沃通电子认证服务有限公司
通用证书策略（CP1）

版本：1.0.1

发布日期：2024 年 3 月 1 日

生效日期：2024 年 3 月 1 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
1.0.1	版本发布	初始版本	沃通安全策略管理委员会	2024 年 3 月 1 日

声明

本 CP 全部或者部分支持下列标准：

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

RFC5280：互联网 X.509 公钥基础设施证书和 CRL 属性

RFC2560：互联网 X.509 公钥基础设施-在线证书状态协议-OCSP

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

目 录

1.引言

1.1 概述

沃通电子认证服务有限公司（WoTrus CA Limited）（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，为电子活动提供可信身份、可信时间和可信行为的网络信任环境。

证书策略（Certification Policy，以下简称 CP）是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。

本文档《沃通电子认证服务有限公司通用证书策略》（以下简称《沃通通用证书策略》）满足互联网标准组织制定的 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》，以及国内标准 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》的框架和内容要求。《沃通通用证书策略》适用范围为沃通发放的通用证书，包括个人证书、机构证书和设备证书。具体设定了证书策略、生命周期、使用、依赖和管理的角色、责任与要求，以及各相关主体的职责。为批准、签发、管理和使用证书和相关的可信服务制定业务，提供技术、策略和法律上的要求和规范。

1.2 文档名称与标识

本文档的名称为《沃通电子认证服务有限公司通用证书策略》（简称《沃通通用证书策略》），该文档没有分配对象标识符。

1.3 PKI 参与者

1.3.1 电子认证服务机构

沃通电子认证服务有限公司是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，依法设立的第三方电子认证服务机构（简称：沃通）。

沃通是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。

1.3.2 注册机构

注册机构（简称：RA 机构）是受理数字证书的申请、更新、恢复和吊销等业务的实体。

沃通可以授权下属机构或委托外部机构作为注册机构，负责提供证书业务办理、身份鉴证与审核等服务。

沃通授权外部机构作为注册机构，应与外部机构签署合同中，明确双方的权利与义务，以及承担的法律责任。

1.3.3 订户

订户是指向沃通申请数字证书的实体。

1.3.4 依赖方

依赖方是指为某一应用而使用、信任沃通签发的证书，并验证证书和相应签名的实体。

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

沃通签发的通用证书适合应用在企业信息化、电子政务和电子商务等领域，用于证明订户在电子化环境中所进行的身份认证和电子签名，以及数据加密等服务。证书类型包括：

1） 个人证书

个人证书，包括个人用户证书和机构雇员证书，用于区分、标识、鉴别个人身份的场景，适用于个人身份认证和电子签名，以及数据加密等服务。

2） 机构证书

机构证书，包括机构单位证书和机构法人证书，用于需要区分、标识、鉴别机构身份的场景，适用于机构身份认证和电子签名，以及数据加密等服务。

3） 设备证书

设备证书，包括各种设备证书和域名证书，用于标识各种设备身份，实现设备身份认证以及交互数据的加解密，保证传输数据的完整性和安全性等。

1.4.2 限制的证书应用

沃通颁发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，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

《沃通通用证书策略》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《沃通通用证书策略》的制订、发布、更新等事宜。

1.5.2 联系人

《沃通通用证书策略》在沃通官网进行发布，对具体个人不另行通知。

官网地址：https://www.wotrus.com/

服务邮箱：casupport@wotrus.com

总机号码：+86-755-8600 8688

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 CP 符合策略的机构

沃通安全策略管理委员会。

1.5.4 CP 批准程序

《沃通通用证书策略》经沃通安全策略管理委员会审批通过后，在沃通公司的官网上对外公布。

《沃通通用证书策略》经沃通安全策略管理委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

1.6 定义和缩写

下列定义适用于《沃通通用证书策略》：

1) 公开密钥基础设施（PKI）Public Key Infrastructure

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。

2) 证书策略（CP）Certification Policy

是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。

3) 电子认证业务规则(CPS) Certification Practice Statement

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

4) 电子认证服务机构（CA）Certification Authority

受用户信任，负责创建和分配公钥证书的权威机构。

5) 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，在某些环境下主动吊销或挂起证书，处理订户吊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）。

6) 数字证书(证书) Digital Certificate

也称公钥证书，由电子认证服务机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

7) 证书吊销列表 (CRL)：Certificate Revocation List

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。

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

一个经电子认证服务机构数字签名的列表，标记已经被吊销的 CA 的公钥证书的列表，表示这些证书已经无效。

9) 私钥 Private Key

非对称密码算法中只能由拥有者使用的不公开密钥。

10）公钥 Public Key

非对称密码算法中可以公开的密钥。

2.信息发布与管理

2.1 信息库

沃通的信息库是一个对外公开的信息库，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：证书、CPS、CP 和 CRL 以及其他不定期发布的信息。

