沃通电子认证服务有限公司

沃通电子政务电子认证

证书策略

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《沃通电子政务电子认证证书策略》正文，明确 CP2 策略边界、证书类型、对象标识符、适用 CPS、电子政务用途、证书状态服务、生命周期管理、合规备案与报告、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法律法规、规章和标准规范：

- 《中华人民共和国电子签名法》
- 《中华人民共和国密码法》
- 《商用密码管理条例》（2023 修订）
- 《电子政务电子认证服务管理办法》（国家密码管理局令第 4 号）
- 《电子认证服务使用密码管理办法》（国家密码管理局令第 6 号）
- 国密局字〔2018〕572 号《电子政务电子认证服务业务规则规范》
- 国密局字〔2018〕571 号《电子政务电子认证服务质量评估要求》
- 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》
- 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

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 - 9 -
1.6 定义和缩写 - 10 -
2. 信息发布与管理 - 11 -
2.1 信息库 - 11 -
2.2 认证信息的发布 - 12 -
2.3 发布时间或频率 - 12 -
2.4 信息库访问控制 - 12 -
3. 标识与鉴别 - 12 -
3.1 命名 - 12 -
3.2 初始身份确认 - 14 -
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 - 17 -
4. 证书生命周期操作要求 - 17 -
4.1 证书申请 - 17 -
4.2 证书申请处理 - 17 -
4.3 证书签发 - 18 -
4.4 证书接受 - 19 -
4.5 密钥对和证书的使用 - 19 -
4.6 证书更新 - 19 -
4.7 证书密钥更新 - 20 -
4.8 证书变更 - 20 -
4.9 证书吊销和挂起 - 21 -
4.10 证书状态服务 - 23 -
4.11 订购结束 - 23 -
4.12 密钥托管和恢复 - 23 -
5. 设施、管理和操作控制 - 23 -
5.1 物理控制 - 23 -
5.2 程序控制 - 24 -
5.3 人员控制 - 24 -
5.4 审计日志程序 - 24 -
5.5 记录归档 - 24 -
5.6 密钥变更 - 25 -
5.7 损害与灾难恢复 - 25 -
5.8 电子认证服务机构或注册机构的终止 - 25 -
6. 技术安全控制 - 25 -

6.1 密钥对的生成和安装 - 25 -
6.2 私钥保护和密码模块工程控制 - 26 -
6.3 密钥对管理的其他方面 - 27 -
6.4 激活数据 - 27 -
6.5 计算机安全控制 - 28 -
6.6 生命周期技术控制 - 28 -
6.7 网络安全控制 - 28 -
6.8 时间戳 - 28 -
7. 证书、证书撤销列表和在线证书状态协议 - 28 -
7.1 证书 - 28 -
7.2 证书撤销列表 - 31 -
7.3 在线证书状态协议 - 31 -
8. 合规审计和其他评估 - 32 -
8.1 审计和评估频率 - 32 -
8.2 审计者身份和资质 - 32 -
8.3 审计者与被审计者关系 - 32 -
8.4 审计覆盖主题 - 32 -
8.5 结果沟通 - 32 -
8.6 抽样、整改和证据留存 - 32 -
9. 其他业务和法律事项 - 33 -
9.1 费用 - 33 -
9.2 财务责任 - 33 -
9.3 业务信息保密 - 33 -
9.4 个人信息保护 - 33 -
9.5 知识产权 - 34 -
9.6 陈述与保证 - 34 -
9.7 担保免责 - 34 -
9.8 责任限制 - 34 -
9.9 赔偿 - 34 -
9.10 有效期限和终止 - 35 -
9.11 对参与者的个别通告与沟通 - 35 -
9.12 修订 - 35 -
9.13 争议处理 - 35 -
9.14 适用法律 - 35 -
9.15 符合适用法律 - 36 -
9.16 一般条款 - 36 -
9.17 其他条款 - 36 -

