时，属于生态信任口径；若用于业务签署并对外主张《中华人民共和国电子签名法》项下可靠电子签名效力，须迁移至

适用《中华人民共和国电子签名法》的电子签名认证证书管理体系，或采取技术阻断措施。完成迁移或阻断前，不继续按本 CP 签发、使用或宣传该类证书用于对外业务签署。

3.2.7 时间戳证书身份鉴别

时间戳证书申请人为时间戳服务运营方或经授权主体。沃通核验机构合法存在、时间戳服务系统归属、授权关系、证书用途和申请意愿。时间戳证书本身不独立主张电子签名认证证书效力，其证明力结合所支撑的数据、签名行为、时间戳响应和证据链判断。

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. 证书用途、生态信任来源、适用信任计划和使用限制；

3. SSL/TLS 服务器证书不得用于未经验证或未经授权的域名、IP 地址、服务器或服务；

4. AATL 文档签名证书的信任来源为 Adobe 产品生态；

5. 免费或邮箱控制权型电子邮件证书不证明真实身份；

6. 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。意愿确认结合勾选确认、服务协议签署、电子签名确认、系统审批、接口调用确认、邮件验证、短信验证码、音视频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 互操作准则

本 CP 项下证书参与浏览器、操作系统、Adobe 产品、邮件客户端、国密信任生态相关系统、业务系统或跨平台验证时，遵循下列准则：

1. 沃通负责按照本 CP、CPS3 和适用信任计划签发、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、证书状态和适用生态环境；

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 CPS3 和适用信任计划要求重新证明私钥拥有权，并根据证书类型完成必要的域名验证、邮箱控制权验证、身份确认、授权确认、用途确认和意愿确认。

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 CPS3 和适用信任计划对请求人身份、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、域名控制权丧失、邮箱控制权丧失、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域名持有人、网站运营者、服务器运营方、机构、个人、邮箱控制人、文档签名主体、时间戳服务运营方、单位身份主体或经授权代表。申请实体按照证书类型提交申请信息、身份证明、机构证明、域名控制权证明、邮箱控制权证明、授权材料、用途说明以及 CPS3 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、生态信任来源、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 执行识别与鉴别功能

沃通或注册机构按照第 3 章、CPS3 和适用信任计划对申请实体身份、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 SSL/TLS 服务器证书，特别核验域名或 IP 地

址控制权、CAA 记录和组织验证级别；对 AATL、S/MIME、时间戳和单位身份类证书，特别核验对应生态信任要求。

4.2.2 证书申请批准

符合下列条件的，沃通批准证书申请：

1. 申请材料齐备并符合对应证书类型要求；

2. 身份鉴别、域名控制权验证、邮箱控制权验证、授权关系确认、用途确认和意愿确认通过；

3. 证书主体名称、证书用途、证书策略和有效期符合本 CP、CPS3、适用信任计划和适用标准；

4. 未发现虚假申请、冒用身份、越权申请、违规用途、域名控制权异常或其他不适宜签发情形；

5. 申请人已确认非电子签名法律适用性、生态信任边界、用途限制和相关责任。

4.2.3 证书申请拒绝

存在下列情形之一的，沃通拒绝或暂停证书申请：

1. 申请材料不真实、不完整或无法核验；

2. 申请人身份、机构主体、授权关系、域名控制权、邮箱控制权或证书用途无法确认；

3. 申请用途超出本 CP 或适用信任计划允许范围；

4. 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；

5. 证书主体名称可能误导依赖方或侵犯第三方合法权益；

6. 存在安全风险、合规风险、争议风险或信任计划要求禁止签发的情形。

4.2.4 处理时间

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。处理时间符合 CPS3、服务协议和适用信任计划要求。因补充材料、授权复核、安全风险排查、合规审查、信任计划要求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、CPS3、适用信任计划和适用标准。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。

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、CPS3、证书用途、证书扩展项、适用信任计划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、撤销状态和适用生态环境。依赖方不得在本 CP 允许范围之外信赖证书，不得将本 CP 项下证书用于《中华人民共和国电子签名法》电子签名认证证书场景。

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，订户按照 CPS3 和适用信任计划提交证书更新申请。SSL/TLS 服务器证书更新按照适用信任计划重新执行或确认域名控制权、IP 地址控制权、机构验证和授权验证。