沃通的信息库地址为：https://www.wotrus.com/ca/。

2.2 认证信息的发布

证书状态可以通过沃通提供的在线查询服务获得。

《沃通通用证书策略》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

《沃通通用证书策略》一经网站发布，即时生效。对数字证书的订户及证书申请人均具备约束力。

1） 证书的发布：在证书签发时，沃通通过目录服务器自动将该证书公布。

2） 沃通的 CRL 每 24 小时发布一次。

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，沃通允许公众自行通过网站进行查询和访问。

只有经授权的 RA/CA 管理员可以查询 沃通和注册机构数据库中的其他数据。

3.标识与鉴证

3.1 命名

3.1.1 名称类型

每个订户对应一个甄别名（Distinguished Name，简称 DN）。

数字证书中的主体的 X.500 DN 是 C=CN 命名空间下的 X.500 目录唯一名字。

3.1.2 对名称意义化的要求

订户的甄别名(DN)必须具有一定的代表意义。

证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主体公钥中的公钥绑定的实体信息。

3.1.3 订户的匿名或伪名

不接受或者允许任何匿名或者伪名，仅接受有明确意义的名称作为唯一标识符。

3.1.4 理解不同名称形式的规则

DN 的具体内容依次由 CN、OU、O、C 四部分组成。其中 CN 用来表示用户名，OU、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 CA 认证服务体系中，不同订户的证书主体的名称是唯一的。但对于同一订户，可以用其主体名为其签发多张证书，但证书的扩展项不同。

3.1.6 商标的识别、鉴证和角色

沃通签发的证书不包含任何商标或者可能对其他机构构成侵权的信息。

3.2 初始身份确认

3.2.1 证明持有私钥的方法

通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。在 CA 证书服务体系中，私钥在用户端生成，证书请求信息中包含用私钥进行的数字签名，CA 用其对应的公钥来验证这个签名。

沃通要求证书申请人妥善保管自己的私钥，因此，证书申请人视作其私钥的唯一持有者。

3.2.2 个人身份的鉴别

对于个人订户，沃通或授权的注册机构应验证个人有效身份证件或证件的具体信息，核实个人订户身份的真实性。个人有效身份证件指政府部门签发的证件，包括但不限于：身份证、港澳台居民身份证、户口簿、护照、军官证等。

个人身份的鉴别流程应当明确记录在按照本 CP 制定的 CPS 中。

3.2.3 组织身份的鉴别

对于组织机构订户，沃通或授权的注册机构应验证订户提交的组织有效身份证件或证件的具体信息、组织授予经办人的授权证明和经办人的个人身份证明材料，核实组织订户是合法存在的实体及确认申请人的意愿。组织有效身份证件指政府部门签发的证件或文件，包括但不限于营业执照、组织机构代码证、事业单位登记证、社会团体登记证、政府批文等。如该组织需申请服务器类型的证书，还需向沃通或授权的注册机构提交域名证明文件等方式证明域名的所有权利。

组织身份的鉴别流程应当明确记录在按照本 CP 制定的 CPS 中。

3.2.4 没有验证的订户信息

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。对于没有验证过的订户信息，沃通将对申请信息以书面或电子形式进行归档。沃通将不承诺这类信息的真实性，并且不承担由于这类信息的不真实、不完整等引起的任何责任和解决纠纷的义务。

3.2.5 授权的确认

当申请者代表个人或组织机构申请证书时，需要出示足够的证明信息以证明个人或组织机构是否真实存在，申请者是否已获得个人或组织机构的授权。沃通或授权的注册机构有责任确认该授权信息，并将授权信息妥善保存。

3.2.6 互操作准则

互操作可能是交叉认证、单身交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的 CA 中心之间建立相互信任关系，从而使双方的订户可以实现互相认证。

沃通将根据业务需要，在遵循《沃通通用证书策略》的各项控制要求的基础上，与 CA 的证书服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。但交叉认证并不表示沃通批准了或赋予了其他 CA 中心或电子认证服务机构的权利。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

