沃通电子认证服务有限公司

SM2 全球信任体系电子认证业务规则（CPS）

版本：V1.0.1

发布日期：2025 年 1 月 6 日

生效日期：2025 年 1 月 6 日

沃通电子认证服务有限公司

版本控制表

版本	状态	修订说明	审核/批准人	生效时间
V1.0.1	版本发布	初始版本	沃通安全策略管理委员会	2025 年 1 月 6 日

声明

本 CPS 全部或者部分支持下列标准：

- GB/T 35276-2017　信息安全技术 SM2 密码算法使用规范
- GB/T 20518-2018　信息安全技术 公钥基础设施 数字证书格式
- 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 19713-2005 信息安全技术 公钥基础设施 在线证书状态协议
- RFC3647：互联网 X.509 公钥基础设施-证书策略和证书业务声明框架
- RFC2459:互联网 X.509 公钥基础设施-证书和 CRL 属性
- RFC 5280:InternetX.509 公钥基础设施证书和 CRL 结构
- RFC2560:互联网 X.509 公钥基础设施-在线证书状态协议-OCSP

- ITU-TX.509 V3（1997）:信息技术一开放系统互连-目录:认证框架

目 录

1. 概括性描述

1.1. 概述

1.1.1. 公司介绍

沃通电子认证服务有限公司（WoTrusCALimited）（以下简称“沃通”，或简称“WoTrus”），是获得工业和信息化部颁发《电子认证服务许可证》的电子认证服务机构。公司严格按照《中华人民共和国电子签名法》和《电子认证服务管理办法》的要求，以及相关管理规定，提供数字证书签发、更新、吊销或管理等服务，并通过以 PKI 技术、数字证书应用技术为核心的产品和服务，为电子认证活动提供可信身份、可信时间和可信行为的网络信任环境。

沃通公司遵照《中华人民共和国电子签名法》、《中华人民共和国密码法》、《电子认证服务管理办法》、《电子政务电子认证服务管理办法》、《电子认证服务密码管理办法》等法律法规的要求和相关管理规定，为用户提供数字证书申请、颁发、存档、查询、撤销等服务，并通过以 PKI 技术、数字证书应用技术为核心的应用安全解决方案，为电子政务、电子商务、企业信息化构建安全、可靠的信任环境。沃通公司具备保持多年连续 WebTrust 国际安全审计认证水平，具有国际标准化的运营管理和服务水平，可为全球用户提供规范可信的电子认证服务。

1.1.2. 电子认证业务规则

本电子认证业务规则由沃通公司按照国家密码管理局《电子认证服务密码管理办法》、中华人民共和国工业和信息化部《电子认证服务管理办法》的要求，

依据《电子认证业务规则规范（试行）》、《WebTrust 电子认证机构原则及规范》制定。

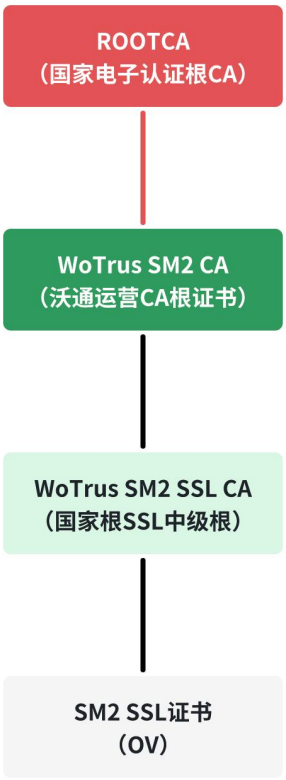
本电子认证业务规则适用于沃通公司基于国家密码管理局认可的国产密码算法并遵循 WebTrust 国际标准运营管理的 RootCA、中级 CA，以及注册机构、证书申请人、订户和依赖方等实体， 涵盖了签发和管理 SM2 算法的 DV SSL 全球服务器证书、 OV SSL 全球服务器证书、EV SSL 全球服务器证书、时间戳证书以及客户端身份证书等相关的具体操作和流程，各参与方必须完整地理解和执行本电子认证业务规则所规定的条款，并承担相应的责任和义务。

沃通公司遵循国际 CA/Browser 论坛最新发布的《Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates》（简称“Baseline Requirements”）、《 Guidelines For The Issuance And Management Of Extended Validation Certificates》（简称“EV Guidelines”）、《Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates》（简称 “ Code Signing Baseline Requirements”）对于 SSL 全球服务器证书和代码签名证书的验证要求，定期查看其更新情况，并将持续根据其发布的版本修订本电子认证业务规则。如果本电子认证业务规则和国际 CA/Browser 论坛发布的相关证书验证规范中的条款有不一致的地方， 则以国际 CA/Browser 论坛正式发布的规范为准。

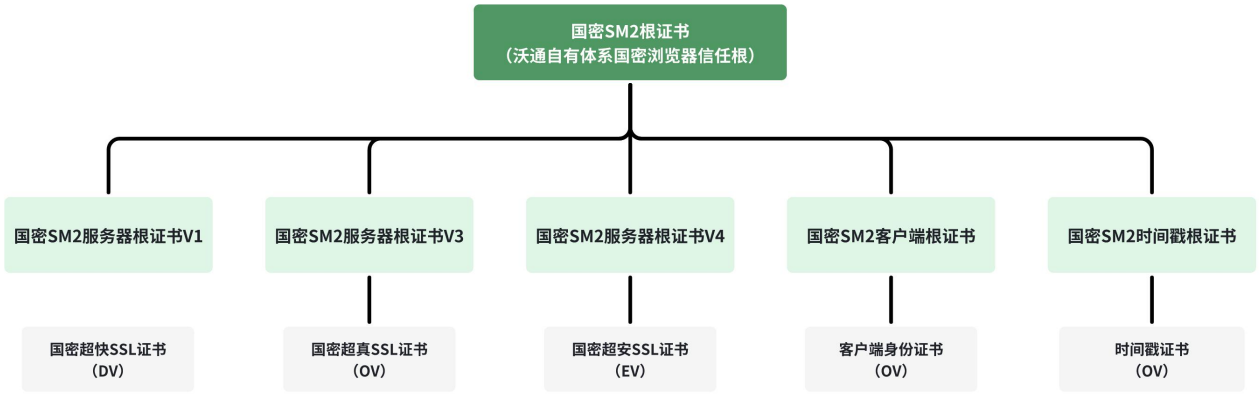
1.1.3. 证书体系架构

本 CPS 中的 SM2 全球信任体系有 2 个根证书，分别为“ROOTCA”、“国密 SM2

根证书”，其中 ROOTCA 是国家密码管理局管理的国家电子认证根 CA，国密 SM2 根证书是沃通电子认证服务有限公司自有体系的 SM2 SSL 根证书。每个根证书下设中级根 CA 证书签发订户证书。



ROOTCA 是国家密码管理局管理的国家电子认证根 CA，密码算法为 SM2，根密钥长度为 256-bit，下设沃通电子认证服务有限公司 WoTrus SM2 CA 证书及 WoTrus SM2 SSL CA 证书，密钥长度为 256-bit，签发密钥长度为 SM2 256-bit 的 OV SSL 全球服务器证书。



国密 SM2 根证书的密码算法为 SM2，根密钥长度为 256-bit，下设 3 个 SSL 中级根 CA 证书，其中：

（1）国密 SM2 服务器根证书 V1，密钥长度为 256-bit，签发密钥长度为 SM2 256-bit 的 DV SSL 全球服务器证书；

（2）国密 SM2 服务器根证书 V3，密钥长度为 256-bit，签发密钥长度为 SM2 256-bit 的 OV SSL 全球服务器证书；

（3）国密 SM2 服务器根证书 V4，密钥长度为 256-bit，签发密钥长度为 SM2 256-bit 的 EV SSL 全球服务器证书。

（4）国密 SM2 客户端根证书，密钥长度为 256-bit，签发密钥长度为 SM2 256-bit 的单位机构（OV）客户端身份证书。

（5）国密 SM2 时间戳根证书，密钥长度为 256-bit，签发密钥长度为 SM2 256-bit 的时间戳证书。

1.2. 文档名称与标识

本文档名称是《沃通电子认证服务有限公司 SM2 全球信任体系电子认证业务规则》（以下简称“本 CPS”或 本《电子认证业务规则》）。

沃通公司向国家 OID 注册管理中心注册了相应的对象标识符（OID），本文档涉及到的证书 OID 如下：

EV SSL 全球服务器证书定义的 OID 为 1.2.156.150570.3.1.4；

OV SSL 全球服务器证书的 OID 为 1.2.156.150570.3.1.3；

DV SSL 全球服务器证书的 OID 为 1.2.156.150570.3.1.1；

OV 客户端证书的 OID 为 1.2.156.150570.3.3.3；

时间戳证书的 OID 为 1.2.156.150570.3.4.3。

1.3. PKI 参与者

1.3.1. 电子认证服务机构

电子认证服务机构是受用户信任，负责证书的创建、颁发、撤销和管理的权威机构，为从事电子交易活动的各方主体颁发数字证书、提供数字证书验证服务。

沃通公司是依法设立的第三方电子认证服务机构（简称“CA 机构”），符合《中华人民共和国电子签名法》、《电子认证服务管理办法》等规定。

1.3.2. 注册机构

注册机构作为电子认证服务机构授权委托的下属机构，包括注册系统（简称：RA 系统）和证书本地受理点，负责受理证书申请。

沃通公司除了承担 CA 机构的角色外，将自行担任 RA 注册机构，不委托第三方担任 RA 注册机构，授权的注册机构即由本 CA 机构担任。

1.3.3. 订户

订户是从 CA 机构接收数字证书的实体，可以是个人、机构或设备。订户通常需要同 CA 机构签订合约以获得数字证书，并承担作为证书订户的责任。

1.3.4. 依赖方

依赖方是为某一应用而使用、信任本 CA 机构签发的证书的实体。依赖方可以是、也可以不是一个订户。

1.3.5. 其他参与者

其他参与者指为 CA 证书服务体系提供相关服务的其他实体。

1.4. 证书应用

1.4.1. 适合的证书应用

本 CA 机构签发的数字证书适合应用在企业信息化、电子政务、电子商务及公共服务等领域，以实现身份认证、关键数据加密等目的，同时也确保互联网信息传递双方身份的合法性和真实性、信息的完整性和保密性。

本 CA 机构的数字证书包含 SSL 全球服务器证书、时间戳证书、客户端身份证书，证书支持相应的合法应用，具体应用如下：

(1) SSL 全球服务器证书

按照所签发证书的安全等级、鉴别方式等不同， SSL 全球服务器证书包括：DV SSL 全球服务器证书、OV SSL 全球服务器证书、 EV SSL 全球服务器证书。DV SSL 全球服务器证书只验证网站域名所有权、控制权，不验证网站域名所有者的真实身份，可以保证网站的信息从用户浏览器到服务器之间的传输是高强度加密传输的；OV SSL 全球服务器证书除了验证网站域名所有权、控制权，还会对网站域名所属机构的真实身份进行验证；EV SSL 全球服务器证书则是经过更加严格的身份验证后签 发的一种扩展验证型服务器证书，其验证流程符合 CA/Browser 论坛制订的增强型身份验证标准（EV Guidelines） 。

SSL 全球服务器证书可用于验证证书中标识的网络主机服务器或互联网域名拥有者的身份，同时该类证书还用于订户浏览器与 WEB 服务器之间建立安全通道， 实现数据信息在客户端和服务器之间的加密传输， 防止数据信息的泄露。适合应用在网上银行、电子商务、电子政务、企业信息化以及公共服务等各个领域，为建设网络可信空间提供基础性信任服务。

(2) 时间戳证书

时间戳证书包括：OV 时间戳证书。

OV 时间戳证书主要用于时间戳服务器，提供数字签名的功能。

(3) 客户端身份证书

客户端身份证书包括：OV 客户端身份证书。

客户端身份证书主要用于网络系统登录认证时，安全识别证书持有人身份的功能。

1.4.2. 限制的证书应用

在本信任体系下的证书根据其类型在功能上有所限制，比如：EV SSL 服务器证书只能用于经过严格认证的 WEB 服务器。

各类证书的密钥用法在订户证书中的扩展项中进行了限制。然而基于证书扩展项限制的有效性取决于应用软件，如果参与方不遵守相关约定，其对证书的应用超出本 CPS 限定的应用范围，将不受 CA 机构的保护。

本 CA 机构发放的数字证书禁止在违反国家法律、法规或破坏国家安全的情况下使用，订户不得将证书用于钓鱼式攻击、欺诈网站或其他恶意犯罪行为，不得将证书用于发布任何包含或疑似包含恶意代码的程序，由此造成的法律后果由订户负责。

1.5. 策略管理

1.5.1. 策略文档管理机构

本 CPS 的管理机构是沃通安全策略管理委员会。由沃通安全策略管理委员会负责本 CPS 的制订、发布、更新等事宜。

1.5.2. 联系人

本 CPS 在沃通官网进行发布，对具体个人不另行通知。

任何有关 CPS 的问题、建议、疑问等以及证书问题报告和证书撤销请求都可以按以下方式进行联系。

官网地址：https://www.wotrus.com/

服务邮箱：casupport@wotrus.com

总机号码：+86-755-86008688

传真号码：+86-755-33975112

联系地址：中国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 CPS 符合策略的机构

本 CPS 由沃通安全策略管理委员会组织制定，报沃通公司安全策略管理委员会批准实行。

1.5.4. CPS 批准程序

本 CPS 由沃通安全策略管理委员会，组织 CPS 编写小组。编写小组完成编写 CPS 草案后，由沃通安全策略管理委员会组织对 CPS 草案进行初步评审。初步评审后，将 CPS 评审稿提交沃通安全策略管理委员会审批。经沃通安全策略管理委

员会审批通过后，在沃通电子认证服务有限公司的网站上对外公布，并根据《电子认证服务管理办法》的规定，从对外公布之日起的三十日之内向工业和信息化部备案。

1.5.5. CPS 修订

CA 机构根据国家政策法规、技术要求、标准变化及业务发展情况等及时修订本 CPS。

CA 机构将对 CPS 进行严格的版本控制，并由安全策略管理委员会负责相关事宜。本 CPS 至少每年修订一次。如果无内容改动，则递增版本号、更新发布时间、生效时间及修订记录。修订后的 CPS，从对外公布之日起的三十日之内向工业和信息化部备案。

1.6. 定义和缩写

1.6.1. 定义

(1) 安全策略管理委员会：沃通公司认证服务体系内的最高策略管理监督机构和 CP、CPS 的批准机构。

(2) 电子认证服务机构：受用户信任，负责证书的创建、颁发、撤销和管理的权威机构。

(3) 注册机构：注册机构（RA）RegistRAtion Authority 具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销或挂起证书，处理订户撤销或挂起其证书的请求，同意或拒绝订户更新

其证书或密钥的请求。但是，RA 并不签发证书（即 RA 代表 CA 承担某些任务）。

(4) 数字证书：由电子认证服务机构签名的包含证书持有者公开身份信息和公开密钥的电子文件。

(5) 证书撤销列表：一个经电子认证服务机构数字签名的列表，它指定了一系列证书颁发者认为无效的证书，也称黑名单服务。

(6) 证书策略：关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

(7) 电子认证业务规则：关于证书电子认证服务机构在签发、管理、撤销或更新证书（或更新证书中的密钥）过程中所采纳的业务实践的声明。

(8) 录入员：负责录入证书申请者提交的信息，协助用户办理数字证书申请、更新、撤销等手续。

(9) 审核员：CA 机构根据业务需要设置一级或多级审核员，负责审核证书申请信息，审核通过后，批准签发证书。

(10) CA 注销列表：一个经电子认证服务机构数字签名的列表，标记已经被注销的 CA 的公钥证书的列表，表明该 CA 及签发的证书已经无效。

(11) 公开密钥基础设施：支持公开密钥体制的安全基础设施，提供身份鉴别、加密、完整性和不可否认性服务。

(12) 私钥：经由数字运算产生的密钥，用于制作数字签名，亦可依据其运

算方式，就相对应的公开密钥加密的文件或信息予以解密。

(13) 公钥：公钥是经由数字运算产生的密钥，用于验证其对应的私钥产生的数字签名。公钥可以公开，一般标示于在线数据库、存储库或其他公共目录中，使任何希望得到公钥的人都能得到。