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”）依法取得《电子政务电子认证服务机构资质证书》等相关许可资质，依法提供电子政务电子认证服务。本《沃通电子政务电子认证证书策略》（以下简称“本 CP”或“CP2”）规定沃通电子政务电子认证证书的策略边界、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 适用于沃通面向电子政务活动签发的 SM2 电子政务证书，包括电子政务个人电子认证证书、电子政务机构电子认证证书、电子政务个人电子签名认证证书、电子政务机构电子签名认证证书和电子政务设备证书。上述证书用于政务活动中的身份认证、电子签名、电子签章、数据加密、设备身份识别、通信加密和政务信息系统访问控制。电子政务内网电子认证服务有关要求不在本 CP 范围内。

本 CP 项下证书适用《中华人民共和国电子签名法》和电子政务电子认证服务监管要求。电子政务电子签名在符合法律法规、证书用途、证书状态、签名人身份、私钥控制和业务规则要求的条件下，可用于电子政务活动中的身份识别、签名验证、数据完整性验证和责任认定。

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、法律适用性和责任边界；CPS2《沃通电子政务电子认证服务业务规则》确定本 CP 项下证书的申请受理、主体核验、意愿确认、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	《沃通电子政务电子认证证书策略》
文档简称	CP2
CP 文档对象标识符	1.2.156.150570.6.2
适用 CPS	CPS2《沃通电子政务电子认证服务业务规则》
CPS 文档对象标识符	1.2.156.150570.7.2
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电子政务电子认证证书策略。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；CPS 文档对象标识符仅用于标识 CPS2 文档自身，不作为独立策略项写入用户证书

certificatePolicies。

电子政务电子认证服务监管文件未强制要求由主管部门统一分配用户证书策略对象标识符。政务对接平台如指定特定策略对象标识符，在平台接入环节逐项核实并经沃通安全策略委员会批准后执行。

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。沃通开展电子政务电子认证服务时，持续符合电子政务电子认证服务资质、备案、公开发布和密码管理要求，并纳入统一的电子认证信任体系，遵守电子认证服务互信互认要求。

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、政务场景确认、订户告知、意愿确认、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 CPS2 规定。

沃通直接承担注册机构职责；如委托其他机构开展电子签名认证证书注册业务的，须符合《电子政务电子认证服务管理办法》第 25 条要求：自委托协议签订之日起 30 日内（及备案内容变更之日起 30 日内）向受委托机构住所地省、自治区、直辖市密码管理部门备案；受委托机构须在委托范围内以沃通名义开展注册业务，不得再委托其他机构或者个人；沃通对受委托机构的行为实施监督，并对其行为后果承担法律责任。

1.3.3 订户

订户（即证书持有者）是申请并持有本 CP 项下证书的个人、政务部门、依法承担行政职能的组织、政务信息系统运营方、政务设备所属机构或其他经授权主体。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、设备、安全介质、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、签名验证、电子签章验证、数据解密、设备识别、通信验证或访问控制的个人、机构、政务信息系统或其他实体。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、签名数据完整性和适用政务场景。

1.3.5 其他参与者

其他参与者包括政务服务平台、政务信息系统、电子签章系统、密钥管理基础设施（KMI）、目录服务、证书状态服务、归档系统、审计系统、国家密码管理部门以及其他经授权参与电子政务电子认证服务流程的相关方。相关方的职责和边界以 CPS2、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电子政务场景：

1. 电子政务个人电子认证证书用于政务活动中个人身份认证、电子签名和数据加密；

2. 电子政务机构电子认证证书用于政务活动中机构身份认证、电子签章和数据加密；

3. 电子政务个人电子签名认证证书用于仅需电子签名、无数据加密需求的个人政务签署场景；

4. 电子政务机构电子签名认证证书用于仅需电子签名或电子签章、无数据加密需求的机构政务签署场景；

5. 电子政务设备证书用于政务服务器、网关、签章服务设备、移动终端或其他政务设备的身份识别、通信加密和访问控制；

6. 经沃通确认符合本 CP、CPS2、电子政务电子认证服务监管要求和服务协议要求的其他电子政务场景。

本 CP 项下双证书机制包括签名证书和加密证书。签名证书用于身份认证、电子签名或电子签章；加密证书用于密钥加密、数据加密或密钥协商。加密证书不得用于电子签名。

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. 非电子政务场景、电子政务内网场景或未经确认的商业、消费、内部办公、私域网络或其他非政务应用场景；