通用证书的常规密钥更新中，通过订户使用当前私钥对密钥更新请求进行签名，沃通使用订户原有公钥验证确认签名来进行订户身份标识和鉴别。

沃通也可以使用初始身份验证相同的流程进行标识与鉴别。

3.3.2 吊销后密钥更新的标识与鉴别

通用证书吊销后密钥更新中对身份标识和鉴别的要求，使用原始身份验证相同的流程，详见 3.2.2 个人身份的鉴别和 3.2.3 机构身份的鉴别。

3.3.3 证书变更的标识与鉴别

通用证书的证书变更是指订户的证书信息发生变更，申请重新签发一张证书，对原证书进行吊销处理。使用原始身份验证相同的流程，详见 3.2.2 个人身份的鉴别和 3.2.3 机构身份的鉴别。

3.4 吊销请求的标识与鉴别

通用证书订户本人吊销时的身份标识和鉴别使用原始身份验证相同的流程，详见 3.2.2 个人身份的鉴别和 3.2.3 组织身份的鉴别。

如果是因为订户没有履行《沃通通用证书策略》和《沃通电子认证业务规则》所规定的义务，由沃通或授权的注册机构申请吊销订户的证书时，不需要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和具有独立法人资格的组织机构(包括行政机关、事业单位、企业单位、社会团体和人民团体等)。

4.1.2 申请过程与责任

证书申请人按照《沃通通用证书策略》和《沃通电子认证业务规则》所规定的要求，填写证书申请表，并准备相关的身份证明材料，沃通会通过包括人脸识别、银行卡验证、实名手机验证或其他可靠的身份认证方式，对申请人进行实名认证。如果实名认证未通过，沃通将拒绝为申请人发放证书，并将未通过的信息存档。沃通或注册机构依据身份鉴别规范对证书申请人的身份进行鉴别，并决定是否受理申请。

证书申请人应当提供真实、完整和准确的信息，沃通或其注册机构需按 3.2 的要求和流程对申请人身份材料信息进行审查。如证书申请人未向沃通提供真实、完整和准确的信息，或者有其他过错，给沃通或电子签名依赖方造成损失的，由证书申请人承担赔偿责任。一旦通过证书申请者的申请并为其签发证书，无论是否已经接受证书，证书申请者即成为证书订户。订户必须确保本身持有的证书用于申请时预定的目的。

申请过程中各方责任为：

1） 订户

订户需要提供本 CP 3.2 所述的有效身份证明材料，并确保材料真实准确。配合沃通或授权的注册机

构完成对身份信息的采集、记录和审核。

2） 沃通

沃通参照本 CP 3.2 的要求对订户的身份信息进行采集、记录和审核。通过鉴证后，沃通向订户签发证书。如果用户身份信息的鉴别由授权的注册机构完成，沃通应对授权的注册机构进行监督管理和审计。

3） 注册机构

授权的注册机构参照本 CP 3.2 的要求对订户的身份信息进行采集、记录和审核。通过鉴证后，注册机构向沃通提交证书申请，由沃通向订户签发证书。注册机构须接受沃通的监督管理和审计。授权的注册机构应当按照沃通的要求，向沃通提交身份鉴证资料或自行妥善保存。

4） 依赖方

在信任沃通签发的证书时，依赖方需承担如下责任：

a. 依赖方需熟知本文档条款及与证书相关的政策、法规，并了解证书的使用目的及限制。

b. 在信任沃通签发的证书前，依赖方应进行合理审查，包括但不限于：核实证书有效期，查阅沃通公布的有效 CRL 以了解证书状态。沃通认为，依赖方始终遵循上述条款。若依赖方因疏忽或其他原因违反该条款，给沃通造成损失，沃通保留采取相应法律行动的权利。

c. 所有依赖方需承认，信任证书的行为即表明他们已了解并接受本文档的相关规定，包括免责、拒绝和限制义务等条款。

5） 密钥生成器提供者

一旦证书申请者选择了某种密钥生成器，则表明该申请者信赖由其产生的密钥对的安全性和可靠性，沃通并不为此提供任何形式的担保，也没有责任和权力对由此产生的纠纷进行处理。