4.6.2 请求证书更新的实体

证书更新请求由订户、经授权代表、域名控制人、邮箱控制人、系统运营方或 CPS3 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、域名复核、邮箱控制权复核、授权复核和意愿确认。证书更新后的有效期不得超过本 CP、CPS3 和适用信任计划规定的最长有效期。

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 CPS3、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

证书密钥更新请求由订户、经授权代表、域名控制人、邮箱控制人、系统运营方或 CPS3 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 CPS3 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 CPS3、服务协议和适用信任计划执行。

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 CPS3、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、域名、IP 地址、邮箱地址、服务器信息、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

证书变更请求由订户、经授权代表、域名控制人、邮箱控制人、系统运营方或 CPS3 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 CPS3、适用信任计划和服务协议根据变更性质、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 CPS3、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. 域名控制权、IP 地址控制权、邮箱控制权、机构授权或系统授权终止或无法确认；

5. 证书被用于超出本 CP 或适用信任计划允许范围的用途；

6. 证书违反 CA/Browser Forum、S/MIME、AATL、WebTrust、360 信创 SM2 根证书计划或其他适用信任计划要求；

7. 沃通发现证书签发、使用或管理存在安全风险、合规风险或信任计划要求撤销的情形；

8. 法律法规、监管要求、法院或仲裁机构生效文书、服务协议或 CPS3 规定的其他撤销情形。

证书自然到期按自动失效处理，不因到期列入 CRL；仅在存在上述撤销事由时按撤销流程发布撤销状态。

4.9.2 请求证书吊销的实体

证书吊销请求由订户、经授权代表、域名控制人、邮箱控制人、依赖方、监管机构、信任计划运营方、司法机关、仲裁机构或 CPS3 认可的其他主体提出。沃通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 7×24 小时渠道或 CPS3 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、证书误签、证书滥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。对适用信任计划及国密 SSL 标准明确规定撤销时限的，从其规定（订户证书高优先级事由 24 小时内撤销、普通事由 5 日内撤销；中级 CA 证书 7 天内撤销；收到证书问题报告后 24 小时内初步调查并决定是否撤销）；对私钥泄露、密钥失控、证书误签、证书滥用或其他重大安全风险情形，按照紧急流程处理，并

在适用信任计划要求的时限内更新证书状态。

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。依赖方同时确认其应用环境支持证书算法、证书链和对应生态信任计划。

4.9.6 证书撤销列表发布频率

公开信任 SSL/TLS 服务器证书和国密信任生态证书的证书撤销列表发布频率符合适用信任计划要求。用户证书撤销列表有效期不超过 10 天、至少每 7 天发布一次；吊销生效后，在适用信任计划要求的时限内更新证书撤销列表，且不得晚于 24 小时；子 CA 吊销时 ARL 与 OCSP 在 24 小时内更新。其他生态证书的用户证书撤销列表至少每 7 天发布一次；吊销生效后，在 24 小时内发布更新。适用信任计划或 CPS3 要求更短周期或更短滞后时间的，从其规定。

4.9.7 证书挂起和恢复

公开信任 SSL/TLS 服务器证书不提供证书挂起服务，适用信任计划另有明确规则的按其规则执行。其他证书类型在 CPS3 明确登记挂起与恢复服务范围时，沃通按照 CPS3、服务协议和适用信任计划提供挂起和恢复服务；未完成登记的证书类型不提供挂起服务。

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 CPS3 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；适用信任计划、CPS3 或服务协议规定更短期限的，从其规定。恢复证书前，沃通重新核验证书用途、主体身份、授权关系、私钥控制状态、信任计划适用性和挂起原因消除情况。挂起期限届满仍不能满足恢复条件的，撤销证书或按照 CPS3 启动重新申请流程。

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 7×24 小时证书状态查询服务，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。

国家根下 SM2 SSL/TLS 服务器证书在线证书状态服务地址为 http://ocsp2.wotrus.com/；其他生态证书在线证书状态服务地址按照证书扩展项、CPS3 或公开发布信息执行。未在证书扩展项、CPS3 或公开发布信息中载明状态服务地址的证书类型，不得新增对外签发。