(14) 在线证书状态协议：在线证书检查协议，可使依赖方应用软件判断某指定证书的状态。

(15) WebTrust：针对电子认证服务机构的现行国际审计标准。

(16) SSL 全球服务器证书：一种可以让访问者通过浏览器来验证网站真实身份的数字证书，通过服务器证书可以为客户端和服务端间建立具有高安全性的 SSL 加密通道。

(17) DV SSL 全球服务器证书：域名验证型 SSL 证书，只验证网站域名所有权的简易型 SSL 证书。

(18) OV SSL 全球服务器证书：企业验证型 SSL 证书，既要验证网站域名所有权，也要验证网站经营者（机构）的真实身份。

(19) EV SSL 全球服务器证书：增强验证型 SSL 证书，需要对网站域名所有权、网站经营者及证书申请者的真实身份进行更加严格的增强型/扩展型验证，遵循全球统一的严格身份验证标准。

(20) 时间戳证书：用于时间戳服务器，提供数字签名的功能。

(21) 客户端身份证书：用于客户端网络系统登录认证时，安全识别证书持有人身份的功能。

1.6.2. 缩写

(1) CA（Certificate Authority）：电子认证服务机构，证书颁发机构。

(2) RA（RegistRAtion Authority）：注册审核服务机构。

(3) CP（Certificate Policy）：证书策略。

(4) CPS（Certification PRActice Statement）：电子认证业务规则。

(5) SSL （Secure Sockets Layer）：加密套接层协议。

(6) TLS （TRAnsport Layer Security）：传输层安全。

(7) CRL（Certificate Revocation List）：证书撤销列表。

(8) ARL （Certificate Authority Revocation List）：CA 注销列表。

(9) LDAP （Lightweight Directory Access Protocol）：轻型目录访问协议。

(10) OCSP（Online Certificate Status Protocol）：在线证书状态协议。

(11) SCA（State CryptogRAphy AdministRAtion）：国家密码管理局。

(12) PIN （Personal Identification Number）：个人身份识别码。

(13) PKCS （Public KEY CryptogRAphy Standards）：公共密钥密码标准。

(14) PKI （Public Key InfRAstructure）：公共密钥基础设施。

(15) RFC （Request For Comments）：互联网建议标准。

(16) CAA（Certification Authority Authorization）：认证机构授权。

(17) CSR （Certificate Signing Request）：证书请求文件。

(18) DBA （Doing Business As）：商业名称。

(19) DNS （Domain Name System）：域名系统。

(20) ICANN （Internet CorpoRAtion for Assigned Names and Numbers）：互联网名字与编号分配机构。

(21) EV（Extended Validation）：扩展验证/增强验证。

(22) FIPS （FedeRAl Information Processing Standards）：联邦信息处理标准。

(23) FQDN （Fully Qualified Domain Name）：完全限定域名。

(24) gTLD （Generic top-level domain）：通用顶级域名。

2. 信息发布与管理

2.1. 信息库

本 CA 机构的信息库面向订户及依赖方提供信息服务，提供信息服务包括但不限于以下内容：根证书和中级 CA 证书、CP 和 CPS 现行和历史版本以及沃通公司不定期发布的信息。

沃通的信息库地址为：https://www.wotrus.com/ca/。

2.2. 认证信息的发布

本 CA 机构通过官网公布以下信息： 根证书和中级 CA 证书、CP 和 CPS 现行和历史版本以及其他由沃通公司不定时发出的信息。沃通公司官网网址：https://www.wotrus.com，是沃通公司发布所有信息最权威的渠道，供相关方下载、查阅。

本 CA 机构通过在线服务发布 CRL 和 OCSP 信息，订户及依赖方可以通过在线服务获取证书状态查询、证书撤销查询服务等。

本 CPS 发布在沃通公司的网站上（https://www.wotrus.com/ca/），供相关方下载、查阅。

2.3. 发布时间或频率

本 CA 机构的 CPS 按照本 CPS 第 1.5.4 节所述的批准流程，经沃通安全策略管理委员会审批通过后，在沃通公司的网站上对外公布。本 CA 机构至少每年发布一次 CP 和 CPS，CP 和 CPS 可通过信息库 7X24 小时获得。

本 CPS 一经网站发布，即时生效。

CA 机构发布 CRL 的频率根据证书策略确定，订户证书的 CRL 一般为 24 小时定期发布，订户证书 CRL 的有效期最长不超过 5 天。中级 CA 的 ARL 一般为 12 个月定期发布，中级证书 ARL 的有效期最长不超过 12 个月。如果根证书被撤销，应及时在网站公布撤销信息。

在特殊情况下，CA 机构可以提前进行证书和 CRL 的发布。

2.4. 信息库访问控制

对于公开发布的 CP、CPS 和 CA 证书等公开信息，本 CA 机构允许公众自行通过网站以只读方式进行查询和访问。

CA 机构通过网络安全防护、系统安全设计、安全管理制度确保只有经过授权的人员才能对信息库中的信息进行增加、删除、修改和发布。

3. 标识与鉴别

3.1. 命名

3.1.1. 名称类型

CA 机构颁发的数字证书应符合 X.509 标准，含有颁发机构和证书订户主题甄别名，每个订户对应一个甄别名（Distinguished Name，简称 DN），甄别名采 用 X.500 标准命名方式，是证书持有者的唯一识别名。

对于 SSL/TLS 服务器证书，所有的域名或 IP 地址都添加到主题别名中， 而

通用名必须是一个出现在主题别名中的域名或 IP 地址。对于 EV SSL 服务器证书， 所有的域名都添加到主题别名中， 且添加到主题别名中的域名不能包含通配符， 而通用名必须是一个出现在主题别名中的域名。

本 CA 机构的 RootCA 主题甄别名命名规则：

属性	值
通用名（ CN）	RootCA 名称
机构（ O）	WoTrus
国家（ C）	CN

本 CA 机构的中级 CA 主题甄别名命名规则：

属性	值
通用名（ CN）	中级 CA 名称
机构部门（ OU）	机构或部门名称（可选）
机构（ O）	WoTrus

地区（ L）	颁发者所在城市（可选）
省（S）	颁发者所在省份（可选）
国家（ C）	CN

证书订户的主题甄别名命名规则：

属性	**值**
通用名（CN）	域名/IP，或订户名称，或其他可识别的名称。
电子邮件（E）	订户的电子邮件地址（可选）。
机构部门（OU）	可以包含以下一个或多个内容：订户所在机构的具体部门； 其他描述身份或证书类型的文字（可选）。
机构（O）	对于有确定机构的订户，是订户所在机构名称。
地区（L）	订户所在城市（可选）。
省（S）	订户所在省份（可选）。

国家（C）	订户所在国家，如：CN。

3.1.2. 对名称意义化的要求

订户的甄别名（DN）是标识证书主题唯一性的元素，必须具有一定的代表意义，可与证书持有者的特有属性相关联。

(1) EV SSL 证书的甄别名通常包含订户所属机构拥有的域名、订户机构的企业身份信息，作为标识订户的关键信息被鉴别和认证，订户机构的企业身份信息需经过第三方严格的身份审核。

(2) OV SSL 证书的甄别名通常包含订户所属机构拥有的域名或公网 IP，以及订户机构的企业身份信息，作为标识订户的关键信息被鉴别和认证，订户机构的企业身份信息需经过第三方严格的身份审核。

(3) DV SSL 证书的甄别名通常仅包含订户所属机构拥有的域名或公网 IP， 作为标识订户的关键信息被认证。

(4) OV 时间戳证书甄别名中的通用名通常可包含组织机构名称，作为标识订户的关键信息被认证。

(5) OV 客户端身份证书甄别名中的通用名通常可包含组织机构名称，作为标识订户的关键信息被认证。

3.1.3. 订户的匿名或伪名

本 CPS 规定，订户（证书申请人）不能使用匿名或伪名。

3.1.4. 理解不同名称形式的规则

CA 机构签发的数字证书符合 X.509 V3 标准,甄别名格式遵守 X.500 标准。甄别名的命名规则由沃通公司定义。甄别名（DN）的内容一般由 CN、O、C 等部分组成。其中 CN 用来表示用户名，O 用来表示组织单位名称、C 用来表示国家。

3.1.5. 名称的唯一性

在本信任体系中，不同订户的证书主题甄别名不能相同，必须是唯一的。但对于同一订户，可以用其主题名为其签发多张证书，但证书的扩展项不同。当证书申请中出现不同订户存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

3.1.6. 商标的识别、鉴证和角色

沃通公司尊重任何订户名称中的注册商标权，任何证书申请者不应使用任何可能侵犯知识产权的名称。证书信息中包含商标时，订户应向沃通公司提供商标注册方所有权的文件证明，这种要求不是也不应该被认为是沃通公司将对商标的归属进行判断和决定。

沃通公司不负责解决证书中任何关于域名、商标等知识产权的纠纷，并且不保证这种权利的唯一性。对于因商标、服务标志等的归属问题造成的纠纷，沃通公司没有权利，也没有义务去拒绝或者质疑任何可能导致产生知识产权纠纷的证

书申请，不负有仲裁或调停等责任，但保留撤销任何涉及知识产权争议的证书的权利。

3.2. 初始身份确认

3.2.1. 证明持有私钥的方法

证书申请者必须证明持有与所注册公钥相对应的私钥，证明方法包括：PKCS#10、其它与此相当的密钥标识方法，或者 CA 机构接受的其它证明方式。

3.2.2. 机构身份和域名的鉴别

订户申请沃通公司在该信任体系下签发的证书前应由证书申请人，提供有效身份证明文件、证书申请文件，并接受证书申请的有关条款，同意承担相应的责任。

CA 机构或注册机构接受订户的证书申请后，应对订户的身份真实性进行审核，并按照双方的约定妥善保存订户申请材料。

3.2.2.1. 机构身份和域名的鉴别

机构订户在申领证书前应持机构有效身份证件，包括但不限于：营业执照、法人代码证、事业单位法人证书、社会团体登记证书、民办非企业登记证书、外国（地区）企业常驻代表机构登记证和政府批文，提出证书申请。

CA 机构或授权的注册机构将确认机构订户是确实存在的、合法的实体及确认申请人的意愿。其鉴别流程方法如下。

(1) 通过权威第三方数据库对有效机构身份证明文件进行核查确认，确保所提供的信息与核查结果一致。

(2) 检查组织机构授权给授权代表办理证书事宜的授权文件及授权代表有效身份证件，确保授权代表得到申请机构的授权。CA 机构可通过鉴证数据源得到的电话号码等方式与申请机构进行联络，以确认申请者某个信息的真实性，如验证申请表中的某个人是否是授权代表。

(3) 通过手机短信、银行打款附言等方式，与证书申请人核实证书请求，确认申请人的真实意愿。

(4) 如果 CA 机构无法从第三方得到所有所需的信息，可委托第三方进行调查或要求申请者提供额外的信息和证明材料。

CA 机构建立和维护证书高风险申请人列表，在收到证书申请时会查询该列表，对于列表中出现的申请人，CA 机构将拒绝其申请。

3.2.2.2. DBA/商业名称的鉴别

若证书主题中包含 DBA 或商业名称，CA 机构或授权的注册机构将通过以下方式中的至少一种确认申请者有权使用该 DBA 或商业名称。

(1) 政府机构提供的可证明申请者合法成立、存在或认可的有效文档。

(2) 可靠的数据来源。（如：邓白氏编码、商务部对外贸易经营者备案）

(3) 其他本 CA 机构认为可靠的验证方式。。

3.2.2.3. 国家的鉴别

若证书主题中包含国家选项，CA 机构或授权的注册机构将通过以下方式中的至少一种进行国家的鉴别。

(1) 通过权威第三方数据库查询网站 DNS 记录显示的 IP 地址或申请者的 IP 地址来确认所在国，确保申请人的 IP 地址所在国与申请人实际所在国一致。

(2) 请求域名的 ccTLD。

(3) 域名注册机构提供的信息。

(4) 通过本 CPS 第 3.2.2.1 节中申请者提供的机构证明信息进行所在国家的确认。

3.2.2.4. 域名的确认和鉴别

对于域名的验证，被验证的实体可以是申请者的母公司、子公司或联营公司，CA 机构或授权的注册机构应当采用以下鉴别方式中的一种，确认申请者拥有该域名。

(1) 参照第 3.2.2.9 节中邮件地址的确认和鉴别方法，通过邮件方式发送随机值，然后接收一个使用该随机值的确认响应，确认申请人对 FQDN 的所有权。随机值必须发送到 WHOIS 注册备案的域名联系人电子邮件地址。（依据 Baseline Requirements v2.1.2 第 3.2.2.4.2 的域名验证方法）。

(2) 参照第 3.2.2.9 节中邮件地址的确认和鉴别方法，通过邮件方式发送随机值，然后接收一个使用该随机值的确认响应，确认申请人对 FQDN 的所有权。随机值必须发送到标识为域名联系人的电子邮件地址或'admin'，'administrator'，'webmaster'，'hostmaster'或'postmaster'，后面是（“@”）之后跟着授权域名。（依据 Baseline Requirements v2.1.2 第 3.2.2.4.4 的域名验证方法）。

(3) 通过在“/.well-known/pki-validation”目录下对约定的文件内容进行验证（包含请求值或随机值的文件），确认订户对 FQDN 的所有权。（依据 Baseline Requirements v2.1.2 第 3.2.2.4.18 的域名验证方法）。

(4) 通过在 DNS CNAME、TXT 或 CAA 记录中是否存在已约定的随机值或请求码，以确认订户对域名的所有权。要求：1）授权域名；或者 2）一个前缀 以下划线字符开头的授权域名。（依据 Baseline Requirements v2.1.2 第 3.2.2.4.7 的域名验证方法）。

上述验证方法中用到的随机值的有效期为从产生该随机值开始的 30 天。本 CA 机构不为.onion 形式的域名签发 SSL 全球服务器证书。

3.2.2.5. IP 地址的确认和鉴别

CA 机构不为 IANA 标注的保留 IP 地址或内部名称签发证书。CA 机构或授权的注册机构应当采用以下鉴别方式中的一种，确认申请者拥有或控制该 IP 地址。

(1) 通过在“/.well-known/pki-validation” 目录下对约定的信息进

行改动，确认订户对 IP 地址的控制权。（依据 Baseline Requirements v2.1.2 第 3.2.2.5.1 的 IP 验证方法）

(2) 参照第 3.2.2.9 节中邮件地址的确认和鉴别方法，通过邮件方式发送随机值，然后接收一个使用该随机值的确认响应，确认申请人对 IP 地址的控制权。（依据 Baseline Requirements v2.1.2 第 3.2.2.5.2 的 IP 验证方法）

(3) 通过 IP 地址上的反向 IP 查找获得与 IP 地址关联的域名，然后使用本 CPS 第 3.2.2.4 节描述的方法验证，确认申请人对 IP 地址的控制权。（依据 Baseline Requirements v2.1.2 第 3.2.2.5.3 的 IP 验证方法）

(4) 通过拨打标识为 IP 联系人的电话号码并获得确认申请人验证 IP 地址请求的响应，确认申请人对 IP 地址的控制权。（依据 Baseline Requirements v2.1.2 第 3.2.2.5.5 的 IP 验证方法）

上述验证方法中用到的随机值的有效期为从产生该随机值开始的 30 天。本 CA 机构不为 IP 地址签发 EV SSL 全球服务器证书。

3.2.2.6. 通配符域名的确认和鉴别

CA 机构应采用本 CP 第 3.2.2.4 节域名验证方法 1、验证方法 2 和验证方法 4 中的一种验证方法，验证确认申请者对通配符右侧域名的所有权和控制权，确保该域名是明确归属于某一商业实体、社会组织或政府机构，并经过合法的注册获得的。

CA 机构拒绝通配符右侧的域名直接是顶级域名、公共后缀或由域名注册管理机构控制的域名的证书申请，除非订户能够证明其完全控制该域名的所有命名空间。

必要时，CA 机构需采取其他独立的审核方法，以确定域名的归属权，如需要订户提供相应的协助，订户不能以任何理由拒绝。

3.2.2.7. 数据源的准确性

CA 机构将 EV 证书鉴证数据源在官方网站上公布，如有需要，请访问 https://www.wotrus.com。

CA 机构在变更证书鉴证数据源之后，应及时披露 EV 证书鉴证数据源的最新版本。

在将任何数据源作为可靠的数据源之前，CA 机构应对该来源的可靠性、准确性及更改或伪造可抗性进行评估，并考虑以下因素：

(1) 所提供信息的年限。

(2) 信息来源的更新频率。

(3) 数据供应商和数据收集的目的。

(4) 数据对公众的可用性及可访问性。

(5) 伪造或改变数据的相对难度。

对于所签发的订户证书，若从评估为可依赖数据来源中获得的数据或文件的时间不超过本 CPS 第 6.3.2 节中约定的证书最大有效期，则本 CA 机构可使用该数据及文件。