2. 超出证书类型、证书用途、证书策略、CPS2、服务协议或接入协议约定范围的用途；

3. 将加密证书用于电子签名、电子签章或不可否认性主张；

4. 将个人证书用于代表机构签署具有机构责任的文件，但经机构授权且业务系统明确支持的除外；

5. 将设备证书用于自然人或机构签名主体身份主张；

6. 违反法律法规、监管要求、密码管理要求、公序良俗或服务协议约定的用途；

7. 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。

政务场景边界存在疑问的，由沃通进行合规评估并留痕；涉及对外业务定性、政务场景归属或监管口径不明确的，提交沃通安全策略委员会裁定。

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、电子政务用途边界、重要安全策略、备案发布事项和重大例外事项。

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
联系部门	沃通合规运营部
客服与投诉热线	4006-967-446（以官方网站“联系我们”及业务指南栏目公布信息为准）
电子邮箱	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 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、CPS2、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 的策略要求和电子政务电子认证服务监管要求。

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。

依据《电子政务电子认证服务管理办法》（国家密码管理局令第 4 号）第 16 条及国密局字〔2018〕572 号第 5.1 条，本 CP 与 CPS2 在提供电子政务电子认证服务前予以公布并向住所地省、自治区、直辖市密码管理部门备案；发生变更的，予以公布，并自公布之日起 30 日内向住所地省、自治区、直辖市密码管理部门备案，同时保持已公布文本的持续可访问性。

1.5.5 CP 修订

发生法律法规或监管要求变化、电子政务电子认证服务规则变化、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 至少每年进行一次全面评审。

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。
电子政务电子认证服务	采用商用密码技术，通过数字证书，为各级政务部门开展社会管理、公共服务等政务活动提供电子签名认证服务，保证电子签名真实性和可靠性的活动。
电子政务电子认证证书	用于电子政务活动中身份认证、电子签名、电子签章、数据加密、设备身份识别、通信加密或访问控制的电子认证证书。
电子政务电子签名认证证书	电子政务电子认证证书中仅含签名证书、用于电子政务活动中电子签名或电子签章的证书类型。
双证书机制	同一订户或同一业务场景下分别使用签名证书和加密证书的证书机制。
签名证书	用于身份认证、电子签名、电子签章或签名验证的证书。
加密证书	用于密钥加密、数据加密或密钥协商的证书。
设备证书	用于政务设备、服务器、网关、服务节点或系统组件身份识别和通信保护

	的证书。
订户	申请并持有证书的个人、机构、设备所属机构或其他授权实体（亦称证书持有者）。
依赖方	基于证书进行身份识别、签名验证、通信验证或信任判断的实体。
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。
密钥管理基础设施（KMI）	由国家密码管理局和省部密码管理部门规划建设、为电子政务电子认证服务提供加密密钥管理服务的基础设施。

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
KMI	Key Management Infrastructure	密钥管理基础设施
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
RA	Registration Authority	注册机构
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、资质信息、投诉渠道和其他依法或按监管要求公开的信息。

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. CPS2《沃通电子政务电子认证服务业务规则》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. 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；

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、电子政务电子认证服务协议、依赖方协议、投诉处理政策、投诉渠道和争议处理方式；

6. 《电子政务电子认证服务机构资质证书》的机构名称、证书编号、有效期限、发证机关和发证日期，以及依法或按监管要求公开的备案、审计或合规信息。

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，沃通及时发布修订后的版本并按规定备案，同时保留必要的历史版本持续可访问能力。