公开信任 SSL/TLS 服务器证书及国密信任生态证书的 OCSP 响应有效期不超过 7 天、至少每 4 天更新一次；其他生态证书 OCSP 响应缓存不超过 24 小时，适用信任计划或 CPS3 要求更严格的从其规定。CRL 和 OCSP 响应时间不超过 10 秒，撤销记录在被撤销证书过期后方可删除；根 CA 禁止直接签发订户证书。服务可用率目标、备用查询机制和异常期间处理规则由 CPS3 和适用信任计划规定。

4.11 订购结束

证书到期、撤销、订户终止服务、服务协议终止、域名控制权终止、邮箱控制权终止、AATL 或 S/MIME 资格终止、服务器下线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 CPS3 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。公开信任 SSL/TLS 服务器证书、文档签名证书、邮件证书和客户端身份证书的私钥保护、生成和恢复限制符合对应信任计划、CPS3 和服务协议要求。

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、信任计划、密码管理要求、服务协议、CPS3 和安全策略委员会批准规则的前提下实施。

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全球信任体系证书服务场所，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。CPS3 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、信任计划适用性核验、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；涉及公开信任、AATL、S/MIME、国密信任生态或其他生态信任计划的业务，按照 CPS3 和适用信任计

划留存验证依据、批准记录和披露记录。

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。关键岗位人员具备全球信任体系证书服务运行、密码安全管理、主体核验、域名验证、邮箱控制权验证、信任计划规则执行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、域名验证、邮箱控制权验证、信任计划适用性确认、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、域名验证记录、邮箱控制权验证记录、信任计划适用性确认记录、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。记录保存期限不低于适用信任计划要求；适用信任计划或服务协议未规定更长期限的，参照电子认证服务记录保存至证书失效后 5 年。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、CPS3 和适用信任计划执行；涉及证书链、信任计划适用性或依赖方验证方式变化的，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、信任计划适用性核验、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 CPS3 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；涉及 360 信创 SM2 根证书计划的严重事件在 24 小时内通知 360 及其战略合作伙伴、48 小时内提供完整事件报告，涉及 CA/Browser Forum 及相关根计划的按规定时限公开事件报告。

5.8 电子认证服务机构或注册机构的终止

沃通终止本 CP 项下全球信任体系证书服务时，按照法律法规、监管要求和 CPS3 处理订户通知、信任计划相关通知、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；适用信任计划规定更严格期限或更细披露要求的，按更严格要求执行。

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和适用信任计划要求的受控密码设备（取得商用密码产品认证或符合 FIPS 140-2/3 Level 3 等效安全等级）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。因业务系统部署、设备初始化或服务器证书安装需要进行密钥导入、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。适用信任计划禁止 CA 生成或传送订户私钥的（如公开信任 SSL/TLS 服务器证书及 360 信创 SM2 根证书计划），沃通严格执行该信任计划限制。

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 CPS3 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、CPS3、适用信任计划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、根计划公开信息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、适用信任计划和 CPS3 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（如 RSA 小于 2048 位、弱密钥或已知泄露密钥）不予签发。

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和适用信任计划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。订户私钥不由沃通托管或归档，适用信任计划或服务协议另有明确允许且经安全策略委员会批准的除外。

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 CPS3 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、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 CPS3 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、适用信任计划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。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、信任计划适用性和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、信任计划相关服务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 CPS3、适用信任计划和服务协议规定。

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
SM2 SSL/TLS 服务器证书	国家电子认证根 ROOTCA → WoTrus SM2 CA（含同名交叉根） → WoTrus SM2 SSL CA → 订户证书	http://ldap.wotrus.com/crl/wotrus_sm2_ssl_ca.crl	http://ocsp2.wotrus.com/
国密 SM2 SSL/TLS 服务器证书	国密 SM2 根证书 → 对应国密 SM2 服务	以证书 CRL Distribution Points 扩	以证书 AIA 扩展项及 CPS3 公布信息为准