6） 主管部门

沃通承诺，将严格按照国家的法律法规和主管部门的书面要求提供符合要求的第三方电子认证服务。

4.2. 证书申请处理

4.2.1 执行识别与鉴别功能

沃通和授权的注册机构，有权利和责任对申请者的身份进行合理的鉴别。出于安全性和审计的需要，证书申请表应记录鉴别人的姓名、签名、验证结果和验证日期。

当接收到订户的证书申请后，证书签发机构应完成以下鉴别工作，将其作为向该订户签发证书的先决

条件：

1)确认证书申请者接受订户协议中的各项条款；

2)按照通用证书的要求对证书申请者的身份进行验证；

3)确认证书申请者合法的拥有与证书中所含公钥配对的私钥(如要求订户作出保证等方式)；

4)确认证书中包含的信息，除了未经验证的订户信息外，都是准确的；

5)确认任何受托人在代表其组织机构申请证书时，该受托人已得到了所代表的组织机构的合法授权；

6)确认任何委托办理的各方之间的授权合法性和委托方、受托方的身份。

7)在签发了证书后，除非被通知该证书发生了本文档所述的安全损害情况，否则沃通将不再负有继续监控和调查证书中信息准确性的责任。

沃通保留更新鉴别程序和要求的权利，更新后的鉴别程序和要求将发布在【https://www.wotrus.com】官方网站。

4.2.2 证书申请批准和拒绝

沃通或授权的注册机构根据《沃通通用证书策略》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。

证书申请人通过身份鉴别流程且鉴证结果为合格，沃通或授权的注册机构将批准证书申请，CA 为证书申请人制作并颁发数字证书。

证书申请人未能通过身份鉴证，沃通或授权的注册机构将拒绝申请人的证书申请，并通知申请人鉴证失败，同时向申请人提供失败的原因(法律禁止的除外)。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.3 处理证书申请的时间

沃通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 2 个工作日内处理证书申请。

沃通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沃通的管理要求。

4.3 证书签发

4.3.1 证书签发过程中电子认证服务机构的行为

一旦证书申请者提交了申请，尽管实际上尚未领取证书，但仍视同为申请人已同意发证机构为其签发证书。

沃通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 电子认证服务机构对订户的通知

沃通通过注册机构对证书订户的通告有以下几种方式：

1) 通过面对面的方式，通知订户到注册机构领取数字证书；注册机构把密码信封和证书等直接提交给订户，来通知订户证书信息已经正确生成；
2) 邮政信函或电子邮件通知订户；
3) 订户实名手机号码的短信通知订户；
4) 沃通认为其他安全的方式通知订户。

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，注册机构将数字证书及其密码信封当面、寄送或电子方式给证书申请人，证书申请人从获得数字证书起，就被视为同意接受证书。

4.4.2 电子认证服务机构对证书的发布

沃通在签发完数字证书后，采用数据库或目录服务方式，实现数字证书的存储与发布。对已发布的数字证书，沃通提供证书目录信息查询服务。

查询方式包括但不限于用户在线自助或人工受理等。对于订户查询，沃通核实身份后提供查询服务。对于其他实体查询，为保护证书订户的数据安全和隐私保护，沃通只承诺对其他实体提交的证书进行核实。

4.4.3 电子认证服务机构在颁发证书时对其他实体的通告

沃通采用数据库或目录服务方式对证书进行发布，其他实体可以通过沃通提供的查询方式自行查询。

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沃通所签发的证书后，均视为已经同意遵守与沃通、依赖方有关的权利和义务的条款。只有在此前提下，订户才能使用相应的证书及与之对应的私钥。证书的使用须遵循本文档及相关 CP/CPS 的规定。订户只能在合法的应用范围内使用私钥和证书，且使用行为需符合订户协议的要求，并且在证书到期或被吊销之后，订户必须停止使用该证书对应的私钥。

在使用与沃通签发的证书相关的电子签名及已签署的信息时，各方参与者需遵守本文档规定，享有相应的权利并承担相应的义务。发证机构、证书订户及依赖方均视为已被告知并同意遵守本文档以及相关 CP/CPS 和沃通与各方签署的协议及规范中的条款。任何超出本文档规定的证书及私钥使用，沃通将不承担由此产生的任何后果。

若证书中某些字段明确了证书的使用范围和用途，则该证书仅在此范围内使用。任何超出证书所标明适用范围的行为，均由行为人自行承担责任。沃通对超出适用范围的任何使用行为，不承担相应责任和义务。

4.5.2 依赖方对公钥和证书的使用

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。验证证书的有效性包括：

1) 用 沃通的证书验证证书中的签名，确认该证书是沃通签发的，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) 检验证书有效性，需要检查该证书没有被吊销。

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签名过的数据。

除非本文档另有规定，否则证书不应被视为发证机构对任何权力或特权的承诺。依赖方仅能在本文档

规定的范围内信任证书及其中包含的公钥，并据此作出决策。

若证书中明确了使用范围和目的，则证书仅在此范围内有效。依赖方须作出合理判断，对于超出证书标明适用范围的行为所产生的信任，依赖方需独立承担责任，沃通对此不承担任何责任和义务。

4.6 证书更新

4.6.1 证书更新的情形

证书更新是指在不改变证书中的公钥和其他任何证书包含的信息的情况下，为订户签发一张新证书。证书更新时无需再提交证书注册信息，订户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，使用原证书的私钥对包含公钥的更新申请信息签名。