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、CPS2、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个人、机构、设备、政务系统或服务节点的主体名称信息。

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、系统或政务场景相对应。个人证书主体名称体现经核验的个人身份；机构证书主体名称体现经核验的机构身份；设备证书主体名称体现设备、服务节点或系统组件及其所属机构。

3.1.3 匿名或伪名

本 CP 项下证书不支持匿名或伪名签发。确需使用设备标识、系统标识或服务节点标识的，按照 CPS2 和服务协议进行管理，并确保可回溯至经授权的机构或责任主体。

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 CPS2 的规定。

个人证书主体名称至少包含 CN、C 等必要字段。涉及身份证件信息、联系方式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、CPS2 和服务协议处理。

机构证书和设备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、设备标识、系统名称、服务节点或其他主体识别信息的，按照适用标准、申请材料和 CPS2 处理。

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、设备、系统或政务场景之间的对应关系清晰、可回溯。对于同一订户或同一机构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。沃通按照本 CP 和 CPS2 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、通过密钥管理系统生成密钥、在设备或服务器端生成密钥，或 CPS2 认可的其他方式。

沃通不得接收、保存或要求订户提交明文签名私钥。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 电子政务个人订户身份鉴别

电子政务个人订户申请证书时，沃通核验申请人的身份真实性、政务场景关联关系、申请意愿和证书用途。

个人订户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. 身份证件核验、在线实名核验、实人查验或 CPS2 认可的其他核验方式；

3. 申请人与政务部门、政务信息系统或政务业务场景的关联证明；

4. 申请人对证书及电子签名使用条件、法律责任、信息保存与使用权限及责任范围等事项的知晓与主动确认，并签订电子政务电子认证服务协议；

5. 与证书签发记录关联保存的身份核验记录、政务场景记录、申请记录、服务协议和意愿确认记录。

个人订户用于政务人员身份、政务业务经办、政务系统登录或政务业务签署的，提供其与相应政务部门、事业单位、依法承担行政职能组织或政务信息系统的任职、授权、服务关系或业务办理关系证明。仅以普通商业、内部办公、一般个人身份识别或非政务业务需求申请证书的，不得纳入本 CP 项下电子政务电子认证服务口径。

3.2.3 电子政务机构订户身份鉴别

电子政务机构订户申请证书时，沃通核验机构主体身份、政务属性或政务场景、经办人身份、授权关系、申请意愿和证书用途。

机构订户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. 政务部门、事业单位、依法承担行政职能组织、政务信息系统运营方或政务服务承办方的身份或场景证明；

3. 法定代表人、负责人或授权经办人身份信息；

4. 经办人授权文件、机构授权记录或其他可验证授权材料；

5. 机构对证书及电子签名使用条件、法律责任、信息保存与使用权限及责任范围等事项的主动确认，并签订电子政务电子认证服务协议；

6. 与证书签发记录关联保存的主体核验、授权记录、政务场景记录、申请记录、服务协议和意愿确认记录。

机构订户的电子政务属性按下列层级识别：各级政务部门、机构编制部门登记的党政机关和事业单位（统一社会信用代码首位为“1”者）按主体维度直接识别；依法承担行政职能的组织提供法定授权、主管部门授权或政务职能证明；受政务部门委托建设、运营或接入政务信息系统的机构，提供政务部门委托、项目合同、系统接入证明、平台开通证明或其他能够证明政务场景的材料。不能证明政务主体身份或政务场景的，不得按本 CP 受理。

3.2.4 电子政务设备证书身份鉴别

电子政务设备证书申请人为设备所属政务部门、政务信息系统运营方或经授权的责任主体。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、政务使用场景和申请意愿。

设备证书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. 设备部署于电子政务活动或政务信息系统的场景证明；