	器中级根（V1/V3/V4） → 订户证书	展项及 CPS3 公布信息为准	
国密客户端身份证书	国密 SM2 根证书 → 国密 SM2 客户端根证书 → 订户证书	以证书 CRL Distribution Points 扩展项及 CPS3 公布信息为准	以证书 AIA 扩展项及 CPS3 公布信息为准
国密时间戳证书	国密 SM2 根证书 → 国密 SM2 时间戳根证书 → 订户证书	以证书 CRL Distribution Points 扩展项及 CPS3 公布信息为准	以证书 AIA 扩展项及 CPS3 公布信息为准
Adobe AATL 文档签名证书	CA WoTrus Root → WoTrus Document Signing CA → 订户证书	以证书 CRL Distribution Points 扩展项及 CPS3 公布信息为准	以证书 AIA 扩展项及 CPS3 公布信息为准
S/MIME 电子邮件证书	CA WoTrus Root → WoTrus V1 Client CA → 订户证书	以证书 CRL Distribution Points 扩展项及 CPS3 公布信息为准	以证书 AIA 扩展项及 CPS3 公布信息为准
单位身份类证书	CA WoTrus Root → WoTrus V3 Client CA → 订户证书	以证书 CRL Distribution Points 扩展项及 CPS3 公布信息为准	以证书 AIA 扩展项及 CPS3 公布信息为准

未在证书扩展项、CPS3 或公开发布信息中登记证书状态服务地址、撤销列表地址或 CA 证书访问地址的证书类型，不得新增对外签发。处于信任计划承诺范围内的合作定制中级根/外部子 CA，经核实后在 CPS3 及公开证书链清单中逐根列明。

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
公开信任 SSL/TLS 服务器证书（RSA/ECC/SM2）	1.2.156.150570.6.5，并按验证级别配置适用信任计划对象标识符	CPS3	服务器身份验证、TLS 握手和通信加密（支持 RSA≥2048、ECC P-256/P-384、SM2）。
国密 SM2 SSL/TLS	1.2.156.150570.6.5，并按	CPS3	国密信任生态下的服务器身份验证

服务器证书	验证级别配置适用信任计划对象标识符		和通信加密。
国密客户端身份证书	1.2.156.150570.6.5	CPS3	客户端身份识别、登录和访问控制；不适用《中华人民共和国电子签名法》及其规定的可靠电子签名法律效力。
国密时间戳证书	1.2.156.150570.6.5	CPS3	时间戳服务系统签发时间戳响应；不独立作为电子签名认证证书。
Adobe AATL 个人文档签名证书	1.2.156.150570.6.5，并按 Adobe AATL 要求配置验证级别信息	CPS3	Adobe 产品生态中的个人文档签名；不适用《中华人民共和国电子签名法》及其规定的可靠电子签名法律效力。
Adobe AATL 企业文档签名证书	1.2.156.150570.6.5，并按 Adobe AATL 要求配置验证级别信息	CPS3	Adobe 产品生态中的企业文档签名；不适用《中华人民共和国电子签名法》及其规定的可靠电子签名法律效力。
S/MIME 电子邮件证书	1.2.156.150570.6.5，并按 S/MIME 要求配置适用对象标识符	CPS3	电子邮件加密、邮件安全应用或对应邮件生态用途。
单位身份类证书	1.2.156.150570.6.5	CPS3	单位身份识别、登录或访问控制；不适用《中华人民共和国电子签名法》及其规定的可靠电子签名法律效力。

本 CP 项下证书适用信任计划、验证级别对象标识符和取严规则如下：

证书类别	适用信任计划或生态规则	已确认验证级别对象标识符	取严规则
公开信任 SSL/TLS 服务器证书、国密 SM2 SSL/TLS 服务器证书	CA/Browser Forum Baseline Requirements、EV Guidelines、WebTrust、适用根计划和国密信任生态规则	DV 2.23.140.1.2.1、OV 2.23.140.1.2.2、EV 2.23.140.1.1	以当期有效信任计划要求、CPS3 和本 CP 中较严格者为准。
国密客户端身份证书	国密信任生态规则、适用浏览器或生态信任计划、CPS3	无适用 CA/Browser Forum L1 验证级别对象标识符；配置 CP5 OID 1.2.156.150570.6.5 和	不得因缺少 L1 验证级别对象标识符而扩大用途；以 CPS3 登记用途和本 CP 限制为准。