4.6.2 请求证书更新的实体

只有下列人员可以请求证书更新：

1) 个人证书订户，如果委托他人办理，需要提供明确的授权文件；

2) 机构证书订户被明确授权的代表；

3) 拥有设备证书的个人，拥有设备证书的单位被明确授权的代表。

4.6.3 证书更新请求的处理

证书更新申请者应在证书到期前，按要求向沃通或授权的注册机构提出更新申请。对于证书更新，其处理过程需要确保提出证书更新请求的人是被更新证书所标识的订户，沃通在为其签发新证书时，可以要求更新申请者提交原有私钥签名，或者使用与初始签发证书相同的过程来进行鉴别，鉴别要求同 3.2.3。

通常，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，发证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、唯一性的验证和鉴别。包括：

1) 订户对申请信息进行签名，CA 用其原有证书中的公钥对签名进行验证；

2) 订户注册信息没有发生变化，CA 基于其原有注册信息对其进行签发新的证书。

订户也可以选择一般的初始证书申请流程进行证书更新，按照要求提交相应的证书申请和身份证明资料。沃通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 签发新证书时对订户的通知

同 4.3.2。

4.6.5 构成接受更新证书的行为

同 4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

同 4.4.2。

4.6.7 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

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，沃通提供证书更新时，密钥必须同时更新。

证书更新的具体情形如下：

1) 当订户证书即将到期或已经到期时；

2) 当订户证书密钥遭到损坏时；

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。

4.7.2 请求证书密钥更新的实体

订户可以请求证书密钥更新。订户包括持有 沃通签发的个人、组织及设备等各类证书的证书持有人。

4.7.3 证书密钥更新请求的处理

同 3.3

4.7.4 颁发新证书对订户的通告

同 4.3.2。

4.7.5 构成接受密钥更新证书的行为

同 4.4.1。

4.7.6 电子认证服务机构对密钥更新证书的发布

同 4.4.2。

4.7.7 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4.8 证书变更

4.8.1 证书变更的情形

证书变更是指订户的证书信息发生变更，申请重新签发一张证书，对原证书进行吊销处理。

4.8.2 请求证书变更的实体

订户可以请求证书变更。订户包括持有沃通签发的个人、机构及设备等各类证书的证书持有人。

4.8.3 证书变更请求的处理

同 3.3.3。

4.8.4 颁发新证书对订户的通告

同 4.3.2。

4.8.5 构成接受变更证书的行为

同 4.4.1。

4.8.6 电子认证服务机构对变更证书的发布

同 4.4.2。

4.8.7 电子认证服务机构对其他实体的通告

同 4.4.3。

4.9 证书吊销和挂起

证书吊销包括申请吊销和强制吊销。证书吊销后，订户可以重新向 CA 申请签发新的证书，与初始申请时的流程和要求相同。

目前，沃通不提供证书挂起服务。

4.9.1 证书吊销的情形

1) 发生下列情形之一的，订户应当申请吊销数字证书：
   a. 数字证书私钥泄露；
   b. 数字证书中的信息发生重大变更；
   c. 认为本人不能实际履行本 CP；
   d. 认为当前密钥管理方式的安全性得不到保证。
2) 发生下列情形之一的，沃通可以吊销其签发的数字证书：
   a. 订户提供的信息不真实；
   b. 和订户达成的协议已经终止；

c. 证书机构、企事业单位或其他社会性团体等组织为其员工申请的证书，若该员工已不再隶属于该组织；

d. 与授权注册机构签订的协议终止或者发生改变；

e. 订户没有履行双方合同规定的义务，或违反本 CP；

f. 在确认域名失去合法性后，例如法院裁定该域名违法、域名注册合同期满或域名注册商已终止对申请人的授权等情况下；

g. 数字证书的安全性得不到保证；

h. 法律、行政法规规定的其他情形。

4.9.2 请求证书吊销的实体

根据不同的情况，订户、沃通、注册机构可以请求吊销最终用户证书。

4.9.3 吊销请求的流程

证书吊销请求的处理采用与原始证书签发相同的过程。

1) 证书吊销的申请人到沃通或授权的注册机构书面或在线提交《证书吊销申请表》，并注明吊销原因；

2) 沃通或授权的注册机构根据 3.2 的要求对订户提交的吊销请求进行审核；

3) 沃通吊销订户证书后，注册机构将通知订户证书被吊销，订户证书在 24 小时内进入 CRL，向外界公布；

4) 强制吊销是指当沃通或授权的注册机构确认用户违反本 CP 4.9. 1）b 的情况发生时，对订户证书进行强制吊销。吊销后将通过官网公告、注册机构或其他安全可行的方式通告订户。