5. 证书用途、接入范围和限制条件；

6. 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、服务协议和意愿确认记录。

政务设备证书明确设备所服务的政务部门、政务信息系统、政务服务事项、接入平台或业务接口范围。政务场景证明材料可包括政务系统立项或验收材料、政务部门出具的接入证明、系统运营授权、平台开通记录、接口接入记录、项目合同或经 CPS2 认可的其他证明材料。

政务平台、业务系统或接入规范指定特定证书策略对象标识符的，沃通在受理、配置和签

发前核实该要求的来源、适用范围、批准记录和证书扩展项配置影响。未经核实和批准的外部平台要求，不得改变本 CP 确定的策略边界。

3.2.5 订户告知与意愿确认

依据《电子政务电子认证服务管理办法》第 21 条，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，并签订电子政务电子认证服务协议：

1. 本 CP 项下证书适用于电子政务电子认证服务；

2. 电子签名认证证书和电子签名的使用条件、证书类型、密钥用法和使用限制；

3. 电子签名所产生的法律责任，以及订户私钥保护、及时报告私钥泄露或证书异常的义务；

4. 保存和使用证书持有人信息的权限和责任、个人信息保护、记录留存要求；

5. 沃通和证书持有人的责任范围、赔偿规则、证书撤销、状态查询、更新和争议处理方式及收费标准。

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。

3.2.6 互操作准则

本 CP 项下证书参与政务平台互认、跨系统验证、电子签章互认或其他电子政务应用时，遵循下列准则：

1. 沃通负责按照本 CP 和 CPS2 签发、管理、撤销证书并提供证书状态服务；

2. 订户负责按照证书用途和授权范围使用证书，并向接入系统说明证书用途限制；

3. 政务平台或业务系统不得扩大解释本 CP 项下证书的用途，不得绕过证书状态验证或政务场景边界；

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 CPS2 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、政务场景确认、用途确认和意愿确认。被撤销或已过期的证书不

得进行密钥更新。

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 CPS2 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、政务部门、依法承担行政职能的组织、政务信息系统运营方、设备所属机构或经授权代表。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、政务场景证明、用途说明、设备信息以及 CPS2 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，并与订户签订电子政务电子认证服务协议。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。

正式签发本 CP 项下证书前，CPS2 完成监管要求的公布和备案。本 CP 文档对象标识符、证书链、证书状态服务和签发系统完成必要的评估、验证和批准。

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 章和 CPS2 对申请实体身份、授权关系、政务场景、证书用途、私钥拥有权和意愿确认进行识别与鉴别。对设备证书，特别核验证书使用范围、设备归属、政务系统部署场景和禁止用途确认。

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、授权关系确认、政务场景确认、用途确认、意愿确认通过且已签订电子政务电子认证服务协议；

3. 证书主体名称、证书用途、证书策略和有效期符合本 CP、CPS2 和适用标准；

4. 未发现虚假申请、冒用身份、越权申请、违规用途或其他不适宜签发情形；

5. 申请人已确认法律适用性、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、设备归属、政务场景或证书用途无法确认；

3. 申请用途超出本 CP 允许范围；

4. 申请人拒绝确认法律适用性、用途限制或拒绝签订服务协议；

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、争议风险或监管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。常规证书申请原则上在 2 个工作日内完成处理；批量申请、政务平台接入申请或复杂授权场景按照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、监管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、CPS2 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、CPS2、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、撤销状态和适用政务场景。依赖方不得在本 CP 允许范围之外信赖证书，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。

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 CPS2 提交证书更新申请。

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、设备所属机构、政务信息系统运营方或 CPS2 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、未过期、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、政务场景复核和意愿确认。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 CPS2、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、设备所属机构、政务信息系统运营方或 CPS2 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 CPS2 规定的复核流程确认订户身份、授权关系、政务场景、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 CPS2 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 CPS2、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、政务场景、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、设备所属机构、政务信息系统运营方或 CPS2 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，并按 CPS2 撤销原证书。

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 CPS2、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. 订户授权关系终止、机构注销、岗位调离、设备退役、系统停止使用或政务场景不再成立；