3.2.2.8. 认证机构授权（CAA）

本 CA 机构在签发 SSL 证书之前，将对待签发证书主题别名扩展项中的每一个 dNSName 做 CAA 记录检查。CA 机构将在查询 CAA 记录的有效期（有效期以 CAA 记录的生存时间或 8 小时的较大值为准）内，向证书申请者发放证书。若超过 CAA 记录的有效期，CA 机构将重新进行 CAA 检查。

CA 机构根据 RFC8659 的规定处理“issue”、“issuewild”及“iodef”的属性标签：若“issue”、“issuewild”标签存在并且其中不包含“wotrus.com”，则 CA 机构不签发对应的证书；若 CAA 记录中出现“iodef”标签，则 CA 机构与申请者沟通后决定是否为其颁发证书。

CA 机构以下列 CAA 记录查找失败情况作为可签发证书的条件：

(1) 在非沃通公司的基础设施中查询 CAA 记录失败；

(2) 至少尝试过一次重新查找 CAA 记录；

(3) 域名所在区域不存在指向 ICANN 根区域的 DNSSEC 验证链。

3.2.2.9. 邮件地址的确认和鉴别

CA 机构或授权的注册机构将对申请者邮件地址的有效性和控制权进行鉴别。

其鉴别流程方法如下。

(1) CA 机构向该邮件地址发送随机值，随机值由系统产生，并且唯一。

(2) 申请者收到邮件并回复该随机值进行确认。

(3) CA 机构收到回复，并将回复中的随机值与发送的随机值进行比对，若结果一致，则邮件地址鉴别通过。

上述鉴别方法中用到的随机值的有效期为从产生该随机值开始的 24 小时内。

3.2.2.10. DV SSL 全球服务器证书订户身份鉴别

个人订户、机构订户如需要申请 DV SSL 全球服务器证书，可以向 CA 机构或授权的注册机构提交申请。DV SSL 全球服务器证书可包含 IP 地址、通配符证书。订户申请 DV SSL 全球服务器证书时，应提交如下材料：

(1) 拥有域名的证明；

(2) 拥有公网 IP 的证明（域名型不适用）；

(3) 证书申请 CSR 文件。

CA 机构要对域名（IP）及 CSR 合规性进行鉴别。其鉴别流程方法如下。

(1) 通过域名注册信息查询（WHOIS）功能，得到所申请域名证书的域名注册者资料，查看域名注册者是否和域名证书申请者一致，初步审核确定域名证书申请者确实拥有此域名。如域名申请者与在（WHOIS）查询到的结果

不一致，则订户可提供授权证明或者 CA 机构采取邮件方式询问是否授权给证书申请者使用。

(2) 按照本 CPS 第 3.2.2.4 节域名鉴别方法，确认申请者对域名的所有权。

(3) 按照本 CPS 第 3.2.2.5 节 IP 地址鉴别方法，确认申请者对 IP 地址的所 有权或控制权。

(4) 如果申请通配符域名证书，按照本 CPS 第 3.2.2.6 节进行通配符域名鉴别。

(5) 对于 CSR 文件的鉴别主要包含，CSR 中的信息是否与申请表中的申请信息一致，是否符合相关规范，比如 DN 的顺序等，并验证其是否拥有私钥。

(6) 按照本 CPS 第 3.2.2.8 节的要求检查 CAA 记录。CA 机构要对域名（IP）及 CSR 合规性进行鉴别。相应的鉴别流程应当明确记录在按照本 CP 制定的 CPS 中。

3.2.2.11. OV SSL 全球服务器证书订户身份鉴别

机构订户如需要申请 OV SSL 全球服务器证书，可以向 CA 机构或授权的注册机构提交申请。OV SSL 全球服务器证书可包含通配符、IP 地址或多域名证书。订户申请 OV SSL 全球服务器证书时，应提交如下材料：

(1) 证书申请表；

(2) 至少一种机构信息证明材料；

(3) 申请人的个人身份证明材料；

(4) 机构授予申请人的授权证明；

(5) 拥有域名的证明；

(6) 拥有公网 IP 的证明（域名型不适用）；

(7) 证书申请 CSR 文件。

CA 机构除对订户身份进行鉴别外，还要对域名（IP）及 CSR 合规性进行鉴别。其鉴别流程方法如下。

(1) 按照本 CPS 第 3.2.2.1 节的要求鉴别订户机构身份。

(2) 通过域名注册信息查询（WHOIS）功能，得到所申请域名证书的域名注 册者资料，查看域名注册者是否和域名证书申请者一致，初步审核确定域名证书申请者确实拥有此域名。如域名申请者与在（WHOIS）查询到的结果不一致， 则订户可提供授权证明或者 CA 机构采取邮件方式询问是否授权给证书申请者使用。

(3) 按照本 CPS 第 3.2.2.4 节域名鉴别方法，确认申请者对域名的所有权。

(4) 按照本 CPS 第 3.2.2.5 节 IP 地址鉴别方法，确认申请者对 IP 地址

的所有权或控制权。

(5) 如果申请通配符域名证书，按照本 CPS 第 3.2.2.6 节进行通配符域名鉴别。

(6) 对于 CSR 文件的鉴别主要包含，CSR 中的信息是否与申请表中的申请信息一致，是否符合相关规范，比如 DN 的顺序等，并验证其是否拥有私钥。

(7) 按照本 CPS 第 3.2.2.8 节的要求检查 CAA 记录。

3.2.2.12. EV SSL 全球服务器证书订户身份鉴别

机构订户如需要申请 EV SSL 全球服务器证书，可以向 CA 机构或授权的注册机构提交申请。EV SSL 全球服务器证书申请，只能是 WEB 服务器的域名，并且域名不能包含通配符，不受理 IP 地址的申请，EV SSL 全球服务器证书可包含多域名证书。申请者只能是国家机关、企事业单位、社会团体等机构订户。且申请机构需要满足如下条件：

1. 国家机关应满足如下条件：

(1) 经由上级按照其职能批准建立；

(2) 在订户申请材料中必须明确单位的授权代表；

(3) 所在国家允许 CA 签发证书；

(4) 不在中国政府拒绝名单或禁止名单（如贸易禁运）中。

2. 企事业单位应满足如下条件：

(1) 获得当地监管机构承认的合法组织；

(2) 不在监管机构的“停业”、“无效”、“过期”名单之列；

(3) 在订户申请材料中必须明确单位的授权代表；

(4) 拥有固定的营业场所；

(5) 机构和授权代表所在国家允许 CA 签发证书；

(6) 机构和授权代表不在中国政府拒绝名单或禁止名单（如贸易禁运）中。

3. 社会团体应满足如下条件：

(1) 获得当地监管机构承认的合法组织；

(2) 不在监管机构的“停业”、“无效”、“过期”名单之列；

(3) 在订户申请材料中必须明确单位的授权代表；

(4) 拥有固定的营业场所；

(5) 所在国家允许 CA 签发证书；

(6) 不在中国政府拒绝名单或禁止名单（如贸易禁运） 中。

4. 申请机构应拥有的角色：

(1) 申请人：申请单位经办人员；

(2) 审批人：申请单位主管人员签署人；

(3) 申请代理人：在 CA 与申请者是关联方，且双方有适用于 EV 证书使用准则的情况下，申请者需设定申请代理人，代表申请者认可证书的使用准则。

证书申请机构可授权一个人来完成所有的角色，也可分别多人来完成。以上角色必须是申请单位的职员或被授权的代理人，申请单位需确认申请角色的信息真实准确并以 CA 机构认可的方式（包括但不限于注册公章、注册法人人名章、角色签名等方式）对证书申请及订户协议进行签名，对于不实的申请角色信息，CA 机构有权拒绝申请，并对已发放的证书进行撤销。

5. 申请机构的域名：

(1) 申请机构拥有域名所有权或唯一使用权且意识到其对域名拥有所有权或唯一使用权；

(2) 域名注册信息应公开在 WHOIS 数据库。

6. 订户申请 EV SSL 全球服务器证书时，应提交如下资料：

(1) EV 证书申请表；

(2) 至少一种机构信息证明材料；

(3) 至少两种申请人的身份证明材料；

(4) 机构授予申请人的授权证明；

(5) 企业存在证明文件；

(6) 拥有域名的证明；

(7) 证书申请 CSR 文件。

CA 机构对 EV SSL 证书申请的鉴别过程如下：

1. 订户身份鉴别

(1)验证申请机构的身份合法性

通过 EV 证书鉴证数据源查询申请机构注册编码（如统一社会信用代码）真伪； 验证申请机构身份信息及注册地址；

必须直接通过合格的独立信息来源进行验证。

(2)对机构验证的内容

申请机构身份信息是否存在；

申请机构身份信息是否准确；

申请机构提供的经营地址是否与注册文件（如：营业执照）中登记的注册地址一致。

(3)验证申请机构的存续状态

通过 EV 证书鉴证数据源查询申请机构注册编码（如统一社会信用代码），验证其是否正常存续或查询申请机构提供的银行验资报告验证机构存续状态。

(4)对 EV 证书申请相关人员的身份验证

EV 证书申请人（个体工商户申请 EV 证书时，证书申请人需是经营者本人）必须经过面对面（视频）的方法进行验证；

通过公安部身份核验平台验证身份信息；

通过拨打固定电话（必须是通过鉴证数据源得到的公司电话）与申请机构人事部门联系，确认申请人、审批人、签署人的人员身份及授权。

2. 域名鉴别

按照本 CPS 第 3.2.2.4 节域名鉴别方法，确认申请者对域名的所有权。

3. CSR 文件鉴别

对订户提交的 CSR 文件内容进行验证， 检查 CSR 中的信息是否与申请表中的信息一致，是否符合相关规范，并验证其是否拥有私钥。

4. EV SSL 全球服务器证书公钥证书分发

关于 EV SSL 全球服务器证书的分发控制，CA 机构为订户签发公钥证书，并通过安全通道（如：邮件方式）将签发的公钥证书交付给订户。

3.2.2.13. 时间戳证书订户身份鉴别

机构订户如需要申请时间戳证书，可以向 CA 机构或授权的注册机构提交申请。订户申请时间戳证书时，应提交如下材料：

(1) 证书申请表；

(2) 至少一种机构信息证明材料；

(3) 申请人的个人身份证明材料；

(4) 机构授予申请人的授权证明。

CA 机构除对订户身份进行鉴别外，还要对 CSR 合规性进行鉴别。其鉴别流程方法如下。

（1）按照本 CPS 第 3.2.2.1 节的要求鉴别订户机构身份。

（2)对于 CSR 文件的鉴别主要包含:CSR 中的信息是否与申请表中的申请 信息一致，如 CSR 申请信息与申请表中的不一致，则以申请表为准；是否符合相关规范，比如 DN 的顺序等；验证其是否拥有私钥。

3.2.3. 个人身份的鉴别

个人订户或机构订户申请人在申领证书前应持个人有效身份证件，包括但不限于：身份证、户口簿、军官证、港澳居民来往内地通行证、台胞证、护照和外国人永久居留证等，提出证书申请。

CA 机构或授权的注册机构将确认个人身份的真实性和有效性。其鉴别流程方法如下。

（1）通过权威第三方数据库对有效身份证明文件进行核查确认，确保所提供的信息与核查结果一致。

（2）通过手机短信、银行打款附言等方式，与个人订户核实证书请求。必要时可通过语音、视频、拍照、面对面等方式对个人订户的身份进行确认。

（3）当申请信息包含机构信息时，需要确认该机构是否存在，以及申请人是否属于该机构的成员。

（4）在域名、设备名称或者邮件地址被作为证书主题内容申请证书时，还需要验证该个人申请者是否拥有该权利，例如要求提交域名所有权文件、归属权证明文件或者申请者对所有权的书面承诺等。

CA 机构建立和维护证书高风险申请人列表，在收到证书申请时会查询该列表，对于列表中出现的申请人，CA 机构将拒绝其申请。

3.2.4. 没有验证的订户信息

若订户提交鉴证文件不属于鉴别范围内的信息，为没有验证的订户信息。证书中的信息必须经过验证，未经验证的信息不得写入证书。

3.2.5. 授权的确认

为确保办理人具有特定的许可，代表组织获取数字证书，需要出具组织授权

其代表该组织为办理 CA 数字证书事宜的授权文件。组织在 CA 机构的数字证书申请表上加盖单位公章后，则证明本组织对办理人的授权确认。

本 CA 机构允许申请者指定独立个人来申请证书。若申请者以书面形式指定了可以进行证书申请的独立个人，则不接受在该指定人员以外的任何证书申请请求。在收到申请者已核实的书面请求时，应向申请者提供其已授权人员的清单。

3.2.6. 互操作准则

本 CA 机构可以与其他电子认证服务机构进行互操作，要求该电子认证服务机构的 CP 及 CPS 必须符合《沃通电子认证服务有限公司 SM2 全球信任体系证书策略（CP3）》的要求，并与沃通公司签署相关协议。

如果国家法律法规对其有要求，沃通公司将严格遵守。

截止目前，本 CA 机构未签发任何交叉认证的证书。

3.3. 密钥更新请求的身份标识与鉴别

3.3.1. 常规密钥更新的标识与鉴别

对于密钥更新申请，订户须提交能够识别原证书的足够信息，如订户甄别名、证书序列号等，对申请的鉴别基于：

(1) 原证书存在并由 CA 机构签发；

(2) 用原证书上的订户公钥对申请的签名进行验证；

(3) 基于原注册信息进行身份鉴别。

密钥更新会造成使用原密钥对加密的文件或数据无法解密，订户在申请密钥更新前，须确认使用原密钥对加密的文件或数据已解密，由此造成的损失，CA 机构将不承担责任。

3.3.2. 撤销后密钥更新的标识与鉴别

证书撤销后的密钥更新等同于订户重新申请证书，则撤销后密钥更新的标识与鉴别使用初始身份确认相同的流程，其要求与本 CPS 第 3.2 节相同。

3.4. 撤销请求的标识与鉴别

若订户主动申请撤销证书，则撤销请求的标识与鉴别使用初始身份确认相同的流程，其要求与本 CPS 第 3.2 节相同。

若因订户未履行本 CPS 所规定的义务或由于本 CPS 第 4.9.1.1 节所述理由，由本 CA 机构或授权的注册机构申请撤销订户的证书时，无需对订户身份进行标识和鉴别。

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

证书申请实体包括个人、组织或其他实体。

4.1.2. 申请过程与责任

证书申请人按照本 CPS 所规定的要求，通过现场面对面或在线方式提交证书

申请，包括相关的身份证明材料。CA 机构或注册机构受理证书申请，依据身份鉴别规范对证书申请人的身份进行鉴别，并决定是否签发证书。

订户：订户应事先对订户协议、本 CPS 及相关 CP 所规定的责任和义务进行了解，并确认接受。正式发起注册请求，则订户需要提供本 CPS 第 3.2 节所述的证书申请表、相应证明文件及证书请求文件等，并确保材料真实准确。应配合 CA 机构或授权的注册机构完成对身份信息的采集、记录和审核。注册成功后，订户有责任保护其所获得的证书私钥的安全。

根据《中华人民共和国电子签名法》的规定，证书申请人未向 CA 机构提供真实、完整和准确的信息，或者有其他过错，给 CA 机构或电子签名依赖方造成损失的，应承担相应的法律责任和经济赔偿。

CA 机构：CA 机构录入员、审核员参照本 CPS 第 3.2 节及第 5.2.4 节的要求对订户的身份信息进行采集、记录，审核。通过录入员、审核员两个可信人员的鉴证审批后，CA 机构向订户签发证书。

4.2. 证书申请处理

4.2.1. 执行识别与鉴别功能

CA 机构或授权的注册机构接收到订户的证书申请后，按照本 CPS 所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见本 CPS 第 3.2 节初始身份确认。

CA 机构会对待签发的全球服务器证书主题别名扩展项中的每一个 dNSName

做 CAA 记录检查，并按照本 CPS 第 3.2.2.8 中的检查方法和结果判定是否批准该证书申请。在全球服务器证书签发前，若 CA 机构根据本 CP 第 3.2 节获得的数据或证明文件的时间不超过本 CPS 第 6.3.2 节中约定的服务器证书最大有效期，且该信息未发生变化，则 CA 机构可重用该数据或证明文件，对订户身份进行识别与鉴别。