4.9.4 吊销请求宽限期

如果出现证书私钥泄露等事件，吊销请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他吊销原因的吊销请求必须在 48 小时内提出。

4.9.5 电子认证服务机构处理吊销请求的时限

注册机构接到吊销请求后立即处理，24 小时生效。沃通每日签发一次 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(version)

2) 签名算法标识符(signature)

3) 颁发者名称(issuer)

4) 本次更新(this update)

5) 下次更新(next update)

6) 用户证书序列号/吊销日期(user certificate/revocation date)

7) 签名算法(signature algorithm)

8) 签名(signature value)

4.9.6 依赖方检查证书吊销的要求

在具体应用中，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，通过目录服务器提供的查询系统，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) ：服务系统接受证书状态查询请求，从目录服务器中查询证书的状态，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，确保是经沃通发布并且签名的。

4.9.7 CRL 的颁发频率

沃通可采用实时或定期的方式发布 CRL。颁发 CRL 的频率根据证书策略确定，一般为 24 小时定期发布。

4.9.8 CRL 发布的最长滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.10 证书状态服务

4.10.1 操作特点

证书状态可以通过沃通提供的在线查询服务获得。

4.10.2 服务可用性

提供 7X24 小时的证书状态查询服务。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，沃通可以提供以下通知服务：

1） 收到证书主题的电子签名消息的接受者要求，确认该证书是否已被吊销；

2） 提供通知服务，当指定的证书被吊销时，沃通将通知请求该项服务的请求者。

4.11 订购结束

订购结束是指当证书有效期满或证书吊销后，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，证书被吊销后，即订购结束。

4.12 密钥生成、备份与恢复

4.12.1 密钥生成、备份与恢复的策略与行为

个人和机构订户的签名密钥对由订户的密码设备（如：智能 USB KEY 或智能 IC 卡）生成，加密密钥对由密钥管理中心生成。

个人和机构证书密钥恢复是指加密密钥的恢复，密钥管理中心不负责签名密钥的恢复。密钥恢复分为两类：订户密钥恢复和司法取证密钥恢复。

4.12.2 会话密钥的封装与恢复的策略与行为

非对称算法组织数字信封的方式来封装会话密钥。数字信封使用信息接受者的公钥对会话密钥加密，接受者用自己的私钥解开并恢复会话密钥。

5. 电子认证服务机构设施、管理和操作控制

本章规定参见沃通已发布的 CPS。

6. 认证系统技术安全控制

6.1 密钥对的生成和安装

密钥对是电子签名安全机制的关键，本文档制订了相应的规定，确保密钥对的产生、传送、安装等具备保密性、完整性和不可否认性。

6.1.1 密钥对的产生

CA 系统和 RA 系统的密钥对是在密码机内部产生，密码机应具有商用密码产品认证证书。在生成 CA 密钥对时，沃通按照密码机密钥管理制度，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，密钥管理员凭借智能 IC 卡对密钥进行控制。

6.1.2 私钥传送给订户

订户的签名密钥对由自己的密码设备生成并保管。加密密钥对由密钥管理中心产生，通过安全通道传到订户手中的密码设备中。

6.1.3 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到沃通。

从 RA 到 CA 以及从密钥管理中心到 CA 的传递过程中，采用国家密码主管部门许可的通讯协议及密钥算法，保证了传输中数据的安全。

6.1.4 电子认证服务机构公钥传送给依赖方

依赖方可以从沃通公司的网站(https://www.wotrus.com/ca/)下载根证书和 CA 证书，从而得到 CA 的公钥。

6.1.5 密钥的长度

密钥算法和长度符合国家密码主管部门的规定。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码主管部门许可的加密设备生成。对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均符合国家密码主管部门要求。

6.1.7 密钥使用目的

订户的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥对可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

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

沃通所用的密码设备都是经国家相关部门认可的产品，其安全性达到以下要求：

1) 接口安全：不执行规定命令以外的任何命令和操作；

2) 协议安全：所有命令的任意组合，不能得到私钥的明文；

3) 密钥安全：密钥的生成和使用必须在硬件密码设备中完成；

4) 物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

6.2.2 私钥的多人控制

CA 证书的私钥的生成、更新、吊销、备份和恢复等操作采用多人控制机制，即采取“五选三”方式，将私钥的管理权限分散到 5 张管理员卡中，只有其中超过半数以上管理员在场并许可的情况下，才能对私钥进行上述操作。