		CPS URI	
国密时间戳证书	国密信任生态规则、时间戳服务规则、CPS3	无适用 CA/Browser Forum L1 验证级别对象标识符；配置 CP5 OID 1.2.156.150570.6.5 和 CPS URI	不独立主张电子签名认证证书效力；以 CPS3 和时间戳服务规则中较严格者为准。
Adobe AATL 个人文档签名证书	Adobe AATL 政策、WebTrust、CPS3	Adobe 受信 OID 1.3.6.1.4.1.50570.2.9、1.3.6.1.4.1.36305.1.3.1；个人验证型按照适用规则配置 IV 2.23.140.1.2.3；同时配置 CP5 OID 和 CPS URI	以当期有效 Adobe AATL 要求与 CPS3 中较严格者为准。
Adobe AATL 企业文档签名证书	Adobe AATL 政策、WebTrust、CPS3	Adobe 受信 OID 1.3.6.1.4.1.50570.2.9、1.3.6.1.4.1.36305.1.3.1；同时配置 CP5 OID 和 CPS URI	以当期有效 Adobe AATL 要求与 CPS3 中较严格者为准。
S/MIME 电子邮件证书	CA/Browser Forum S/MIME Baseline Requirements、WebTrust、CPS3	按 S/MIME Baseline Requirements 对应 Mailbox-validated、Organization-validated 或其他实际验证级别配置；同时配置 CP5 OID 和 CPS URI	未在 CPS3 登记具体 S/MIME 验证级别和对象标识符的证书类型，不得新增对外签发。
单位身份类证书	WebTrust、适用生态信任计划、CPS3	配置 CP5 OID 1.2.156.150570.6.5 和 CPS URI；适用生态规则另有验证级别对象标识符的，按 CPS3 登记配置	用于身份识别、登录或访问控制；不适用《中华人民共和国电子签名法》及其规定的可靠电子签名法律效力。

注：《公共可信证书管理 SSL 服务器证书运营和管理要求》（国密行业标准草案）预留了向国家密码管理局申请保留的国密 SSL 策略 OID（DV 1.2.156.10197.6.6.1.1、IV 1.2.156.10197.6.6.1.2、OV 1.2.156.10197.6.6.1.3、EV 1.2.156.10197.6.6.1.4）；待该行业标准正

式发布实施并完成申请保留后，按标准要求增配或切换，现网签发以已登记的验证级别 OID 与 CP5 OID 为准。

证书实际包含的策略对象标识符以证书扩展项为准。任何外部信任计划对象标识符未在 CPS3、签发系统配置和发布资料中完成一致登记前，不得进入新增对外签发。

7.1.4 证书主体名称

SSL/TLS 服务器证书主体名称与经验证的域名或 IP 地址、机构身份及验证级别一致。文档签名证书主体名称与经验证的个人或机构身份一致。电子邮件证书主体名称与经验证的邮箱地址、个人身份或机构身份一致。时间戳证书主体名称与经验证的时间戳服务运营方或系统名称一致。

7.1.5 算法对象标识符

本 CP 项下支持主流密码算法体系：（1）RSA 算法（密钥长度不低于 2048 位，采用 SHA-256 及以上签名算法）；（2）ECC 算法（NIST P-256 / P-384 曲线，采用 ECDSA-SHA256/SHA384）；（3）国密 SM2 算法（256 位，采用符合 GM/T 0003、GM/T 0015、GM/T 0034 及《公共可信证书管理 SSL 服务器证书运营和管理要求》的 SM2/SM3 算法对象标识符）。具体算法对象标识符以证书实际编码、CPS3、适用信任计划和适用标准为准。

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
SSL/TLS 服务器签名证书	数字签名；国密双证书机制按照协议要求设置	服务器身份验证 1.3.6.1.5.5.7.3.1，按用途包含客户端身份验证 1.3.6.1.5.5.7.3.2
SSL/TLS 服务器加密证书	密钥加密、数据加密、密钥协商，按算法和协议要求确定	服务器身份验证 1.3.6.1.5.5.7.3.1，按用途包含客户端身份验证 1.3.6.1.5.5.7.3.2
客户端身份证书	数字签名、密钥加密，按证书用途和信任计划要求确定	客户端身份验证 1.3.6.1.5.5.7.3.2
时间戳证书	数字签名	时间戳 1.3.6.1.5.5.7.3.8
文档签名证书	数字签名，Adobe AATL 技术要求另有规定的从其规定	文档签名用途按 Adobe AATL 和 CPS3 执行
电子邮件证书	数字签名、密钥加密或数据加密，按 S/MIME 要求确定	电子邮件保护 1.3.6.1.5.5.7.3.4 或对应 S/MIME 用途
单位身份类证书	数字签名、密钥加密，按证书用	客户端身份验证或其他经批准用途