5. 证书被用于超出本 CP 允许范围的用途；

6. 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；

7. 法律法规、监管要求、法院或仲裁机构生效文书、服务协议或 CPS2 规定的其他撤销情形。

证书到期按自动失效处理，不因自然到期列入证书撤销列表。

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、设备所属机构、政务信息系统运营方、依赖方、监管机构、司法机关、仲裁机构或 CPS2 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渠道或 CPS2 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。

4.9.6 证书撤销列表发布频率

用户证书撤销列表至少每 24 小时发布一次。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

沃通按照 CPS2 提供本 CP 项下证书的挂起和恢复服务。证书挂起适用于证书使用权、授权关系、私钥控制、设备状态、政务场景或证书信息存在短期不确定性，但尚未达到撤销条件的情形。

证书挂起请求由订户、经授权代表、设备所属机构、政务信息系统运营方、沃通或 CPS2

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 CPS2 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；适用法律法规、监管要求、政务平台规则或 CPS2 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、政务场景或私钥控制状态。挂起期限届满仍不能满足恢复条件的，撤销证书或按照 CPS2 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。在线证书状态服务地址为 http://ocsp2.wotrus.com/。当在线状态服务异常时，依赖方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（不低于 99.9%）和异常期间处理规则由 CPS2 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、政务场景终止、设备退役、系统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 CPS2 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 项下签名私钥由订户或其授权系统在专控密码设备或模块中自行生成与控制，沃通不得以恢复签名能力为目的托管或恢复签名私钥。

本 CP 项下加密证书的加密密钥对由国家密码管理局和省部密码管理部门规划建设的密钥管理基础设施（KMI）提供管理服务。在符合法律法规、密码管理要求、CPS2、服务协议和安全策略委员会批准规则的前提下，密钥恢复仅限满足数据解密、业务连续性或依法问责取证要求的加密用途，不得用于恢复或复制签名私钥。

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电子政务电子认证服务场所，覆盖机房、公共区、服务区、管理区、核心区、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、7×24 小时视频监控（记录保存不少于 6 个月）、出入登记、双人双因素控制和访问复核控制人员进出，并通过国标 A 级机房环境监测、BMB3-1999 C 级屏蔽室定期检测（每 5 年不少于 1 次）、消防、防水、防雷、电力保障（含门禁与入侵报警独立 8 小时以上 UPS）、防盗、防破坏和介质交接管理保障系统连续运行。CPS2 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、政务场景核验、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；涉及政务系统、政务主体或平台指定策略的业务，按照 CPS2 留存核验依据和批准记录。

5.3 人员控制

沃通对参与本 CP 项下证书服务的人员（含受委托机构人员）实施身份背景核验、岗位授权、保密承诺、岗位培训、再培训、权限管理、岗位变更管理和离岗管理。关键岗位人员具备电子政务电子认证服务运行、密码安全管理、主体核验、政务场景识别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、政务主体和政务场景确认、平台策略核实、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、政务主体识别记录、政务场景证明、平台策略核实记录、授权记录、用途确认、告知确认、服务协议、证书签发记录、撤销记录、CRL 备份、状态服务记录和审计日志。面向政务部门的电子政务电子认证服务记录至少保存至对应证书失效后 10 年；面向企事业单位、社会团体、社会公众的相关服务记录至少保存至对应证书失效后 5 年；CRL 备份保存不少于对应证书失效后 10 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 条和 CPS2 执行；涉及政务平台接入或证书链变化的，沃通同步完成平台影响评估、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、政务场景核验、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《电子政务电子认证服务管理办法》第 36 条规定的重大安全风险和安全事件、重要系统或关键设备事故、关键岗位人员变动、重大财产损失时，沃通自发生之日起 15 日内向住所地省、自治区、直辖市密码管理部门报告，并按照 CPS2 启动应急处置、影响评估、业务恢复、状态更新和记录留存流程。