订户的私钥由订户自己通过密码设备控制。

6.2.3 私钥托管

订户加密证书对应的私钥由密钥管理中心托管，订户的签名证书对应的私钥由自己保管，密钥管理中心不负责托管。

密钥管理中心严格保证订户密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。

6.2.4 私钥备份

沃通和密钥管理中心不备份订户的签名密钥。

加密私钥由密钥管理中心备份，备份数据以密文形式存在。

6.2.5 私钥归档

订户加密密钥对的归档是将已过生命周期或决定暂不使用的加密密钥以密文形式保存在数据库中，并通过数据库备份出来进行归档保存，归档后的密钥形成历史信息链，供查询或恢复。

6.2.6 私钥导入或导出密码模块

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。

沃通不提供订户私钥从密码设备或密码模块中导出的方法。

6.2.7 私钥在密码模块的存储

私钥在国家密码主管部门批准和认可的密码设备及密码模块中存储。

6.2.8 激活私钥的方法

对于 CA 私钥，具有激活私钥权限的管理员使用含有自己的身份的加密 IC 卡登录，启动密钥管理程序，进行激活私钥的操作，需要超过半数以上管理员同时在场。

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加密 IC 卡登录，启动密钥管理程序，进行解除私钥的操作，需要超过半数以上管理员同时在场。

6.2.10 销毁密钥的方法

对于 CA 私钥，具有销毁密钥权限的管理员使用含有自己的身份的加密 IC 卡登录，启动密钥管理程序，进行销毁密钥的操作，需要超过半数以上管理员同时在场。

6.2.11 密码模块的评估

沃通使用国家密码主管部门批准和许可的密码产品，接受其颁布的各类标准、规范、评估结果、评价证书等各类要求，根据沃通对产品性能、工作效率、供应厂商的资质等方面的条件，选择所需要的模块。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

订户证书中的公钥包括签名证书中的公钥和加密证书中的公钥。它们由沃通和密钥管理中心定期归档。

6.3.2 证书操作期和密钥对使用期限

所有订户证书的有效期和其对应的密钥对的有效期都是一致的。

6.4 激活数据

6.4.1 激活数据的产生和安装

激活数据是私钥保护密码，通用证书存储介质（如：智能 KEY)出厂时设置了缺省的 PIN 值，证书制作时将此 PIN 值在安全可靠的环境下随机产生。所有的 PIN 值都应该是不容易被猜到的，从而激活了证书存储介质的 PIN。

PIN 值的生成规则应该遵循以下几个原则：

1) 至少 8 位字符；

2) 至少包含一个字符和一个数字；

3) 至少包含一个小写字母；

4) 不能包含很多相同的字符；

5) 不能和操作员的名字相同；

6) 不能使用生日、电话等数字；

7) 用户名信息中的较长的子字符串。

6.4.2 激活数据的保护

通用证书的激活数据，必须将激活数据按照可靠的方式分割后由不同的可信人员掌管，而且掌管人员必须符合职责分割的要求。

如果证书订户使用口令或 PIN 码保护私钥，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户也应注意防止其生物特征被人非法获取。同时，为了配合业务系统的安全需要，应该经常对激活数据进行修改。

6.4.3 激活数据的其他方面

只有在拥有证书介质并知道通用证书介质的 PIN 值时才能激活证书存储介质，进而使用私钥。当私钥的激活数据进行传送时，应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

当私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢失、偷窃、泄露或 非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或全部， 比如记录有口令的在纸页必须粉碎。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

为了保证系统的正常运行，对所需要的计算机设备进行正确的选型、验收，制定操作规范。另外，本系统采用增加冗余资源的方法，使系统在有故障时仍能正常工作。

对于设备有一套完整的保管和维护制度：

1) 专人负责设备的领取和保管，做好设备的领用、进出库和报废登记。

2) 对设备定期进行检查、清洁和保养维护。

3) 制定设备维修计划，建立满足正常运转最低要求的易损坏备件库。

4) 对设备进行维修时，必须记录维修的对象、故障原因、排除方法、主要维修过程及与维修有关的情况等。

5) 设备维修时，必须有派专人在场监督。

6.5.2 计算机安全评估

CA 系统及其运行环境通过了国家密码管理局和工信部的审查，并取得了相应资质。

CA 系统使用的网络设备、主机、系统软件等均取得了国家有关认证检测机构出具安全标准的凭证。

6.6 生命周期技术控制

6.6.1 系统开发控制

系统开发采用先进的安全控制理念，同时应兼顾开发环境的安全、开发人员的安全、产品维护期的配置管理安全。系统设计和开发运用软件工程的方法，做到系统的模块化和层次化，系统的容错设计采用多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