	途和信任计划要求确定	

本 CP 项下证书的密钥用法不得使依赖方误认为证书属于《中华人民共和国电子签名法》项下电子签名认证证书。Adobe AATL 文档签名证书如因 Adobe 产品生态技术要求需要保留特定密钥用法（如认可签名位 Non-Repudiation），须明确其保留原因、信任边界和不适用电子签名认证证书口径的专项告知。

国密客户端身份证书、单位身份类证书、Adobe AATL 文档签名证书如被业务系统用于对外签署并主张可靠电子签名效力，须迁移至适用《中华人民共和国电子签名法》的电子签名认证证书管理体系，或采取技术阻断措施。完成迁移或阻断前，不继续按本 CP 签发、使用或宣传该类证书用于对外业务签署。

7.1.7 标准扩展项和自定义扩展项

本 CP 项下证书序列号由密码安全伪随机数生成器生成至少 64 位非连续正整数，禁止包含 issuerUniqueID 与 subjectUniqueID，并可包含下列扩展项（支持 RFC 6962 证书透明度 SCT 扩展，如适用）：

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、信任计划和 CPS3 的其他扩展项。

扩展项的关键性符合 X.509、RFC 5280、GB/T 20518-2018、GM/T 0015-2023、CPS3、适用信任计划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
公开信任 SSL/TLS 服务器证书（RSA / ECC）	200 天或适用信任计划当期更严格上限	按 CA/Browser Forum Ballot SC-081：自 2026 年 3 月 15 日起最长 200 天，2027 年 3 月 15 日起 100 天，2029 年 3 月 15 日起 47 天；以 CPS3、BR 和适用根计划中较严格者为准。
国密 SM2 SSL/TLS 服务器证书	最长支持 2 年 + 宽限期（不超过 825 天）；适用特定根计划时从其更严格上限	国密 SM2 SSL 最大可支持 2 年 + 宽限期（不超过 825 天）的有效期策略；如纳入 360 信创 SM2 根证书计划（不超过 398 天）、《公共可信证书管理 SSL 服务器证书运营和管理要求》（草案，不宜超过 397 天/不得超过 398 天）或其他特定信任计划的，按对应计划当期更严格上限执行。
国密客户端身份证书	825 天或适用信任计划当期更严格上限	仅限客户端身份识别、登录和访问控制；以当期有效信任计划要求与 CPS3 中较严格者为准。
国密时间戳证书	1827 天或适用信任计划当期更严格上限	仅用于时间戳服务系统签发时间戳响应；以当期有效信任计划要求与 CPS3 中较严格者为准。
Adobe AATL 文档签名证书	825 天或 Adobe AATL 当期更严格上限	以当期有效 Adobe AATL 要求与 CPS3 中较严格者为准。
S/MIME 电子邮件证书	825 天或 S/MIME Baseline Requirements 当期更严格上限	以当期有效 S/MIME Baseline Requirements（Strict/Multipurpose 上限 825 天）与 CPS3 中较严格者为准。
单位身份类证书	825 天或适用信任计划当期更严格上限	仅限单位身份识别、登录或访问控制；以当期有效信任计划要求与 CPS3 中较严格者为准。

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、CPS3、服务协议或适用信任计划规定的限制。

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、RFC 5280、GB/T 20518-2018、GM/T 0015-2023、CPS3 和适用信任计划处理。

SM2 SSL/TLS 服务器证书撤销列表地址为 http://ldap.wotrus.com/crl/wotrus_sm2_ssl_ca.crl。国密 SM2 根证书相关撤销列表地址包括 http://crl.wotrus.com/wotrus-sm2.crl。其他中级根和用户证书撤销列表地址以证书 CRL Distribution Points 扩展项、CPS3 和公开发布信息为准；未完成登记和公开的，不得新增对外签发。

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、CPS3 和服务运行规则处理。SM2 SSL/TLS 服务器证书在线状态服务地址为 http://ocsp2.wotrus.com/；其他证书在线状态服务地址以证书 AIA 扩展项、CPS3 和公开发布信息为准。未完成登记和公开的，不得新增对外签发。

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、适用信任计划、CPS3 和认证业务运行管理要求对本 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；年度外部合规审计或检测周期不超过 1 年，审计周期结束后 3 个月内公开审计报告（含根及中级根 SM3 指纹）；WebTrust、CA/Browser Forum、AATL、S/MIME、360 信创