4.2.2. 证书申请批准和拒绝

CA 机构或授权的注册机构根据本 CPS 所规定的身份鉴别流程对证书申请人身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

如果证书申请人通过本 CPS 所规定的身份鉴别流程且鉴证结果为合格，CA 机构或授权的注册机构将批准证书申请，为证书申请人制作并颁发数字证书。

如果发生下列情形，CA 机构有权拒绝证书申请：

(1) 根据本 CPS 第 3.2 节的规定，不能完成识别和认证所有必需的订户信息；

(2) 订户不能根据要求提供所需要的身份证明材料；

(3) 订户反对或者不能接受订户协议的有关内容和要求；

(4) 订户没有或者不能够按照规定支付相应的费用；

(5) 申请的证书含有 ICANN 考虑中的新顶级域名；

(6) CA 机构认为批准该申请将会对沃通公司带来争议、法律纠纷或者损失。

对于拒绝的证书申请，CA 机构通知申请人证书申请失败，同时告知申请人失败的原因（法律禁止的除外）。

CA 机构应根据反钓鱼联盟、防病毒厂商或相关联盟、负责网络安全事务的政府机构等第三方发布的名单，或公共媒体公开报道中披露的信息，建立和维护证书高风险申请人列表，在收到证书申请时应查询该列表，对于列表中出现的申请人，CA 机构将拒绝其申请。对于已签发的证书，会定期根据列表予以复核，一旦发现证书持有人出现在列表中，CA 机构有权撤销该证书或采取适当机制进行处理。

对于法律法规、国家政府部门、行业监管部门或当地政府明确禁止从事商业活动或其它公开活动的机构，CA 机构有权拒绝为其签发证书。此外，如果证书申请相关人员（包括申请人、审批人、签署人等）受到法律法规、国家或地方政府的相关限制，CA 机构拒绝受理由其参与的证书申请事宜。

4.2.3. 处理证书申请的时间

CA 机构或授权的注册机构将做出合理努力来尽快确认证书申请信息，一旦注册机构收到了所有必须的相关信息，将在下一个工作日内受理，并在 3-5 个工作日完成审核与证书签发。

CA 机构或授权的注册机构能否在上述时间期限内处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了 CA 的管理

要求。

4.3. 证书签发

4.3.1. 证书签发中电子认证服务机构和注册机构的行为

根 CA 的证书签发由本 CA 机构授权的可信人员谨慎地发布直接指令，使根 CA 执行证书签名操作。

在订户证书的签发过程中，CA 机构的录入员负责录入证书申请者提交的信息，审核员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 的证书签发系统。RA 发出的证书签发请求信息需有注册机构的身份鉴别与信息保密措施，并确保请求发到正确的 CA 机构。

CA 机构在获得证书签发请求后，判断证书签发请求的有效性，在批准证书申请之后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

4.3.2. 电子认证服务机构和注册机构对订户的通知

CA 机构通过注册机构告知证书订户证书的签发结果和获取证书的方式，可通过面对面、电子邮件、网络下载，或 CA 机构认为其他安全可行的方式告知订户。

4.4. 证书接受

4.4.1. 构成接受证书的行为

证书签发完成后，订户通过 CA 机构所通告的方式获取证书，在订户发生以

下任意一种行为后，CA 机构认为订户接受了证书：

(1) 订户下载或安装了证书；

(2) 本 CA 机构在订户的允许下，代替订户下载证书，并把证书通过面对面、电子邮件或其他安全可行的方式发送给订户；

(3) 在本 CA 机构将证书获取通知发送给订户后，在约定的时间内订户未表示拒绝。

4.4.2. 电子认证服务机构对证书的发布

CA 机构在签发证书后，将证书发给订户视为证书的发布。

4.4.3. 电子认证服务机构对其他实体的通告

CA 机构不对其他实体进行通告，其他实体可以在信息库上自行查询。

4.5. 密钥对和证书使用

4.5.1. 订户私钥和证书使用

订户在提交了证书申请并接受了 CA 机构所签发的证书后，均视为已经同意遵守与 CA 机构、依赖方有关的权利和义务的条款。

订户只能在适用的法律、本 CPS 以及订户协议指定的应用范围内使用私钥和证书，并且在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

对于 SSL/TLS 证书，订户有责任和义务保证只在证书列出的主题别名对应的

服务器中部署证书。

4.5.2. 依赖方公钥和证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了解对方的身份，并通过公钥验证对方电子签名的真实性。在验证电子签名的真实性时，依赖方应准确知道被签名的数据内容。

依赖方应验证证书的有效性，包括：

(1) 用 CA 机构的证书验证证书中的签名，确认该证书是依赖方所信任的 CA 机构签发的，并且证书的内容没有被篡改；

(2) 检验证书的有效期，确认该证书在有效期之内；

(3) 通过查询 CRL 或 OCSP，确认该证书没有被注销。

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示被签名的数据。

4.6. 证书更新

4.6.1. 证书更新的情形

证书更新指在不改变证书中订户的公钥或其他任何信息的情况下，为订户签发一张新证书。本 CA 机构推荐订户优先选用证书密钥更新服务，详见本 CPS 第 4.7 节。

订户需在证书到期前 30 天进行证书更新。证书过期后，订户必须重新申请新证书。

本 CA 机构支持为 SSL 全球服务器证书、时间戳证书提供证书更新服务。

4.6.2. 请求证书更新的实体

请求证书更新的实体为证书订户。

4.6.3. 证书更新请求的处理

证书更新请求的处理过程包括申请验证、鉴别、签发证书。对申请的验证和鉴别须基于以下几个方面：

(1) 订户的原证书存在并且由本 CA 机构签发；

(2) 证书更新请求在许可期限内；

(3) 基于原注册信息进行身份鉴别；

(4) 若 CA 机构根据本 CPS 第 3.2 节获得的数据或证明文件的时间不超过本 CPS 第 6.3.2 节中约定的此类证书的最大有效期且该信息未发生变化，则 CA 机构可重用该数据或证明文件，对订户身份进行识别与鉴别。

在以上验证和鉴别通过后 CA 机构才可批准签发证书。

在证书更新时，订户可以用原有的私钥对更新请求进行签名，CA 机构将会对用户的签名和公钥、更新请求内包含的用户信息进行正确性、合法性和唯一性的

验证和鉴别。

订户也可以选择按照本 CPS 第 3.2 节的要求进行证书更新申请操作，重新提交身份证明材料，CA 机构在任何情况下都可将这种初始证书申请的鉴别方式作为证书更新时的鉴别处理手段。

4.6.4. 颁发新证书时对订户的通告

同本 CPS 第 4.3.2 节。

4.6.5. 构成接受更新证书的行为

同本 CPS 第 4.4.1 节。

4.6.6. 电子认证服务机构对更新证书的发布

同本 CPS 第 4.4.2 节。

4.6.7. 电子认证服务机构对其他实体的通告

同本 CPS 第 4.4.3 节。

4.7. 证书密钥更新

4.7.1. 证书密钥更新的情形

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书，CA 机构提供证书更新时，密钥必须同时更新。

若 CA 机构根据本 CPS 第 3.2 节指定来源获得的数据或证明文件的时间不超

过本 CPS 第 6.3.2 节中约定的此类证书的最大有效期且该信息未发生变化，则 CA 机构可以重用这些此前已验证的信息。此时，订户在申请证书密钥更新时无需再次提交证书申请所需材料，仅提交协助识别原证书的相应信息即可，如证书序列号、订户甄别名等，以及采用原证书对应私钥对证书密钥更新请求进行签名以便 CA 机构验证。

证书密钥更新的具体情形如下：

(1) 当订户证书即将到期时；

(2) 当订户证书私钥泄露而撤销证书时；

(3) 当订户证实或怀疑其证书密钥不安全时；

(4) 其它可能导致密钥更新的情形。

CA 机构支持为本 CPS 中的所有证书提供证书密钥更新服务。

4.7.2. 请求证书密钥更新的实体

请求证书密钥更新的实体为证书订户。

4.7.3. 证书密钥更新请求的处理

同本 CPS 第 3.3 节。

4.7.4. 颁发新证书时对订户的通告

同本 CPS 第 4.3.2 节。

4.7.5. 构成接受密钥更新证书的行为

同本 CPS 第 4.4.1 节。

4.7.6. 电子认证服务机构对密钥更新证书的发布

同本 CPS 第 4.4.2 节。

4.7.7. 电子认证服务机构对其他实体的通告

同本 CPS 第 4.4.3 节。

4.8. 证书变更

4.8.1. 证书变更的情形

如订户提供的注册信息发生改变，必须向 CA 机构提出证书变更。证书变更的申请和证书申请所需的流程、条件一致。

4.8.2. 请求证书变更的实体

请求证书变更的实体为证书订户。

4.8.3. 证书变更请求的处理

证书变更按照初次申请证书的注册过程进行处理。

4.8.4. 颁发新证书时对订户的通告

同本 CPS 第 4.3.2 节。

4.8.5. 构成接受变更证书的行为

同本 CPS 第 4.4.1 节。

4.8.6. 电子认证服务机构对变更证书的发布

同本 CPS 第 4.4.2 节。

4.8.7. 电子认证服务机构对其他实体的通告

同本 CPS 第 4.4.3 节。

4.9. 证书撤销和挂起

4.9.1. 证书撤销的情形

4.9.1.1. 撤销订户证书的原因

如果出现下列任何一种或多种情况，CA 机构应在 24 小时内撤销该订户证书：

(1) 订户以书面形式申请撤销数字证书；

(2) 订户认为原始证书请求未经授权，且不能追溯授权行为；

(3) CA 机构有证据证明，与订户证书中的公钥对应的私钥已泄露；

(4) CA 机构获知已出现了经过验证的订户私钥泄露方法，该方法可基于公钥很容易地计算出订户私钥（例如：Debian 弱密钥，请参阅 http://wiki.debian.org/SSLkeys）；

(5) CA 机构获得证据，证书中所包含的域名或 IP 地址的控制权验证已

不再可靠；

(6) CA 机构收到通知或以其他方式得知任何表明订户不再合法使用证书中电子邮件地址的情况；

(7) 其他 CA 机构认为应当撤销证书的情形。

如果出现下列任何一种或多种情况，CA 机构宜在 24 小时之内撤销证书，且必须在 5 天之内撤销证书：

(1) 证书不再符合本 CPS 第 6.1.5 和 6.1.6 节的要求；

(2) CA 机构掌握了证书被滥用的证据；

(3) CA 机构获知订户未履行订户协议、使用条款中规定的一项或多项重要义务或责任；

(4) CA 机构获知法律上不再认可该订户证书中使用的 FQDN 或 IP 地址。如，法院或仲裁机构已撤销域名注册人使用域名的权利、域名注册人与申请人之间的相关许可或服务协议已终止或域名注册人未能续订域名等；

(5) CA 机构获知订户的通配符证书已被用于验证欺诈性的下级域名；

(6) CA 机构获知证书中包含的信息发生了重大变化；

(7) CA 机构获知订户证书的签发未遵循 CP/CPS 的相关要求；

(8) CA 机构确定或获知订户证书中包含了不准确或错误的信息；

(9) 当 CA 机构从事电子认证业务的资格被撤销后，除继续维持 CRL/OCSP 信息库的外，应撤销所有已签发的证书；

(10) 当出现 CA 机构 CP/CPS 要求撤销证书的情形；

(11) CA 机构获知已出现了经过验证的订户私钥泄露方法，或者有明确证据表明用于生成私钥的具体方法存在缺陷；

(12) 当 CA 机构因某种原因终止电子认证服务，且未安排其他 CA 机构支持完成撤销证书的操作；

(13) 订户被列入任何第三方钓鱼网站联盟、信用监管机构的黑名单中，或 CA 机构所在国家的监管机构禁止在订户经营所在地开展服务；

(14) CA 机构履行证书服务费用催缴义务后，订户仍未缴纳；

(15) 法律、行政法规规定的其他情形。

4.9.1.2. 撤销中级 CA 证书的原因

如果出现下列任何一种或多种情况，CA 机构在 7 天内撤销中级 CA 证书：

(1) CA 机构以书面形式申请撤销中级 CA 证书；

(2) CA 机构认为中级 CA 证书请求未经授权，且不能追溯授权行为；

(3) CA 机构有证据证明与证书中的公钥对应的中级 CA 的私钥已泄露，或不 再符合本 CP 第 6.1.5 和 6.1.6 节的要求；

(4) CA 机构有证据证明证书被滥用；

(5) CA 机构获知证书的签发未遵循 CP/CPS 的相关要求；

(6) CA 机构确定了证书中包含有不准确或具有误导性的信息；

(7) CA 机构或中级 CA 因任何原因停止运营，并未安排其他 CA 机构提供撤销证书的支持；

(8) 当出现 CA 机构 CP/CPS 要求撤销证书的情形。

4.9.2. 请求证书撤销的实体

根据不同的情况，订户、CA 机构、注册机构可以发起撤销证书的请求。

此外，订户、依赖方、应用软件供应商和其他第三方均可提交证书问题报告，告知 CA 机构申请撤销证书的合理原因。

4.9.3. 撤销请求的流程

4.9.3.1. 订户主动提出撤销申请

(1) 证书撤销的申请人向 CA 机构或授权的注册机构提交《证书撤销申请表》，并注明撤销原因；

(2) CA 机构或授权的注册机构根据本 CPS 第 3.4 节的要求对订户提交的撤销请求进行鉴别； 如鉴证通过则进行撤销处理；

(3) CA 机构执行撤销操作，订户证书撤销后，注册机构将通过电话、邮

件等方式通知订户证书被撤销及被撤销的理由；若未能联络到订户，在必要的情况下，CA 机构对撤销的证书将通过网站进行公告；

(4) CA 机构提供 7X24 小时的证书撤销申请服务,订户可通过发邮件至：casupport@wotrus.com 或致电：+86-755-86008688。

CA 机构收到申请后 24 小时内处理撤销申请。

4.9.3.2. 订户被强制撤销证书

(1) 当 CA 机构有充分的理由确信出现本 CP 第 4.9.1.1 节中会导致订户证书被强制撤销的情形时，CA 机构将通过内部流程申请撤销证书；

(2) 在证书撤销后，CA 机构将通过适当的方式，包括邮件、电话等，通知最终订户证书已被撤销及被撤销的理由；若未能联络订户时，在必要的情况下，CA 机构对撤销的证书将通过网站进行公告；

(3) CA 机构提供 7X24 小时的证书问题报告和处理流程；

(4) 当依赖方如司法机构、应用软件提供商、防病毒机构等第三方发现证书可能存在问题，如证书滥用、私钥出现或怀疑出现泄漏、证书被用于可疑代码签名等，可及时通过发邮件至：casupport@wotrus.com 或致电：+86-755-86008688 的方式进行问题报告；

CA 机构收到报告后，在 24 小时内对该证书问题报告内容进行调查，并基于以下标准来决定是否撤销证书：

(1) 所报告问题的性质；

(2) 相应问题的出现次数和频率；

(3) 问题报告或投诉的实体；

(4) 订户对本 CA 机构 CP/CPS 和订户协议等相关规范的遵循情况；

(5) 现行法律法规的遵循。

4.9.3.3. 电子认证服务机构本身证书的撤销

对于沃通公司的根证书和中级 CA 证书，沃通公司根据本 CPS 的规定决定是否撤销证书。

4.9.4. 撤销请求宽限期

如果出现私钥泄露等事件，撤销请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他撤销原因的撤销请求必须在 48 小时内提出。

4.9.5. 电子认证服务机构处理撤销请求的时限

CA 机构接到撤销请求后将立即处理，调查与证书问题报告或证书撤销请求相关的事实和情况。CA 机构处理撤销请求的周期为 24 小时。

4.9.6. 依赖方检查证书撤销的要求

CA 机构每 24 小时签发一次 CRL，并将最新的 CRL 发布到目录服务器指定的位置，供请求者查询下载。

CRL 的结构如下：

(1) 版本号

(2) 签名算法

(3) 颁发者名称

(4) 本次更新时间

(5) 下次更新时间

(6) 被撤销的证书列表

(7) 颁发机构密钥标识符

(8) 证书撤销列表号

在信任和使用证书前，依赖方必须使用以下两种功能之一进行所依赖证书的状态查询：

(1) CRL 查询：利用证书中标识的 CRL 地址，通过 CRL 信息库查询并下载 CRL 到本地，进行证书状态的检验。

(2) 在线证书状态查询（OCSP）：CA 机构提供 Get 和 Post 两种方式的 OCSP 查询服务，查询结果经过签名后，返回给请求者。

注意： 依赖方要验证 CRL 的可靠性和完整性，确保是经 CA 机构发布并且签

名的。

4.9.7. CRL 发布频率

CA 机构可采用实时或定期的方式发布 CRL。

发布 CRL 的频率根据证书策略确定，订户证书一般为 24 小时定期发布 CRL，并且订户 CRL 的有效期为 5 天。中级 CA 证书一般为每 12 个月定期发布 CRL，并且中级根 CRL 的有效期为 12 个月。在撤销中级 CA 证书后，将在 24 小时内更新 CRL。