5.8 电子认证服务机构或注册机构的终止

沃通暂停或终止本 CP 项下电子政务电子认证服务时，按照《电子政务电子认证服务管理办法》第 29 条及 CPS2 处理订户通知、政务平台通知、业务承接、证书撤销或迁移、记录移交、状态服务延续、公告和善后事项。拟暂停或者终止服务的，沃通至少提前 90 日通知有关各方，并至少提前 60 日向国家密码管理局报告，同时与其他电子政务电子认证服务机构就业务承接进行协商；未能达成承接协议的，在报告时一并向国家密码管理局提出安排其他机构承接业务的申请。沃通同时履行根据国家密码管理局安排承接其他机构电子政务电子认证服务业务的法定义务。

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 项下证书签名密钥对由订户在其专控的智能密码钥匙、智能 IC 卡或符合 GM/T 0034、GM/T 0028 要求的密码模块中生成，加密密钥对由国家密码管理局和省部密码管理部门规划建设的 KMI 生成与管理。CA 密钥和证书状态服务密钥在符合国家密码管理要求的硬件密码设备中生成，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

订户签名私钥在专控密码设备内生成并由订户专有专控，不以任何形式传送。加密证书密钥由 KMI 按 GM/T 0034 安全下发至订户介质；任何情况下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 CPS2 认可的其他安全方式提交给沃通。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、CPS2 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 CPS2 的 SM2 算法（密钥长度 256 比特）及 SM3 杂凑算法。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

订户使用符合国家密码管理要求的智能密码钥匙、安全芯片、服务器密码机等密码设备或密码模块，结合强口令、PIN 码等措施保护私钥。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国家密码管理局认定的硬件密码设备中生成、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 5 选 3 门限秘密共享及职责分离机制。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、5 选 3 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 KMI 规范、CPS2、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，并在受控密码设备中进行。订户签名私钥不从密码设备导出。

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 CPS2 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、基线扫描、渗透测试、源代码审计和安全加固；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。开发、测试与生产环境严格隔离；涉及证书策略、证书格式、证书状态服务、政务平台接入和安全控制的重要变更经过评估、审批、验证和记录，涉及重大变更的按规定向国家密码管理部门办理审批或报备手续。

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、不同运营商双网络链路接入、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 CPS2 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，符合 GM/T 0015-2023 及 GB/T 20518-2018，

并载明《电子政务电子认证服务管理办法》第 19 条规定的全部法定要素（认证机构名称、持有人名称、序列号、有效期、证书策略对象标识符、电子签名验证数据、认证机构电子签名等）。

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
电子政务个人电子认证证书、电子政务机构电子认证证书、电子政务个人电子签名认证证书、电子政务机构电子签名认证证书、电子政务设备证书	国家电子认证根 ROOTCA → WoTrus SM2 CA → WoTrus GCA → 订户证书	http://ldap.wotrus.com/crl/wotrussm2gca.crl	http://ocsp2.wotrus.com/	http://ldap.wotrus.com/subca/wotrussm2gca.crt

7.1.3 证书类型

本 CP 项下证书类型如下：

证书类型	证书机制	策略对象标识符	适用 CPS	用途边界
电子政务个人电子认证证书	双证书	1.2.156.150570.6.2	CPS2	政务活动中个人身份认证、电子签名和数据加密。
电子政务机构电子认证证书	双证书	1.2.156.150570.6.2	CPS2	政务活动中机构身份认证、电子签章和数据加密。
电子政务个人电子签名认证证书	单证书	1.2.156.150570.6.2	CPS2	仅需电子签名、无数据加密需求的个人政务签署场景。
电子政务机构电子签名认证证书	单证书	1.2.156.150570.6.2	CPS2	仅需电子签名或电子签章、无数据加密需求的机构政务签署场景。
电子政务设备证书	双证书	1.2.156.150570.6.2	CPS2	政务设备身份识别、通信加密和访问控制。