SM2 根证书计划或其他生态信任计划要求更高频率或专项审计的，从其规定。

8.2 审计者身份和资质

审计者具备与电子认证服务、WebTrust、公开信任证书、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、信任计划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、CPS3、证书申请受理、身份鉴别、域名验证、邮箱控制权验证、授权确认、告知确认、证书签发、证书撤销、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、信任计划披露和信息发布等。

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、信任计划要求或依赖方利益的重要事项，按照 CPS3、法律法规、监管要求和适用信任计划进行报告或公告。

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、域名验证记录、邮箱控制权验证记录、AATL 证书记录、S/MIME 证书记录、国密客户端身份证书记录、时间戳证书记录和单位身份类证书记录。至少每季度开展一次内部自我审核，随机抽样率不得低于当期同类业务记录的 3%，且每类证书不少于 5 件；当期记录不足 5 件的，全量抽查。适用信任计划、WebTrust 审计或外部评估要求更高抽样比例的，从其规定。

整改关闭以验证材料、授权材料、证书扩展项核验、状态服务记录、系统配置复核、日志记录、重新签发或撤销记录、阻断措施证明、迁移记录或复核结论等证据为基础。涉及证书被用于对外主张可靠电子签名效力的，重点核查迁移至适用《中华人民共和国电子签名法》的电子签名认证证书管理体系或技术阻断措施是否完成；未完成整改闭环的，不得作为已关闭事项处理。

9. 其他业务和法律事项

9.1 费用

本 CP 项下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。免费电子邮件证书、测试类或生态计划特殊证书按照服务条款免费提供或按照专项协议约定收费。

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、信任计划、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、信任计划要求、服务协议和 CPS3 建立与其证书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、CPS3、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、域名验证信息、邮箱验证信息和安全信息承担保密义务，法律法规、信任计划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、CPS3、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、CPS3、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、CPS3、适用法律法规、适用信任计划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、信任计划、本 CP、CPS3 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、证书被用于电子签名认证证书场景或第三方违规使用证书所造成的损失承担责任。

本 CP 项下全部证书（含 Adobe AATL 文档签名证书、客户端身份证书、单位身份类证书等）均不属于《中华人民共和国电子签名法》规定的电子签名认证证书，不适用《中华人民共和国电子签名法》及其规定的可靠电子签名法律效力。任何主体将本 CP 项下证书用于电子签名认证证书场景或其他超出本 CP 限定用途的，相关风险和责任由责任方依法承担。

国密客户端身份证书、单位身份类证书、Adobe AATL 文档签名证书被用于对外主张《中华人民共和国电子签名法》项下可靠电子签名效力，须迁移至适用《中华人民共和国电子签名法》的电子签名认证证书管理体系，或采取技术阻断措施。完成迁移或阻断前，不继续按本 CP 签发、使用或宣传该类证书用于对外业务签署；违反本限制导致依赖方误信或业务损失的，由责任方依法承担相应责任。

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、信任计划、CPS3、服务协议或项目合同执行；对与根 CA 签订根证书分发协议的应用软件供应商，依法承担相应抗辩与免责保障（应用软件自身错误显示证书有效性除外）。法律法规规定不得限制的责任，不因本 CP、CPS3 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、CPS3、信任计划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、CPS3、服务协议、接入协议、信任计划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、信任计划适用性、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，并按照赔偿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、CPS3、服务协议、信任计划或项目合同执行；法律法规规定不得排除或限制的责任，不因服务协议、信任计划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、信任计划要求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、信任计划要求、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、信任计划或监管要求履行通知、披露或备案义务。

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，相关方按照 CPS3、服务协议、接入协议、信任计划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 5 个工作日内确认受理或告知补正。争议处理方式包括协商、调解、投诉处理、信任计划处理、监管机关处理、仲裁或诉讼。

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、信任计划处理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、信任计划处理、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；信任计划、订户协议、依赖方协议或跨境生态信任安排另有约定且不违反强制性法律规定的，从其约定。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、信任计划要求和合同义务。

9.16 一般条款

本 CP 与 CPS3 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；CPS3 承担实施细则，不得改变本 CP 的策略结论。

如 CPS3、服务协议、业务规则、信任计划披露材料或其他文件与本 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 CPS3 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 CPS3、服务协议、接入协议、适用法律法规、监管要求、信任计划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。