4.9.8. CRL 发布的最大滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.9.9. 在线状态查询的可用性

CA 机构向订户和依赖方提供在线证书状态查询服务（OCSP），OCSP 响应符合 RFC6960 的要求，且将由审核其证书撤销状态的 CA 机构和 OCSP 响应器进行签名。

OCSP 响应器使用的签名证书服务器的证书与正在查询状态的证书由同一个 CA 签发，并且包含 RFC6960 所定义的类型为 id-pkix-ocsp-nocheck 的扩展项。

4.9.10. 在线状态查询要求

CA 机构提供 Get 和 Post 两种方式的 OCSP 查询服务。

对于订户证书，CA 机构至少每四天更新一次 OCSP 信息。OCSP 响应的最长有

效期为 10 天。对于已经撤销的证书，立即更新 OCSP。

对于中级 CA 证书，CA 机构至少每 12 个月更新一次 OCSP 信息。撤销中级 CA 证书后 24 小时内更新。

针对尚未签发的证书的在线证书状态查询请求，OCSP 响应不返回“good”状态。

4.9.11. 撤销信息的其他发布形式

证书撤销信息可以通过 CRL 或者 OCSP 服务获得。CA 机构不提供证书撤销信息的其他发布形式。

4.9.12. 密钥损害的特别要求

除本 CPS 第 4.9.1 节中规定的情况外，当订户发现或有充分证据证明其密钥受到损害时，应主动及时向 CA 机构提出证书撤销请求。

当各相关方发现私钥泄漏时，可通过本 CPS 第 4.9.3.2 节的规定向 CA 机构提交证书问题报告，使用以下方法中的一种来证明私钥泄露：

1. 提交由私钥签名并可通过公钥验证的签名文件；

2. 提交包含泄露私钥的二进制文件，包括提取私钥的方法。

若新的用于证明私钥泄露的方法被采用，CA 机构将更新 CPS。

4.9.13. 证书挂起的情形

不适用。

4.9.14. 请求证书挂起的实体

不适用。

4.9.15. 挂起请求的流程

不适用。

4.9.16. 挂起的期限限制

不适用。

4.10. 证书状态服务

4.10.1. 操作特征

证书状态可以通过 CA 机构提供的 CRL、OCSP 服务查询。

对于被撤销的证书，CA 机构不删除其在 CRL 中的撤销记录。

CA 机构不删除 OCSP 服务器中的撤销记录。

4.10.2. 服务可用性

CA 机构提供 7X24 小时的证书状态查询服务，查询响应时间不超过 10 秒。即在网络允许的情况下，订户能够实时获得证书状态查询服务。

4.10.3. 可选特征

根据请求者的要求，在请求者支付相关费用后，CA 机构可以提供通知服务，当指定的证书被撤销时，CA 机构将通知该项服务的请求者。

4.11. 订购结束

订购结束是指当证书有效期满或证书撤销后，该证书的服务时间结束。

订购结束包含以下两种情况：

(1) 证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订户可以终止订购；

(2) 在证书有效期内，证书被撤销后，即订购结束。

4.12. 密钥托管和恢复

4.12.1. 密钥托管和恢复政策及行为

本信任体系无密钥托管和恢复业务。为了保证订户签名私钥的安全性和唯一性，建议订户自己生成密钥并进行备份，在密钥丢失后进行恢复。

4.12.2. 会话密钥的封装与恢复的策略与行为

不适用。

5. 电子认证服务机构设施、管理和操作控制

5.1. 物理控制

5.1.1. 场地位置与建筑

CA 机房的建筑物和机房建设严格按照下列标准设计与实施：

(1) GB/T 25056-2010《信息安全技术 证书认证系统密码及其相关安全技术规范》

(2) GB 50174-2008：《电子计算机机房设计规范》

(3) GB 2887-2011：《计算站场地技术条件》

(4) GB 9361-88：《计算站场地安全要求》

(5) GB 6650-1986：《计算机机房用活动地板技术条件》

(6) GB50116-98：《火灾自动报警系统设计规范》

(7) GB 50034-1992：《工业企业照明设计标准》

(8) GB 5054-95：《低压配电装置及线路设计规范》

(9) GBJ 19-87：《采暖通风与空气调节设计规范》

(10) GB50057-2010：《建筑物防雷设计规范》

(11) GBJ 79-85：《工业企业通信接地设计规范》

CA 机房实行分层访问的安全管理，功能区域划分为“六个层次，四个区域”。

(1) 六个层次由外到里分别是：入口、办公、管理、数据中心、屏蔽机房、保密机柜。

(2) 四个区域由外到里分别是：公共区域、DMZ 区域（非军事区）、操作区域和安全区域。

其中，入口之外的区域为公共区域，入口和办公层位于 DMZ 区，敏感层位于操作区，其他各层位于安全区。

5.1.2. 物理访问控制

为了保证本系统的安全，采取了一定的隔离、控制、监控手段。机房的所有门都足够结实，能防止非法进入。机房通过设置门禁和侵入报警系统来重点保护机房物理安全。

物理访问控制包括如下几个方面：

1） 门禁系统： 控制各层门的进出。工作人员需使用身份识别卡结合指纹鉴定才能进出，进出每一道门应有时间纪录和信息提示。

2） 报警系统：当发生任何非法闯入、非正常手段的开门等异常情况都应触发报警系统。报警系统明确指出报警位置。

3） 监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对安全区域和操作区域进行 24 小时不间断录像。所有录像资料需要保留不少于 6

个月，以备查询。

门禁和物理侵入报警系统备有 UPS，并提供至少 8 小时的不间断供电。

5.1.3. 电力与空调

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统，按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供配电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。

使用不间断电源（UPS）来保证供电的稳定性和可靠性。采用双电源，在单路电源损坏时，可以自动切换，维持系统正常运转。

根据机房环境及设计规范要求，主机房和基本工作间，均设置了空气调节系统。空调系统使用中央空调，并采用独立空调作为备份。其组成包括精密空调、通风管路、新风系统。

CA 机房的要求参照电信设施管理的规定，而且每年对物理系统的安全性进行检查。

5.1.4. 水患防治

机房内无上下水系统，无渗水、漏水现象并做了严格防水处理，防止雨水或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

机房内主要设备均采用专用的防水插座，还具有动力与环境检测系统 7X24 小时实时监测各类漏水现象，能在漏水情况出现第一时间发出告警。

5.1.5. 火灾防护

火灾预防：

(1) 敏感区（物理三层）、高度敏感区域（物理四、五、六层）， 其建筑物的耐 火等级必须符合 GBJ45《高层民用建筑设计防火规范》中规定的二级耐火 等级。

(2) CA 机房设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位设置烟、温感探测器。

(3) 敏感区及高敏区配置独立的气体灭火装置，使用七氟丙烷（HFC-227ea）等洁净气体灭火系统，备有相应的气体灭火器，非敏感区根据实际情况可配置干粉灭火装置。CA 机房内敏感区域除对纸介质等易燃物质进行灭火外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂。

(4) 火灾自动报警、自动灭火系统避开可能招致电磁干扰的区域或设备，同时配套设置消防控制联动控制主机。还设有不间断的专用消防电源和直流备用电源，并具有自动和手动两种触发装置。

(5) 火灾自动灭火设施的区域内，其隔墙和门的耐火极限不低于 1 小时，吊顶的耐火极限不低于 15 分钟。

(6) 在非敏感区及敏感区的办公区域内，须设置紧急出口，紧急出口必须设有消防门，消防门符合安全要求。

(7) 紧急出口有监控设备进行实时监控，并保证紧急出口门随时可用。CA 机房采取适当的管理手段来保障非紧急避险状态下，紧急出口门不能被内部人员任意打开。

灭火系统采用电动，手动，紧急启动三种方式：

- 电动方式：防护区报警系统第一次火警确认后，发出声光警示信号，第二次火警确认后，经延时，同时发出气体释放信号，并发出启动电信号，送给对应的管网启动钢瓶，喷气灭火。
- 手动方式：人员对钢瓶或药剂瓶直接开启操作。
- 紧急启动：防护区外设有紧急启动按钮供紧急时使用。

CA 机房通过与专业防火部门协调，实施消防灭火等应急响应措施。

5.1.6. 介质存储

CA 机房的存储介质包括硬盘、软盘、磁带、光盘等，注意防磁、防静电干扰、防火、防水，由专人管理。

5.1.7. 废物处理

当 CA 机房存档的敏感数据或密钥已不再需要或存档期限已满时，应当将这些数据进行销毁。纸介质、光盘或软盘必须切碎或烧毁。如果保存在磁盘中，应

多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。密码设备在作废处置前根据制造商提供的方法先将其初始化再进行物理销毁。

5.1.8. 异地备份

CA 机构建立了同城异地容灾备份中心，机房的电子认证数据定期同步到容灾备份中心，用于容灾备份系统应急恢复。

5.2. 程序控制

5.2.1. 可信角色

电子认证服务机构、注册机构、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。

可信角色应包括：

(1) 系统管理员：系统管理员负责对数字证书服务体系在本单位的系统进行日常管理，执行系统的日常监控，并可根据需要签发服务器证书和下级操作员证书。

(2) 安全管理员：安全管理员对 CA 中心的物理、网络、系统的安全全面负责。并且拟订安全管理制度和操作流程，监督各岗位安全管理的执行情况。

(3) 审计管理员：审计管理员控制、管理、使用安全审计系统，安全审计系统分布于证书管理系统的各个子系统中，负责各个子系统的运行和操作

日志记录。

(4) 密钥管理员：密钥管理员负责管理 CA 中心的密钥相关设备，进行 CA 中心密钥的生成、备份、恢复、销毁等操作。

(5) 证书业务管理员：证书业务管理员对注册机构操作员进行管理，并对注册机构业务进行管理。

(6) 专业技术人员：专业技术人员对 CA、RA 系统和运营管理系统进行开发与优化、测试与验证，并为证书订户提供证书部署等相关技术支持。

5.2.2. 每项任务需要的人数

CA 机构制定了完善的管理策略，对关键任务的职责承担严格控制，对于敏感操作，至少有两人以上的可信角色共同完成。具体地，对密钥和加密设备的操作，需要 5 个可信人员中的 3 个共同完成；对证书签发系统后台修改、增删，或审核、签发数字证书，需至少 2 个负责证书业务管理的可信人员。

5.2.3. 每个角色的识别与鉴别

所有 CA 机构的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用双因素验证机制进行身份鉴别。CA 机构将独立完整地记录其所有的操作行为。

5.2.4. 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，CA 机构进行职责分离的角色，

包括但不限于证书业务受理、订户身份鉴别、订户身份鉴别审批、证书或 CRL 签发、系统工程与维护、CA 密钥管理、安全审计等。

5.3. 人员控制

5.3.1. 资格、经历和无过失要求

所有的员工与沃通公司签订保密协议。对于充当可信角色或其他重要角色的人员，必须具备的一定的资格或通过 CA 机构相关的培训和考核后方能上岗，具体要求在人事管理制度中规定。CA 机构要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响 CA 机构运行的其它兼职工作、无同行业重大错误记录、无违法记录等。

5.3.2. 背景审查程序

CA 机构与有关的政府部门和调查机构合作，完成对 CA 机构可信任员工的背景调查。

所有目前的可信任员工和申请调入的可信任员工都必须书面同意对其进行背景调查。

背景调查分为：基本调查和全面调查。

基本调查包括对工作经历，职业推荐，教育，社会关系方面的调查。

全面调查除包含基本调查项目外还包括对犯罪记录，社会关系和社会安全方面的调查。

调查程序包括：

(1) 人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

(2) 人事部门通过电话、信函、网络、走访、等形式对其提供的材料的真实性进行鉴定。

(3) 用人部门通过现场考核、日常观察、情景考验等方式对其考察。

(4) 经考核，人事部门和用人部门联合填写《可信雇员调查表》，报主管领导批准后准予上岗。

5.3.3. 培训要求

CA 机构对运营人员按照其岗位和角色安排不同的培训。培训有：PKI 基础知识、CP/CPS、信息验证过程中常见威胁、CA/Browser 论坛最新发布的 Baseline Requirements、系统硬件安装与维护、系统软件运行与维护、系统安全、应用软件的运行和维护、CA 中心的运行管理、CA 中心的内部管理、政策和规定及系统备份与恢复等。对负责 EV SSL 证书的运营人员，培训 EV 证书相关标准。

对于运营人员，其 CA 的相关知识与技能，每年至少要总结一次并由 CA 机构组织培训与考核。技术的进步、系统功能更新或新系统的加入，都需要对相关人员进行培训并考核。

CA 机构将员工参加培训的情况形成记录并存档，对于签发 SSL/TLS 服务器

证书的操作员和审核员，上岗前必须通过培训并达到 Baseline Requirements 中要求的从事该项工作所必须的技能水平。CA 机构每年至少组织一次培训与考核，确保其有足够的能力胜任该岗位。

5.3.4. 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受 CA 机构组织的培训一次，以保证其保持完成所负责工作的技能水平。

认证策略调整、系统更新时，应对全体人员进行再培训，以适应新的变化。

5.3.5. 工作岗位轮换周期和顺序

对于可替换角色，CA 机构应根据业务的安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。

5.3.6. 未授权行为的处罚

当 CA 机构员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用 CA 系统或进行越权操作，CA 机构得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

5.3.7. 独立合约人的要求

对不属于 CA 机构内部的工作人员，但与本 CA 机构订户证书签发业务有关的人员等独立签约者，CA 机构的统一要求如下：

(1) 人员档案备案；

(2) 正规劳务公司派遣人员；

(3) 具有相关业务的工作经验；

(4) 必须接受 CA 组织的岗前培训和再培训要求，达到 5.3.3 要求的技能要求。

5.3.8. 提供给员工的文档

为使得系统正常运行，CA 机构应向其员工提供完成其工作所必须的文档。

5.4. 审计日志程序

5.4.1. 记录事件的类型

CA 机构对如下事件进行记录：

(1) CA 密钥生命周期的管理事件，包括：

- 密钥生命周期的管理事件，例如生成、备份、存储、恢复、和归档。
- 密码设备生命周期的管理事件，例如接收、使用、和销毁。

这些记录都是密钥管理员完成的手工记录。

(2) CA 和订户证书生命周期的管理事件，包括，

- 证书的申请、批准、更新、撤销等。

- 成功或失败的证书操作。

这些记录由认证系统的系统日志和操作人员的手工记录组成。

(3) 系统操作事件，包括，

- 系统启动和关闭。
- 系统权限的创建、删除、变更、和密码修改。

这些记录由认证系统的系统日志和操作人员的手工记录组成。

(4) 系统安全事件，包括，

- 成功或不成功访问 CA 系统的活动。
- 对于 CA 系统网络的非授权访问及访问企图。
- 系统崩溃，硬件故障和其他异常。
- 防火墙记录的安全事件。

这些记录由系统的自动日志和操作人员的手工记录组成。

(5) CA 机构场地的工作记录，如，

- 授权人员进出。
- 非授权人员进出及陪同人。

- 场地设施的维护操作。

这些记录由系统的自动日志和操作人员的手工记录组成。

日志记录一般包括如下信息：

(1) 事件发生的日期和时间；

(2) 记录的序列号；

(3) 记录的类型；

(4) 记录的来源；

(5) 记录事件的实体；

(6) 其它的事件说明信息。

5.4.2. 处理日志的周期

CA 机构应建有 CA 应用系统的日志收集分析系统，实时收集应用日志并归档保存。CA 机构每月进行一次日志跟踪处理，检查违反策略及其它重大事件，每月进行发证系统日志分析。

5.4.3. 审计日志的保存期限

CA 系统审计日志至少保存十年，合格审计师可按需调阅。

5.4.4. 审计日志的保护

CA 机构授权的人员才能对审查日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作。审计日志的制作和访问进行岗位分离。