7.1.4 证书主体名称

个人证书主体名称体现经核验的个人身份。机构证书主体名称体现经核验的机构身份。设备证书主体名称体现设备、服务节点或系统组件及其所属机构。证书主体名称不得误导依赖方将证书用于本 CP 允许范围之外的用途。

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。具体算法对象标识符以证书实际编码、CPS2 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
签名证书	数字签名、认可签名	客户端身份验证 1.3.6.1.5.5.7.3.2，或按证书用途和 CPS2 确定
加密证书	密钥加密、数据加密、密钥协商	按证书用途和 CPS2 确定
设备证书	数字签名、认可签名、密钥加密、数据加密、密钥协商，按签名证书和加密证书分别设置	服务器身份验证 1.3.6.1.5.5.7.3.1、客户端身份验证 1.3.6.1.5.5.7.3.2，或按设备用途和 CPS2 确定

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 CPS2 的其他扩展项（如个人身份证件标识、统一社会信用代码等标准扩展项）。

扩展项的关键性符合 X.509、GB/T 20518-2018、GM/T 0015-2023、CPS2 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 项下订户证书最长有效期不超过 1827 天，且不得超过 5 年。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、CPS2、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 CPS2 处理。

本 CP 项下证书撤销列表地址为 http://ldap.wotrus.com/crl/wotrussm2gca.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、CPS2 和服务运行规则处理。在线证书状态服务地址为 http://ocsp2.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、CPS2 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、服务质量自评估、技术检查和风险评估。本 CP 至少每年进行一次适用性评审；沃通自行或者委托专业机构每年至少进行一次电子政务电子认证服务合规性评估，并向住所地省、自治区、直辖市密码管理部门报送合规性评估报告；每年 1 月 15 日前向住所地省、自治区、直辖市密码管理部门报送上一年度工作报告。电子政务主体判定、身份鉴别、意愿确认、证书状态服务、密钥管理和记录留存纳入定期审计范围。

8.2 审计者身份和资质

审计者具备与电子政务电子认证服务、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、CPS2、证书申请受理、身份鉴别、政务场景确认、授权确认、告知确认、服务协议签署、受委托机构管理与备案、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 CPS2、法律法规和《电子政务电子认证服务管理办法》第 36 条等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、状态服务记录和政务场景记录，并重点覆盖政务主体识别、政务场景证明、平台指定策略对象标识符配置、设备证书授权和高风险撤销事件。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。外部审计、监管检查或政务平台规则要求更高抽样比例的，从其规定。

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。整改关闭以业务记录更正、配置核验、补充授权材料、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 CPS2 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 项下电子政务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。

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 CPS2 建立与其电子认证服务相适应的责任风险保障机制，维持与电子政务电子认证业务规模相称的财务保障能力（责任资金保障额不低于上年度电子认证业务总营收的 1.5%）。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、CPS2、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国家秘密、工作秘密、非公开业务信息、技术信息、身份信息、授权信息、系统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《中华人民共和国个人信息

保护法》、GB/T 35273、CPS2、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、CPS2、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、CPS2、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、CPS2 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或第三方违规使用证书所造成的损失承担责任。担保免责不免除沃通依法应承担的法定赔偿责任。

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、监管要求、CPS2、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、CPS2 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、CPS2 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。依据《中华人民共和国电子签名法》第 28 条及《电子政务电子认证服务管理办法》第 40 条，电子签名人或者电子签名依赖方因依据沃通提供的电子政务电子签名认证服务在政务活动中遭受损失，沃通不能证明自己无过错的，依法承担赔偿责任。因订户、依赖方或第三方违反本 CP、CPS2、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、状态服务、告知记录、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、CPS2、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，并按《电子政务电子认证服务管理办法》第 16 条予以公布并在 30 日内向住所地省、自治区、直辖市密码管理部门备案。

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 CPS2、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 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 CPS2 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；CPS2 承担实施细则，不得改变本 CP 的策略结论。

如 CPS2、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 CPS2 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 CPS2、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。