6.6.2 安全管理控制

沃通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 生命周期的安全控制

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通过了主管部门鉴定，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。

6.7 网络的安全控制

系统网络安全的主要目标是保障网络基础设施、主机系统、应用系统及数据库运行的安全。沃通采取防火墙、病毒防治、入侵检测、漏洞扫描、数据备份、灾难恢复等安全防护措施。

6.8 时间戳

时间戳系统提供的时间戳服务在技术实现上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，时间源采用国家授时中心提供的标准时间。

7. 证书、证书吊销列表和在线证书状态协议

7.1 证书

沃通签发的证书符合国家相关标准的要求，遵循 RFC5280 等技术标准。

7.1.1 版本号

X.509 V3。

7.1.2 算法对象标识符

符合国家密码主管部门批准的算法对象标识符。

7.1.3 名称形式

CA 数字证书中的主体 Subject 的 X.500 DN 是 C=CN 命名空间下的 X.500 目录唯一名字，各属性的编码一律使用 UTF8String。

主体 Subject 的 X.500 DN 支持多级 O 和 OU，其格式如：“C=CN,O=XX,O=XX,OU=XX,OU=XX,CN=XX”。

1) C (Country) 应为 CN ，表示中国；

2) O (Organization) 中的内容分为 2 种：

a. 证书主体或者证书主体所属单位具有明确的上一级单位，则应为其上一级单位的名称全称；

b. 不存在 a ）中所述的上一级单位，则应为证书主体或者证书主体所属单位的所在省、 自治区、直辖市名称全称；

3) OU (Organization Unit) 应为证书主体或者证书主体所属单位的名称全称；

4) CN (Common Name) 中的内容分为 4 种：

a. 个人证书中应为证书主体的姓名；

b. 单位机构证书中应为证书主体单位的标准名称或简称；

c. 服务器证书应为证书主体设备的域名或者 IP 地址或者设备编码；

d. 代码签名证书应为负责人的姓名，或者是所属单位的标准简称；

5) Email 仅在邮件证书的 DN 中存在，应为证书主体的有效电子邮件地址。

沃通签发的证书，其识别名称不允许为匿名或者伪名，必须是有确定含义的识别名称。

7.1.4 证书扩展项

沃通除了使用 IETF RFC 5280 中定义的证书标准项和标准扩展项以外，还使用了沃通私有的自定义扩展项。

采用的 IETF RFC 5280 中定义的证书扩展项如下：

1) 颁发机构密钥标识符 Authority Key Identifier

2) 主体密钥标识符 Subject Key Identifier

3) 密钥用法 Key Usage

4) 扩展密钥用途 Extended Key Usage

5) 主体可选替换名称 Subject Alternative Name

6) 基本限制 Basic Constraints

7） 证书吊销列表分发点 CRL Distribution Points

沃通私有定义扩展项如下：

1） 个人身份证号码 Identify Card Number

2） 营业执照（统一社会信用代码）IC Registration Number

3） 签名证据项：Signature Evidences ，应包含签名相关证据内容，如声音、图像等。

7.2 证书吊销列表

沃通签发的证书吊销列表符合 X.509 V2 格式。遵循 RFC5280 标准。

7.2.1 版本号

X.509 V2。

7.2.2CRL 和 CRL 条目扩展项

不使用 CRL 扩展项。

7.3 在线证书状态协议

7.3.1 版本号

RFC2560 定义的 OCSPV1 版本。

7.3.2 OCSP 扩展项

不使用 OCSP 扩展项。

8. 电子认证服务机构审计和其他评估

8.1 评估的频率和情形

审计是为了检查、确认 CA 是否按照《沃通通用证书策略》和《沃通电子认证业务规则》及其管理制度和安全策略开展业务，发现存在的可能风险。根据工作需要，定期组织开展审计评估。

8.2 评估者的资质

内部审计人员由沃通内部人员组成，外部审计的审计人员的资质由第三方确定。

8.3 评估者与被评估者之间的关系

评估者与被评估者应无任何业务、财务往来或其它利害关系，足以影响评估的客观性。

8.4 评估的内容

审计所涵盖的主题包括：人事、机房物理安全、安全运营管理、密钥安全和运行服务、客户服务等内容。

8.5 对问题与不足采取的措施

对审计中发现的问题，沃通将根据审计报告的内容准备一份解决方案，明确对此采取的行动。沃通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

除非法律明确要求，沃通一般不公开评估结果。

对 CA 关联方，沃通将依据签署的协议来公布评估结果。

9. 法律责任和其他业务条款

本章规定参见沃通发布的正式 CPS 文件。