5.4.5. 审计日志备份程序

CA 系统审计日志备份采用数据库自身备份程序，根据记录的性质和要求，按照实时、每日、每周等策略进行备份。

5.4.6. 审计收集系统

审计日志收集系统涉及：

(1) 证书注册系统；

(2) 证书签发系统；

(3) 证书受理系统；

(4) 网站和数据库系统；

(5) 网络安全等其他需要审计的系统。

CA 机构应使用审计工具满足对上述系统审计的各项要求。

5.4.7. 对导致事件实体的通告

CA 机构发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻

击者，CA 机构保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

CA 机构有权决定是否对导致事件的实体进行通告。

5.4.8. 脆弱性评估

CA 机构对系统每季度进行一次漏洞扫描、每年进行一次渗透测试等脆弱性评估和识别内部和外部威胁、证书数据和管理面临的风险、以及应对这些风险的政策与程序是否完善等风险评估，以降低系统运行的风险。当 CA 机构技术架构或操作系统发生重大变更时，应进行漏洞扫描。在发现 CA 系统的重大漏洞时，CA 机构应在 4 天内完成处置。

5.5. 记录归档

5.5.1. 归档记录的类型

归档记录包括所有证书申请信息、证书和证书撤销列表、与证书申请相关的信息、身份鉴别材料等。

5.5.2. 归档记录的保存期限

所有归档记录的保存期为证书失效后十年。

5.5.3. 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能查询。CA 机构保护相关的档案内容，免遭恶劣

环境的威胁，如温度、湿度和强磁力等的破坏。

5.5.4. 归档文件的备份程序

所有存档的文件和数据库除了保存在 CA 主机房的存储库，应在异地保存其备份。存档的数据库应采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。CA 机构应当在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5. 记录时间戳要求

所有记录都要在存档时加具体准确的时间标识以表明存档时间。系统产生的记录，用标准时间加盖时间戳。

5.5.6. 归档收集系统

CA 机构有电子化的电子认证归档信息的存放系统。

5.5.7. 获得和检验归档信息的程序

由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，需要对这两个拷贝进行比较。CA 机构每年会验证归档信息的完整性。

5.6. 电子认证服务机构密钥更替

电子认证服务机构密钥更替指 CA 根证书到期和电子认证服务机构证书到期时，需要更换密钥而采取的措施。

1. CA 根密钥由加密机产生，更替办法为：

(1)使用旧的私钥对新的公钥及信息签名生成证书；

(2)使用新的私钥对旧的公钥及信息签名生成证书；使用新的私钥对新的公钥及信息签名生成证书。

(3)通过以上 3 张证书达到密钥更换的目的，使新旧证书之间互相信任。

2. 电子认证服务机构证书到期之前，CA 机构将采取以下方式更替：

(1)CA 机构将在 CA 证书到期前的 60 天内停止签发新的下级证书（“停止签发日期”）；

(2)产生新的密钥对，签发新的 CA 证书；

(3)在“停止签发日期”之后，CA 机构将采用新的 CA 密钥签发下级证书。

(4)密钥更替时直接把当前 CA 证书撤销，签发到 CRL 并发布，然后签发一个新的 CA 证书，通过证书库和 LDAP 方式下发给证书应用系统。

3. 机构将继续使用旧的私有密钥签发的 CRL，直到旧的私钥签发的最后证书到期为止。

5.7. 损害与灾难恢复

5.7.1. 事故和损害处理程序

针对故障事件，CA 机构制定了完善的应急处理预案和灾难恢复计划，发生故

障时，CA 机构将执行对应处理方案，并记录事件处理过程。

CA 机构每年测试、审查和更新应急处理预案和灾难恢复计划，以保证有效性。

5.7.2. 计算资源、软件和/或数据的损坏

CA 机构遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，CA 机构将按照灾难恢复计划实施恢复。

5.7.3. 实体私钥损害处理程序

CA 机构应每年执行一次根密钥泄漏应急程序的演练。

当 CA 根证书被作废时，CA 机构通知订户。

当 CA 的私钥被攻破或需要作废时，CA 机构根据 CA 灾难恢复计划规定的灾难恢复步骤进行操作。

当 CA 机构的根 CA 或中级 CA 出现私钥损害或者证书被作废时，将通过邮件方式通知依赖方及应用软件供应商如 360 等。

5.7.4. 灾难后的业务连续性能力

CA 机构针对证书系统的核心业务系统，证书签发系统和证书接口系统采用双机热备方式；对核心数据库，证书管理系统数据库采用磁盘阵列方式来确保证书系统的高可靠性和可用性。

发生自然或其它不可抗力性灾难后，CA 机构可采用远程热备站点对运营进

行恢复。具体的安全措施按照 CA 灾难恢复计划实施。

5.8. 电子认证服务机构或注册机构的终止

因各种情况，CA 机构需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

CA 机构在终止服务九十日前，就业务承接及其他有关事项通知有关各方，包括但不限于 CA 授权的发证机构和订户等。

CA 机构采用以下措施终止业务：

(1) 起草 CA 终止业务声明；

(2) 停止认证中心所有业务；

(3) 处理加密密钥；

(4) 处理和存档敏感文件；

(5) 清除主机硬件；

(6) 处理 CA 系统业务管理员和业务操作员；

(7) 通知与 CA 终止运营相关的实体。

根据 CA 机构与注册机构签订的运营协议终止注册机构的业务。

6. 认证系统技术安全控制

6.1. 密钥对的生成和安装

6.1.1. 密钥对的生成

6.1.1.1. CA 密钥对生成

CA 系统和 RA 系统的密钥对应在获得商用密码产品认证证书或 FIPS 140-2 认证且符合 Level 3 及以上安全规格的加密机内部产生。在生成 CA 密钥对时，CA 机构按照加密机密钥管理制度，执行详细的操作流程控制计划，选定并授权 5 个密钥管理员，采取五选三方式，密钥管理员凭借安全介质（如：USBKey）对密钥进行控制。

CA 密钥生成过程需要在第三方审计人员见证下进行，并由其出具见证报告。

6.1.1.2. 订户密钥对生成

对于全球服务器证书和时间戳证书，订户的密钥对由订户自己生成并保管。

对于客户端身份证书，本 CA 机构允许订户通过 USBKey、加密机或受签名人控制的其他安全方式生成密钥对。若订户选择由 CA 机构代其在 CA 机构提供的 USBKey 中生成，则生成的私钥不允许明文导出；若订户选择在自己的安全介质中生成密钥对，安全介质应获得商用密码产品认证证书或 FIPS 140-2 认证且符合 Level 2 及以上安全规格，订户在选择这些设备前，应事先向 CA 机构咨询有关系统兼容和接受事宜。

订户负有保护私钥安全的责任与义务，并承担由此带来的法律责任。如果订

户使用弱密钥申请证书，CA 机构将会拒绝该申请。除订户外的其他任何机构，不应对订户私钥进行归档。

6.1.2. 私钥传送给订户

若 CA 机构代订户在 USBKey 内部生成私钥时，由 CA 机构将 USBKey 邮寄给订户；若由订户自行生成时，不需要将私钥传送给订户。

6.1.3. 公钥传送给证书签发机构

订户或订户通过注册机构，将 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包，以电子文本的方式将公钥提交给本 CA 机构签发证书。当需要

通过网络传送时将使用安全套接层协议（SSL）或其他安全加密方式。

6.1.4. 电子认证服务机构公钥传送给依赖方

本 CA 机构的公钥包含在本 CA 机构自签发的根证书和中级 CA 证书中，依赖方可以从沃通公司官网：https://www.wotrus.com，下载根证书和中级 CA 证书，从而得到 CA 的公钥。

6.1.5. 密钥的长度

SM2 算法的根 CA 密钥长度为 256 位，签名算法为 SM3WithSM2。

SM2 算法的中级 CA 密钥长度为 256 位，签名算法为 SM3WithSM2。

SM2 算法的订户证书密钥长度为 256 位，签名算法为 SM3WithSM2。

6.1.6. 公钥参数的生成和质量检查

公钥参数必须使用国家密码管理部门许可的加密设备生成，并遵从这些设备的生成规范和标准。对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均已达到足够的安全等级要求。

6.1.7. 密钥使用目的

根 CA 密钥仅用于签署以下证书：

(1) 为根 CA 自身签发的根 CA 自签名证书；

(2) 中级 CA 的证书；

(3) OCSP 响应验证证书。

订户的密钥可以用于提供安全服务，例如：身份认证、信息加密和解密、不可抵赖性和信息的完整性。

6.2. 私钥保护和密码模块工程控制

6.2.1. 密码模块的标准和控制

CA 机构所用的密码模块经过认证，密码模块的标准、使用和控制都符合国家密码管理部门的有关规定。

6.2.2. 私钥多人控制（m 选 n）

CA 证书的私钥的生成、激活、更新、撤销、备份和恢复等操作必须采用多人控制机制，并且采用密钥分割技术，将 CA 私钥的管理权限分散到 m 张管理员卡

中，只有其中 n 人及以上在场并许可的情况下，插入管理员安全介质（如：USBKey）并输入 PIN 码，才能对私钥进行上述操作。其中 m 不小于 5，n 不小于 3。

6.2.3. 私钥托管

CA 机构的根私钥和 CA 私钥不允许托管，订户的证书对应的私钥由自己保管。

6.2.4. 私钥备份

CA 私钥备份以加密的形式保存在外部存储介质中并存放在安全区域，备份私钥的恢复采用多人控制，应由 3 人或以上密钥管理员到场方能执行恢复操作，私钥备份过程应符合本 CPS 第 5.2.2 节的要求，并在安全物理环境中执行。

CA 机构不备份订户的密钥。

6.2.5. 私钥归档

CA 私钥过期后，CA 机构必须对 CA 私钥归档加密保存至少十年。对 CA 私钥归档保存的方式为加密保存在外部存储介质中并存放在安全区域。

CA 机构不对订户证书的私钥进行归档。

6.2.6. 私钥导入、导出密码模块

CA 私钥在硬件密码模块中产生。在需要备份或迁移 CA 私钥时，从密码模块中导出的私钥必须由多人控制。

订户私钥不允许从硬件密码模块中导出，CA 机构不提供订户私钥从硬件密码模块中导出的方法。

6.2.7. 私钥在密码模块的存储

私钥以密文的方式，在硬件密码模块中加密保存。订户私钥存储在文件证书或 USBKey 等安全介质中，使用的 USBKey 等安全介质符合国家密码管理部门的相关规定，CA 系统采用国家密码管理部门认证的密码模块， 这些设备内置的协议 、算法等均已达到足够的安全等级要求。

6.2.8. 激活私钥的方法

CA 私钥存放在硬件密码模块中，激活需要按本 CPS 第 6.2.2 节使用加密设备的管理员权限实现，具有激活私钥权限的管理员使用安全介质（如：USBKey）登录，启动密钥管理程序，进行激活私钥的操作，需要三名管理员以上同时在场。

订户的私钥保存在密码模块中，订户使用密码模块口令（或 PIN 码）保护私钥。订户的私钥需要验证口令（或 PIN 码）后才能被激活和使用。

6.2.9. 解除私钥激活状态的方法

对于 CA 私钥，具有解除私钥激活状态权限的管理员使用含有自己的身份的安全介质（如：USBKey）登录，启动密钥管理程序，进行解除私钥激活状态的操作，需要三名管理员以上同时在场。

对于订户私钥，订户解除私钥激活状态由其自行决定。当服务程序关闭、系统注销或系统断电后私钥进入非激活状态。

6.2.10. 销毁私钥的方法

当 CA 私钥生命周期结束后，将通过本 CPS 第 6.2.5 节的方法进行 CA 私钥归

档，其他的 CA 私钥备份将被安全销毁。在 CA 私钥归档期结束后，具有销毁密钥权限的管理员，启动密钥管理程序，进行销毁密钥的操作，需要三名管理员以上同时在场。

6.2.11. 密码模块能力

CA 机构使用经国家密码管理部门认证的密码模块，以及支持本 CPS 第 7.1.3 节中的算法要求。

6.3. 密钥对管理的其他方面

6.3.1. 公钥归档

CA 机构必须对证书公钥进行归档，证书可在数据库中存放并异地备份。

6.3.2. 证书操作期和密钥对使用期限

CA 证书的有效期和其对应的密钥对的有效期都是一致的。订户证书的有效期和其对应密钥对的有效期保持一致。特殊情况下，对于签名类证书（如：时间戳证书），为验证在证书有效期内签名的信息，公钥可以在证书有效期限以外使用。

对于 CA 机构的根 CA 证书，有效期最长不超过 25 年。

对于 CA 中级证书，有效期最长不超过 20 年。

对于 SSL 全球服务器证书，有效期最长不超过 397 天。在 2020 年 8 月 31 日之前签发的 SSL 全球服务器证书，有效期最长不超过 2 年。

对于时间戳证书，有效期最长不超过 10 年。

对于客户端身份证书，有效期最长不超过 825 天。

6.4. 激活数据

6.4.1. 激活数据的产生和安装

为了保护私钥的安全，证书订户产生和安装激活数据必须保证安全可靠，从而避免私钥被泄漏、被偷窃、被非法使用、被篡改、或者被非法授权的披露。

CA 私钥的产生遵循本 CPS 第 6.2.2 节中的要求，严格进行生成、分发和使用。

订户私钥的激活数据，包括用于下载证书的口令（以邮件等形式提供）、USBKey 登录口令等，都必须在安全可靠的环境下随机产生。这些激活数据，都是通过安全可靠的方式，如离线当面递交、邮政专递等方式交给订户。对于非一次性使用的激活数据，CA 机构建议用户自行进行修改。

如果订户证书私钥的激活数据是口令，这些口令必须：

(1) 至少 8 位字符或数字；

(2) 至少包含一个字符和一个数字；

(3) 不能包含很多相同的字符；

(4) 不能和操作员的名字相同；

(5) 不能包含用户名信息中的较长的子字符串。

6.4.2. 激活数据的保护

CA 私钥的激活数据，CA 机构必须按照本 CPS 第 6.2.2 节中的密钥分割保护的方式将激活数据分割后由不同的可信人员掌管。

如果证书订户使用口令或 PIN 值保护私钥，订户应妥善保管好其口令或 PIN 值，并根据业务应用的需要随时进行变更，防止泄露或窃取。

6.4.3. 激活数据的其他方面

当订户私钥的激活数据进行传输时，需要保护激活数据在传输过程中免于丢失、偷窃、修改、泄露、或非授权使用，私钥激活数据与私钥存储介质应采用不同的传输通道分发给订户。

订户证书私钥的激活数据由订户自己进行保管、变更。在不需要时订户自行销毁激活数据，并确保他人无法通过残余信息、存储介质直接或间接的恢复订户私钥的激活数据。

6.5. 计算机安全控制

6.5.1. 特别的计算机安全技术要求

CA 系统的信息安全管理符合国家相关规定，主要安全技术和控制措施包括：采取严格的身份识别和人员访问控制、安全可信的操作系统、多层防火墙设置、防病毒软件、人员职责分权管理等。

对每位拥有系统（包括 CA 系统、RA 系统）业务操作权限的可信人员实行严格的双因素验证机制，访问时同时采用用户名、口令以及数字证书双因素登录方

式。

通过严格的安全控制手段，确保 CA 软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。

核心系统必须与其他系统物理分离，生产系统与其他系统逻辑隔离。使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动。在需要远程进行管理时，应通过安全网关进行访问并使用双因素身份鉴别规格来识别访问者身份。

6.5.2. 计算机安全评估

CA 系统使用的密码设备必须是经国家密码管理部门认证的密码设备，其他涉及安全的网络设备、主机、系统软件等都属经正式验收测试合格的产品。

6.6. 生命周期技术控制

6.6.1. 系统开发控制

CA 机构的软件设计和开发过程遵循以下原则：

(1) 制定公司内部的升级变更申请制度，并要求工作人员严格按照流程执行；

(2) 制定公司内部的采购流程及管理制度；

(3) 开发程序必须在开发环境进行严格测试成功后，再申请部署于生产环境；

(4) 变更部署前进行有效的在线备份；

(5) 第三方验证和审查；

(6) 安全风险分析和可靠性设计。

6.6.2. 安全管理控制

CA 系统使用严格的控制措施，所有的系统都经过严格的测试验证后才能进行安装和使用。通过对系统的维护保证操作系统、网络设置和系统配置安全。通过日志检查来检查系统和数据完整性和硬件的正常操作。

6.6.3. 生命期的安全控制

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均符合相关标准，使用了基于标准的强化安全通信协议确保了通信数据的安全，在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。在 CA 系统运行期间，周期性开展漏洞扫描及渗透测试，并及时消除系统安全弱点。

6.7. 网络的安全控制

CA 机构采用多级防火墙和网络控制系统，并且实施完善的访问控制技术。

认证系统只开放与申请证书、查询证书等相关的操作功能，供用户通过网络进行操作。

为了确保网络安全，认证系统安装部署了防火墙、入侵检测、安全审计、病

毒防范系统，并且及时更新防火墙、入侵监测、安全审计、病毒防范系统的版本，以尽可能的降低来自网络的风险。

6.8. 时间戳

时间戳系统提供的时间戳服务在技术实现上须严格遵循国际标准时间戳协议（RFC3161），采用标准的时间戳请求、时间戳应答以及时间戳编码格式，时间源须采用国家授时中心提供的标准时间。

7. 证书、证书撤销列表和在线证书状态协议

7.1. 证书模板

本 CA 机构签发的证书详细格式符合 X.509 V3 格式，同时遵循 RFC 5280 标准。证书至少包含基本的 X.509 V1 域，其规定值或值的限制参考如下表格。

证书结构的基本域

域	值或值的限制
版本	X.509 证书的格式版本，值为 V3。
序列号	通过 CSPRNG 生成大于零的 80 位非序列性的唯一标识符。
签名算法	签发证书时使用的签名算法（见本 CPS 第 7.1.3 节）。

签发者 DN	签发者的甄别名，包含 CN、O、C。
有效起始日期	基于国际通用时间（UTC）和北京时间同步。
有效终止日期	基于国际通用时间（UTC）和北京时间同步；有效期限的设置符合本 CPS 规定的限制。
主题 DN	证书持有者或实体的甄别名（见本 CPS 第 7.1.4 节）。 CA 根证书甄别名，包含 CN、O、C。 CA 中级证书甄别名，包含 CN、O、C。 订户 DV 证书甄别名，包含 CN。 订户 OV 证书甄别名，包含 CN、O、L、S、C。 订户 EV SSL 证书甄别名，包含 CN、O 、streetAddress、postalCode、L、S、C、serial Number、businessCategory、jurisdictionLocalityName（OID: 1.3.6.1.4.1.311.60.2.1.1 ）、jurisdictionStateOrProvinceName（OID：1.3.6.1.4.1.311.60.2.1.2 ）、jurisdictionCountryName（OID：1.3.6.1.4.1.311.60.2.1.3）。

公钥	使用本 CPS 第 7.1.3 节指定的算法，密钥长度满足本 CPS 第 6.1.5 节指定的要求。

7.1.1. 版本号

CA 机构签发的证书符合 X.509 V3 版本格式。版本信息在证书版本格式一栏体现。

7.1.2. 证书扩展项

本 CA 机构除使用 X.509 V3 版证书标准项和标准扩展项，还使用了自定义扩展项，证书内容和扩展项参考如下表格。

SM2 数字证书

域	根证书	中级证书	订户证书
版本	X.509 V3	X.509 V3	X.509 V3
签名算法	SM3WithSM2	SM3WithSM2	SM3WithSM2
密钥长度	256bits SM2	256bits SM2	256bits SM2
颁发机构	当同一个 X.500 名字用	当同一个 X.500 名字用	当同一个 X.500 名字用

密钥标识符	于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500 名字。	于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500 名字。	于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500 名字。
主题密钥标识符	当同一个 X.500 名字用于多个证书持有者 时，用一比特字符串来唯一标识证书持有者的 X.500 名字。	当同一个 X.500 名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500 名字。	当同一个 X.500 名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500 名字。
CRL 分发点	无	由本 CA 机构指定的 CRL 发布点。	由本 CA 机构指定的 CRL 发布点。
授权信息访问	无	包含颁发者的 OCSP 响应地址。（accessMethod = 1.3.6.1.5.5.7.48.1） 包含颁发者证书的访问地址。（accessMethod =	包含颁发者的 OCSP 响应地址。（accessMethod = 1.3.6.1.5.5.7.48.1） 包含颁发者证书的访问地址。（accessMethod =

		1.3.6.1.5.5.7.48.2）	1.3.6.1.5.5.7.48.2）
证书策略	无	包含颁发者指定的 policy Identifier。包含颁发者 CA 的 CPS 发布地址。	包含颁发者指定的 policy Identifier 和 CA/Browser 论坛中保留的 Policy Identifier 。包含颁发者 CA 的 CPS 发布地址。
增强型密钥用法	无	进一步指明已认证的公开密钥具体用途。	进一步指明已认证的公开密钥具体用途。
基本约束	CA 证书的基本限制 扩展项中的主体类型 被设为 CA。	CA 证书的基本限制扩展项中的主体类型被设为 CA。	订户证书的基本限制扩展项的主体类型设为最终实体 （End-Entity）。
密钥用法	指明已认证的公开密钥用于何种用途。	指明已认证的公开密钥用于何种用途。	指明已认证的公开密钥用于何种用途。

本 CA 机构签发的 SSL 全球服务器证书、时间戳证书包含增强型密钥用法，

用于指明已认证的公开密钥具体用途。增强型密钥用法参考如下表格。

增强型密钥用法

订户证书	增强型密钥用法
SSL 全球服务器证书	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）
时间戳证书	时间戳（1.3.6.1.5.5.7.3.8）
客户端身份证书	客户端身份验证（1.3.6.1.5.5.7.3.2） 安全电子邮件（1.3.6.1.5.5.7.3.4）

7.1.3. 算法对象标识符

本 CA 机构签发 SM2 证书的密码算法标识符为 SM3WithSM2，证书符合 GB/T 20518-2018 标准。

7.1.4. 名称形式

本 CA 机构签发的证书，其名称形式的格式和内容符合 X.501 的甄别名格式。

7.1.5. 名称限制

无规定。

7.1.6. 证书策略对象标识符

证书策略对象标识符同本 CPS 第 1.2 节。

7.1.7. 策略限制扩展项的用法

无规定。

7.1.8. 策略限定符的语法和语义

无规定。

7.1.9. 关键证书策略扩展项的处理规则

无规定。

7.2. 证书撤销列表

CA 机构定期签发证书撤销列表，供用户查询使用。签发的证书撤销列表符合 X.509 V2 格式。

7.2.1. 版本号

CA 机构签发 X.509 V2 版本的 CRL。版本信息在证书版本格式一栏体现。

7.2.2. CRL 和 CRL 条目扩展项

本 CA 机构的证书撤销列表（CRL）是一个带时间戳并经过数字签名的已撤销证书的列表。

CRL 数据定义如下：

CRL 数据	定义
CRL 的版本号	指定 CRL 的版本信息，本 CA 机构采用同 X.509 V3 证书对应的 CRLV2 版本。
签名算法	本 CA 机构采用 SM3WithSM2 签名算法。
颁发者	指定签发机构的 DN 名。
生效时间	指定一个日期/时间值，用以表明本 CRL 发布的时间。
更新时间	指定一个日期/时间值，用以表明下一次 CRL 将要发布的时间（本标准强制使用该域）。
撤销证书列表	指定已经撤销的证书列表，含有证书的序列号和证书被撤销的日期和时间。
颁发机构密钥标识符	用来验证在 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥。

证书撤销列表号	用来确定一个特定的 CRL 何时取代另一个 CRL。
CRL 条目扩展项	不使用 CRL 条目扩展项。

7.3. 在线证书状态协议

本 CA 机构采用 IETF PKIX 工作组开发的一个在线证书状态协议（Online Certificate Status Protocol，OCSP），提供在线证书状态查询服务，签发的 OCSP 响应符合 RFC6960 标准。

7.3.1. 版本号

RFC 6960 定义的 OCSP v1 版。

7.3.2. OCSP 扩展项

不使用 OCSP 扩展项。

8. 认证机构审计和其他评估

8.1. 评估的频率或情形

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子政务电子认证服务管理办法》以及《电子认证服务密码管理办法》规定，接受相关主管部门的评估与检查；

CA 机构应进行的评估频率：

(1) 每年至少一次进行内部相关安全合规基线的自评估检查；

(2) 每年一次接受相关主管部门根据法律法规规定，对 CA 机构的年度检查。

8.2. 评估者的资质

内部审计人员的选择一般包括：CA 的安全负责人及安全管理人员、CA 业务负责人、认证系统及信息系统负责人、人事负责人、其他需要的人员。

8.3. 评估者与被评估者之间的关系

内部审计人员与本 CA 机构的系统管理员、业务管理员、业务操作员的工作岗位不能重叠。

8.4. 评估内容

评估审核工作包括但不限于：

(1) CA 物理环境控制是否得到充分的实施；

(2) 运营工作流程与制度是否得到严格遵守；

(3) 是否严格按照 CPS、业务规范和安全要求开展认证业务；

(4) 日志与记录是否完整无误；

(5) 密钥管理、证书生命周期管理是否符合业务规则；

(6) 是否存在其他潜在安全风险。

8.5. 对问题与不足采取的措施

由 CA 机构管理层对审计报告进行评估，并将审计中发现的问题交由相应责任职能部门进行业务改进和完善。CA 机构将根据国际惯例和相关法律、法规迅速解决问题。

8.6. 评估结果的传达与发布

(1) CA 机构内部审计结果将仅在公司内部传达；

(2) 如 CA 机构的审计结果发现可能造成订户安全隐患的情况，则应及时向订户通报。

任何第三方向被评估实体通知评估结果或者类似的信息，都必须事先明确向 CA 机构表明通知的目的和方式，并征得 CA 机构的同意，法律另有规定的除外；CA 机构保留在这方面的法律权利。

8.7. 自我评估

CA 机构将进行持续的自我评估，根据国际和国内相关标准和本 CPS 的规定，通过至少每年一次的内部风险评估、至少每三个月一次的抽样自我审查来严格控制服务质量。自我评估对上次审核期间末至本次审核期间初期间内的电子认证活动是否符合相关规定。抽样审查的样本数量不得少于此期间内签发证书总数的 3%。

9. 法律责任和其他业务条款

9.1. 费用

9.1.1. 证书签发和更新费用

沃通公司可根据提供的电子认证相关服务向证书订户收取费用，具体收费标准根据市场和管理部门的规定自行决定。CA 机构在不高于收费标准的前提下可以对证书价格进行适当调整。在订户向 CA 机构订购证书时，将提前告知证书的签发与更新费用。如果沃通公司签署的协议中指明的价格和沃通公司公布的价格不一致，以协议中的价格为准。

9.1.2. 证书查询费用

在证书有效期内，对该证书进行信息查询，CA 机构暂不收取此项费用，但保留对此项服务收费的权利。

9.1.3. 证书撤销或状态信息的查询费用

CA 机构暂不收取此项费用，除非用户提出的特殊需求，需要 CA 机构支付额外的费用，CA 机构将与用户协商收取应该收取的费用。

9.1.4. 其他服务费用

CA 机构保留对其他服务收费的权利。CA 机构可根据请求者的要求，订制各类通知服务，具体服务费用，在与订制者签订的协议中约定。

9.1.5. 退款策略

在实施证书操作和签发证书的过程中，CA 机构遵守严格的操作程序和策略。除非出现 CA 机构违背了本 CPS 所规定的责任或其他重大义务的情况，订户可以要求 CA 机构撤销证书并退款，其他情况下，CA 机构对订户收取的费用均不退还。

完成退款后，订户如继续使用该证书，CA 机构将追究其法律责任。

订户应当提供符合 CA 机构要求的完整、真实、准确的证书申请信息，否则，CA 机构对此造成的损失和后果不承担任何责任。

如果订户在证书服务期内退出数字证书服务体系，CA 机构将不退还剩余时间的服务费用。

9.2. 财务责任

9.2.1. 保险范围

出现以下情形并经 CA 机构确认后，证书订户、依赖方等实体可以申请 CA 机构承担赔偿责任（法定或约定免责的除外）：

(1) CA 机构错误地将证书签发给订户以外的第三方，且导致订户或依赖方遭受损失；

(2) CA 机构发现订户提供了虚假的注册信息或资料，仍为其签发证书，并导致依赖方遭受损失；

(3) CA 机构未按鉴证要求对订户证书申请信息进行审核，并据此签发了

数字，导致订户或依赖方遭受损失；

(4) CA 机构使证书私钥被破译、窃取，导致订户或依赖方遭受损失；

(5) CA 机构未能及时撤销证书，导致订户或依赖方遭受损失。

CA 机构只对由于自身原因造成证书订户、依赖方的直接损失承担责任，对间接损失不承担责任。CA 机构对于任何证书或依赖方等实体的证书赔偿合计责任不得超出证书市场购买价格的 10 倍。

9.2.2. 其他资产

CA 机构确保本公司拥有足够的财务实力以维持正常运营并保证相应义务的履行，且能够合理承担对订户及依赖方的责任。

上述要求对证书订户同等适用。

9.2.3. 对最终实体的保险或担保

如果 CA 机构根据本 CPS 或相关法律法规的规定，以及相应的司法判定需承担赔偿和/或补偿责任的，CA 机构将按照相关法律法规规定、仲裁机构的裁决或法院的裁判结果承担相应的赔偿责任。

9.3. 业务信息保密

9.3.1. 保密信息范围

在 CA 机构提供的电子认证服务中，保密信息包括但不限于：

(1) CA 机构与订户之间的协议以及资料中未公开的内容。除法律明文规定或政府及执法机关的要求，CA 机构承诺不对外公布或透露订户证书信息以外的任何保密信息。

(2) 订户私钥属于机密信息，订户应根据本 CPS 的规定进行妥善保管，如因订户个人原因导致私钥泄露而造成损失，由订户自行承担；

(3) 其他由 CA 机构和 RA 保存的订户信息应视为保密，除相关法律法规或政府及执法机关的要求，不予公布。

9.3.2. 不属于保密的信息

以下信息不属于 CA 机构认定的保密信息：

(1) 与证书有关的申请流程、申请需要的手续、申请操作指南等信息；

(2) 由 CA 机构签发的证书和 CRL 中的信息；

(3) 由 CA 机构支持、CPS 识别的证书策略信息；

(4) 提供方披露数据和信息前，已被接受方所持有的数据和信息；

(5) 提供方披露数据和信息时或之后，非因接受方原因而被披露的数据和信息；

(6) 有权披露的第三方披露给接受方的数据和信息；

(7) 其他可通过公开渠道获取的信息。

9.3.3. 保护保密信息的责任

CA 机构通过严格的管理制度、流程和技术手段保护机密信息，包括但不限于商业机密、客户信息等。CA 机构的全体员工都将严格遵守保密条款。

CA 机构有妥善保管本 CPS 第 9.3.1 节中规定的保密信息的责任与义务。

9.4. 用户隐私保密

依据相关法律、法规，CA 机构在受理客户申请证书及相关电子签名业务时，需由证书申请人及/或经办人提供相关个人信息。其中个人信息包括但不限于：姓名、联系方式、身份证号、地址和身份证（原件及/或任何形式的副本）。CA 机构针对用户个人信息提供如下保障措施。

9.4.1. 隐私保密方案

CA 机构尊重证书订户个人资料的隐私权并在官网发布了个人信息保护政策，保证完全遵照国家对个人资料隐私保护的相关法律法规及有关规定。同时，CA 机构确保全体员工严格遵守安全和保密标准对个人信息给予的保密。订户选择使用 CA 机构的证书服务时，即表明已经同意接受 CA 机构的《个人信息保护政策》。

9.4.2. 作为隐私处理的信息

CA 机构在管理和使用订户提供的相关信息时，除证书中已包含的信息以及证书状态信息外，订户的基本信息将被视为隐私处理。包括但不限于以下信息：

(1) 订户的有效身份证号码，如居民身份证号码、单位机构代码；

(2) 订户的联系电话；

(3) 订户的通信地址和住址；

(4) 订户的银行账户。

上述信息仅由 CA 机构使用，非经订户同意或有关法律法规、执法机关或政府根据合法的程序要求，CA 机构不会予以公开。

9.4.3. 不被视为隐私的信息

订户持有的证书信息，以及证书状态信息不被视为隐私信息。

9.4.4. 保护隐私的责任

CA 机构有妥善保管本 CP 第 9.4.2 节中规定的证书申请者个人信息使用、共享、管理、查阅、删改等责任与义务。

在政府或执法机关根据合法程序要求 CA 机构向特定对象公布隐私信息的情况下，CA 机构无需承担由此造成的责任。

9.4.5. 使用隐私信息的告知与同意

(1) 订户同意，CA 机构应采取适当的步骤保护证书订户的个人信息，应在订户协议中事先告知订户并征得订户同意；

(2) 订户同意，CA 机构在业务范围内按照本 CPS 规定的隐私保护政策使用所获取的任何订户信息，如需超出约定范围及用途使用证书订户的隐私信息，应事先告知证书订户并获得同意及授权。如未获得同意及授权，CA 机构不会将订户

隐私信息透露给任意第三方；

(3) 订户同意，在有关法律法规、执法机关或政府根据合法的程序要求下，CA 机构向特定对象披露隐私信息时，CA 机构无需告知订户。

9.4.6. 依法律或行政程序的信息披露

除非符合以下条件，CA 机构不会将订户的保密信息提供给其他第三人或第三方机构：

(1) 执法机关、政府或其他相关法律法规授权的部门依据法律、法规、规章、决定、命令等提出申请；

(2) 订户采用书面形式授权相关信息的披露；

(3) 本 CPS 规定的其他可以披露的情形。

9.4.7. 其他信息披露情形

如果证书订户要求 CA 机构提供某类特定客户支援服务，如资料邮寄时，CA 机构可以将不被视为订户隐私信息的相关信息，如订户的姓名和邮寄地址提供给第三方，如邮寄公司。

9.5. 知识产权

(1) CA 机构享有并保留对证书及 CA 机构提供的全部软件、资料、数据等的著作权、专利申请权等全部知识产权；

(2) CA 机构享有由本机构制定并发布的 CPS、CP、技术支持手册、发布的

证书和 CRL 等的所有权和知识产权；

(3) CA 机构官方网站上公布的一切信息均属于 CA 机构财产，未经 CA 机构书面允许，他人不得转载用于商业行为；

(4) CA 机构对外运营管理策略和规范属于 CA 机构财产。

9.6. 陈述与担保

9.6.1. 电子认证服务机构的陈述与担保

CA 机构在提供电子认证服务活动过程中的担保如下：

(1) CA 机构遵守《中华人民共和国电子签名法》及相关法律的规定，对签发的数字证书承担相应的法律责任；

(2) 验证申请人对列在证书主题字段及主题别名扩展（或，仅针对域名而言，获得了拥有域名所有权或控制权人士的授权）中的域名及 IP 地址拥有所有权或控制权；

(3) 验证申请人授权了证书的签发且申请人代表获得了合格授权，以代表申请人申请证书；

(4) 验证证书中包含的全部信息的准确性（organizationUnitName 信息除外）；

(5) 采取措施以减小证书主题“organizationUnitName”中所含信息存在误导的可能性；

(6) 根据本 CPS 第 3.2 节的要求验证申请人身份；

(7) CA 机构维护针对所有未过期证书的当前状态信息(有效或已撤销)，并据此建立并维护一个全天候的（24 X7）公开可访问信息库；

(8) 根据本 CPS 制定的原因可撤销证书；

(9) CA 机构准确描述了证书政策和认证实践声明中的程序；

(10) CA 机构签发给订户的证书符合本 CPS 的所有实质性要求；

(11) CA 机构将向证书订户通报任何已知的、将在本质上影响订户证书有效性与可靠性的事件；

(12) CA 机构拒绝签发证书后，将立即向证书申请人归还所付的全部费用。

9.6.2. 注册机构的陈述与担保

作为 CA 机构的注册机构，应遵循 CA 机构的 CPS 与 CP 承担电子认证业务中注册机构的职责，注册机构的电子认证业务操作受行业及 CA 机构的相关管理规定约束。CA 机构的注册机构在参与电子认证服务过程中的具体承诺如下:

(1) 注册机构向证书订户提供的注册过程完全符合 CA 机构的 CPS 的所有实质性要求；

(2) 如注册机构对订户的证书申请材料未通过审查，注册机构有告知订户的义务；

(3) 注册机构在合理期间内完成证书申请处理，在申请人提交资料齐全且合规的情况下，处理证书申请的时间一般为 1-3 个工作日；

(4) CA 机构生成证书时，不会由于注册机构的失误而导致证书中的信息与证书申请人的信息不一致；

(5) 注册机构将按本 CPS 的规定，及时向 CA 机构提交撤销、更新等申请；

(6) 注册机构应通过安全通道将证书订户的信息传送给 CA 机构；

(7) 注册机构应妥善保管订户的信息及与认证相关的信息，并适时转交给 CA 机构以存档。注册机构应根据相关协议要求配合 CA 机构进行电子认证业务合规性审计；

(8) 注册机构应尽到对订户的安全提示义务。

9.6.3. 订户的陈述与担保

订户自接受 CA 机构签发的证书时起，即视为向 CA 机构、注册机构及信赖证书的有关当事人作出下述承诺：

(1) 订户确认已知悉并接受了本 CPS 及相关规定的全部内容，且同意受本 CPS 条款的约束；

(2) 订户应遵循诚实守信原则，在申请数字证书及签发相关的其他方面，都有义务始终向 CA 机构提供准确完整的信息和资料，并在上述信息及资料发

生变更时及时通知 CA 机构。如因订户提供的资料不真实、不完整、不准确或变更后未及时通知 CA 机构，由此造成的损失由订户自行承担。如果存在代理人，那么订户和代理人两者负有连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知 CA 机构；

(3) 订户使用 CA 机构数字证书时，应使用合法途径获取相关软件；

(4) 订户应将证书用于合法目的并在有效期内进行数字签名；

(5) 订户应通过可靠方式产生密钥对，并有义务采取一切合理措施防止密钥遭受攻击而丢失、泄露和误用；订户应妥善保管 CA 机构签发的数字证书的私钥和密码，不得泄露或交付他人。如因订户原因导致他人知道、盗用、冒用数字证书私钥和密码，由此造成的损失由订户自行承担；

(6) 与订户证书所含公钥对应的私钥所进行的每一次签名，都是订户自己的签名，且签名时的证书是有效证书（证书没有过期或被撤销），证书的私钥为订户本身访问和使用；

(7) 订户将审查和验证证书内容的准确性，确认其在取得的证书信息无误；

(8) 订户在使用证书时，应在证书中列出的可访问的服务器上安装证书，并符合全部使用的法律法规和用户协议约定的使用范围和条件；

(9) 不得拒绝任何来自 CA 机构公示过的声明、变更、更新、升级等，

包括但不限于策略、规范的修改和证书服务的增加和删减等；

(10) 订户在取得证书后如发现以下情况，应立即向 CA 机构申请撤销：

- 有任何实际或可疑的滥用或泄露用户证书中包含的与公钥相对应的私钥，则要求立即撤销证书，并停止使用证书及其相关的私钥；
- 证书中的信息不正确或不准确，则要求立即撤销并停止使用证书；

(11) 一旦 CA 机构发现了订户证书的不当使用或订户被用于违法甚至犯罪行为，CA 机构有权直接撤销订户证书；

(12) 订户保证，一旦证书被 CA 机构撤销后，将不再使用该证书。

9.6.4. 依赖方的陈述与担保

依赖方应作出如下声明和承诺：

(1) 熟悉本 CPS 的条款，了解证书的使用目的，遵守本 CPS 的所有规定，同意本 CPS 中关于 CA 机构责任限制的规定；

(2) 获取并安装该证书对应的证书链，在信赖证书前，对证书的信任链进行验证；

(3) 在信赖证书所证明的信任关系前确认该证书有效，包括：通过查询 CRL 或 OCSP 确认证书是否被撤销；确认证书在规定的范围和期限使用；检查该证书路径中所有出现过的证书的可靠性；确认该证书记载的内容与所要证

明的内容一致；检查其他可能影响证书有效性的信息；

(4) 不得拒绝任何来自 CA 机构公示过的声明、变更、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等；

(5) 依赖方一旦由于疏忽或其他原因违背了合理检查的条款，依赖方应就此给 CA 机构带来的损失进行赔偿，并应承担因此造成的自身或他人损失。

9.6.5. 其他参与者的陈述与担保

未列于此的其他参与者应遵循本 CPS 的规定。

9.7. 担保免责

除本 CPS 第 9.6.1 节中的明确承诺外，CA 机构不承担其他任何形式的保证和义务：

(1) 不保证证书订户、信赖方及其他参与者的陈述与担保；

(2) 不对电子认证活动中使用的任何其他软件做出担保；

(3) 不承担超出证书范围使用或用于其他未被 CA 机构允许的用途带来的损失；

(4) 不承担超出证书规定目的意外的应用造成的损失；

(5) 不承担因非 CA 机构原因导致的设备故障、网络中断导致证书报错、交易中断或其他事物造成的损失；

(6) 不承担由于不可抗力因素导致的服务中断并由此造成的客户损失；

(7) 明显由于 CA 机构的合作方的越权行为或其他过错行为所引发的违反约定义务而对订户造成的损失，CA 机构不承担责任。

9.8. 有限责任

如果 CA 机构根据本 CPS 或相关法律法规规定，以及司法判定须承担赔偿和或补偿责任的，CA 机构将承担不超过本 CPS 第 9.9 节规定的有限赔偿责任。

CA 机构在与订户和依赖方签订的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

9.9. 赔偿

9.9.1. CA 机构的赔偿

如 CA 机构违反了本 CPS 第 9.6.1 节中的陈述与担保，证书订户、依赖方可以申请 CA 机构承担赔偿责任（法定或约定免责除外）。下述情形应由 CA 机构承担有限赔偿责任：

(1) CA 机构将证书错误签发给订户以外的第三方，导致订户或依赖方遭受损失；

(2) 在订户提交信息或资料完整准确的情况下，CA 机构签发的证书含有错误信息，且导致订户或依赖方由此遭受损失；

(3) CA 机构明知订户提交的信息或资料存在虚假谎报的情况，却仍为订

户签发证书，由此导致依赖方遭受损失；

(4) 由于 CA 机构的原因致使证书私钥的泄露，导致订户或依赖方遭受损失；

(5) CA 机构未能及时撤销证书，由此导致依赖方遭受损失。

9.9.2. 订户的赔偿

证书订户在使用或信赖证书时，若有任何行为或疏漏而导致 CA 机构和注册机构产生损失，订户应承担赔偿责任。

订户接受证书就表示同意在以下情况下承担赔偿责任：

(1) 未向 CA 机构提供真实、完整和准确的信息，而导致 CA 机构或有关各方损失；

(2) 未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时，订户必须对这种行为的后果负责；

(3) 在知悉证书密钥已经失密或者可能失密时，未及时告知 CA 机构，并终止使用该证书，而导致 CA 机构或有关各方损失；

(4) 订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个数字签名后理所当然地相信这些表述，订户必须对这种行为的后果负责；

(5) 证书的非法使用，即违反 CA 机构对证书使用的规定，造成了 CA 机构或有关各方的利益受到损失。

9.9.3. 依赖方的赔偿

如因下述情形而导致 CA 机构或订户遭受损失，依赖方应承担赔偿责任：

(1) 未履行 CA 机构与依赖方的协议和本 CPS 中规定的义务；

(2) 未依照本 CPS 合理审核，导致 CA 机构及其授权的证书服务机构或第三方遭受损失；

(3) 在明显不合理的情形下信赖证书，如依赖方明知证书超范围、超期限使用，证书已经或可能被窃取等情形；

(4) 依赖方未验证证书的信任链；

(5) 依赖方未通过查询 CRL 或 OCSP 验证证书是否被撤销。

9.10. 有效期限与终止

9.10.1. 有效期限

本 CPS 在生效日期零时正式生效，上一版本的 CPS 同时失效。

9.10.2. 终止

CA 机构有权终止本 CPS（含修订版）。本 CPS 在下一版本 CPS 生效之日或在 CA 机构终止电子认证服务时失效。

9.10.3. 效力的终止与保留

本 CPS 终止后，其效力将同时终止，CPS 中的内容将视为无效使用。但对终止之日前发生的法律事实，CPS 中对各方责任的规定及免除责任仍然有效。CPS 中涉及的审计、保密信息、隐私保护、知识产权等方面继续有效。

9.11. 对参与者的个别通告与沟通

参与者如需进一步了解本 CPS 中提及的条款，可以通过电话联系 CA 机构。

本 CPS 终止后，CA 机构将就文档失效的有关事宜通知参与本机构电子认证活动的有关各方。

9.12. 修订

9.12.1. 修订程序

经 CA 机构安全策略管理委员会授权,CPS 编写小组每年至少审查一次本 CPS，确保其符合国家法律法规和主管部门的要求及相关国际标准，确保其符合《沃通电子认证服务有限公司 SM2 全球信任体系证书策略（CP3）》要求，符合认证开展的实际业务需要。

本 CPS 的修订与更新，由 CPS 编写小组提出修订报告，经 CA 机构安全策略管理委员会批准后，由 CPS 编写小组负责组织修订，修订后的 CPS 需经 CA 机构安全策略管理委员会批准后在沃通公司的网站（https://www.wotrus.com）正式对外发布。

本 CPS 将进行严格的版本控制。

9.12.2. 通知机制和期限

修订后的 CPS 经批准后将立即在 CA 机构的官网 https://www.wotrus.com 上发布。 对于需要通过电子邮件、信件、媒体等方式通知的修改，CA 机构将在合理的时间内通知有关各方，合理的时间应保证有关方受到的影响最小。如在修订后发布的 7 个工作日内，订户没有申请对其证书的撤销，将被视为同意该修订。

9.12.3. 必须修改业务规则的情形

(1) 本 CPS 中相关内容与管辖的法律法规或部门规章不一致，CA 机构将据此修改本 CPS 中的相关内容；

(2) 国家监管部门对本 CPS 由明确的更改或调整要求；

(3) 本 CPS 描述的规则、流程和相关技术已经不能满足 CA 机构电子认证业务的要求；

(4) 本 CPS 中相关内容与 WebTrust 对 CA 的规则不一致，CA 机构将据此修改本 CPS 中的相关内容。

9.13. 争议处理

CA 机构、证书订户、依赖方等实体在电子认证活动中产生争议时，应在争议产生之时起 3 个月内向 CA 机构提出争议处理请求并通知有关各方，争议解决的方式可按如下步骤：

(1) 根据本 CPS 及相关法律法规的规定，明确责任方；

(2) 由 CA 机构相关部门负责与申请人协调；

(3) 若 CA 机构协调失败，再由有关法律部门进行裁决；

(4) 任何与 CA 机构或注册机构就本 CPS 所涉及的任何争议，争议双方仅可以将争议提交深圳仲裁委员会仲裁。

9.14. 管辖法律

CA 机构的 CPS 受国家已颁布的《中华人民共和国民法典》、《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子政务电子认证服务管理办法》以及《电子认证服务密码管理办法》法律法规管辖。如本 CPS 中某项条款与上述法律法规条款或其可执行性发生抵触，CA 机构将对此条款进行修订，使之符合相关法律法规规定。

9.15. 与适用法律的符合性

无论 CA 机构的证书订户、依赖方等实体在何地居住以及在何处使用 CA 机构的证书，本 CPS 的执行、解释和程序有效性均适用中华人民共和国法律规定。任何与 CA 机构或授权注册机构就本 CPS 所涉及的任何争议，均应适应中华人民共和国法律。

9.16. 一般条款

9.16.1. 完整协议

CA 机构的 CPS 完整的文档结构包括：标题、目录、主体内容 3 部分。关于对目录和主体内容修改后的替代内容，将完全替代所有先前部分。本 CPS 将替代所

有以前的或同时期的、相同主题的书面或口头解释。本完整协议将放置在 CA 机构的官方网站中以供查询和浏览。

9.16.2. 转让

CA 机构声明，根据本 CPS 中详述的认证实体各方的权利和义务，各方当事人可按照法律法规的相关规定进行权利与义务的转让。此转让行为发生时不影响转让方对另一方的任何债务及责任的更新。

9.16.3. 分割性

本 CPS 的任何条款或应用由于与 CA 机构所在管辖权的法律法规发生冲突而被判定为无效或不具有执行力时，CA 机构可以在最低必要的限度下修订该条款，使其继续有效，其余部分不受影响，CA 机构将在此章节披露修订的内容。

9.16.4. 强制执行

CA 机构声明，若订户证书、依赖方等实体未执行 CA 机构的 CPS 中某项规定，不被认为该实体将来不执行该项或其他规定。

9.16.5. 不可抗力

CA 机构不对因战争、恐怖活动、自然灾害、传染性疾病、罢工、互联网或其他基础设施无法使用等不可抗力的事件所造成本 CPS 规定担保责任的违反、延误或无法履行负责。

9.17. 其他条款

CA 机构对本 CPS 具有最终解释权。