沃通电子认证服务有限公司
电子政务电子认证业务规则

版本：1.2

发布日期：2024 年 3 月 7 日

生效日期：2024 年 3 月 7 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	主要修改说明	审核/批准人	生效时间
1.0	版本发布	初始版本。	沃通安全策略管理委员会	2019 年7 月22 日
1.1	版本发布	按照《电子政务电子认证服务能力评估问题反馈》，对CPS 进行修订与完善。	沃通安全策略管理委员会	2020 年4 月17 日
1.2	版本发布	修订证书业务规则。	沃通安全策略管理委员会	2024 年 3 月 7 日

声明

沃通电子政务电子认证服务业务规则（以下简称 CPS），是沃通电子认证服务有限公司开展电子政务电子认证服务时提供的服务内容、遵循的操作流程、系统的管理规范、相应技术规范以及相关法律责任与关系。

本 CPS 根据服务范围和用户需要，在适当范围内进行公布。

本 CPS 符合国家密码管理局相关规定和规范的要求，并向国家密码管理局进行备案。

目 录

1.概括性描述

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”），是权威、公正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》、《中华人民共和国密码法》和《商用密码管理条例》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应用安全解决方案，为电子政务构建安全、可靠的信任环境。

本文档《沃通电子认证服务有限公司电子政务电子认证业务规则》（以下简称《沃通电子政务电子认证业务规则》），是按照国家密码管理局《商用密码管理条例》的要求，依据《电子政务电子认证服务业务规则规范》制定，并报国家密码管理局备案。

《沃通电子政务电子认证业务规则》详细阐述了沃通公司在实际工作和运行中所遵循的各项规范。《沃通电子政务电子认证业务规则》适用于沃通公司及其员工、注册机构、证书申请人、订户和依赖方，各参与方必须完整地理解和执行《沃通电子政务电子认证业务规则》所规定的条款，并承担相应的责任和义务。

1.2 文档名称与标识

本文档名称为《沃通电子认证服务有限公司电子政务电子认证业务规则》，该文档没有分配对象标识符。

1.3 电子政务电子认证业务范围

电子政务电子认证业务范围包括面向政务部门、企事业单位、社会团体和社会公众的电子政务电子认证服务。

1.4 电子政务电子认证活动参与方及其职责

1.4.1 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》、《中华人民共和国密码法》及《商用密码管理条例》规定，依法设立的电子政务电子认证服务机构（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。

1.4.2 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授权的注册机构，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授权的注册机构，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。

1.4.3 订户

订户是指向沃通申请数字证书的实体。

1.4.4 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。

1.4.5 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。

1.5 电子政务电子认证业务规范

1.5.1 适合的证书应用

沃通签发的数字证书适合应用在企业信息化和电子政务领域，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，为各级政务部门的工作人员和参与电子政务业务的社会公众颁发的个人用户证书，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，为政务机关和参与电子政务业务的企事业单位、社会团体或其他组织颁发的机构单位证书或机构法人证书，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，为电子政务中的服务器或设备颁发的设备证书或域名证书，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。

4） 事件型证书

沃通公司面向签名行为业务场景签发出的数字证书。在业务过程中，根据订户提交的业务场景中相关信息（电子文档、签名行为特征信息、手写笔迹或其他签名行为证据信息等）自动固化至数字证书的扩展域，签发出事件型数字证书。

事件型数字证书所对应的私钥为一次性使用，对业务场景的信息数据进行电子签名，在使用后即被销毁。

5） 其他类型证书

为满足电子政务相关应用的特殊需求而提供的其他应用类型的证书，如：时间戳证书、代码签名证书等。

以上各类数字证书格式符合《电子政务数字证书格式规范》的要求，在标识实体名称时，应保证实体身份的唯一性，且名称类型应支持 X.500、RFC-822、X.400 等标准协议格式。

1.5.2 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。

1.5.3 正式证书和测试证书

沃通提供上述证书类型相对应的正式证书和测试证书：

1） 正式证书的申请者必须通过规定的物理身份认证和沃通需要的鉴别程序。

2） 测试证书申请者不需要经过身份鉴别，有效期一般不超过 3 个月。测试证书只能用于测试证书对于应用系统的适应性，以及实现证书应用目的的技术可行性，不能用于任何正式的用途。

无论是正式证书还是测试证书，凡是涉及证书签发、申请、受理、操作、管理、使用的单位和个人，

应熟悉沃通证书策略中的术语、条件、需求、建议以及权益等内容。

1.6 电子政务电子认证策略管理

1.6.1 策略文档管理机构

《沃通电子政务电子认证业务规则》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《沃通电子政务电子认证业务规则》的制订、发布、更新等事宜。

《沃通电子政务电子认证业务规则》由沃通电子认证服务有限公司拥有完全版权。

1.6.2 联系人

《沃通电子政务电子认证业务规则》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

1.6.3 决定 CPS 符合策略的机构

沃通安全策略管理委员会。

1.6.4 CPS 批准程序

《沃通电子政务电子认证业务规则》由沃通安全策略管理委员会组织编写，编写完成后，由沃通安全策略管理委员会进行审批，审批通过后，在沃通公司的官网上对外公布。

《沃通电子政务电子认证业务规则》经沃通安全策略委员会审批通过后，从对外公布之日起三十日之内向国家密码管理局备案。

1.7 定义与缩写

下列定义适用于《沃通电子政务电子认证业务规则》 ：

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) 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。

3) 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。

4) 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）。

5) 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。

6) 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。

7) 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。

8) 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。

9) 公钥 Public Key

非对称密码算法中可以公开的密钥。

10) 安全授权认证 Secure Authorization

安全授权认证是指通过口令、短信验证码、生物识别信息、数字证书等认证凭证对其订户身份进行核验，同时作为订户对其私钥的控制的激活数据。

11）身份标识（ID）Identity

应用中的身份标识号码，也称为序列号或账号，是某个应用中相对唯一的编码，在应用中相当于是一种“身份标识”，身份标识号一般是不变的，至于用什么来标识该“身份标识”，则由证书应用机构自己制定的规则来确定。

2. 信息发布与信息管理

2.1 认证信息的发布

《沃通电子政务电子认证业务规则》发布在沃通公司的网站上（https://www.wotrus.com/ca/），供相关方下载、查阅。

沃通的信息库面向订户及依赖方提供信息服务。提供的信息服务包括但不限于以下内容：证书、CPS 、CP 以及沃通公司不定期发布的信息。

2.2 发布的时间或频率

《沃通电子政务电子认证业务规则》一经网站发布，即时生效。

2.3 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. 身份标识与鉴证

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。

个人证书的甄别名通常可包含个人的真实名称或者证件号码，作为标识订户的关键信息被认证。

机构证书的甄别名通常包含机构名称或机构的证件号码，作为标识订户的关键信息被认证。

设备证书的甄别名通常包含订户所拥有的域名或者外网 IP ，结合该订户的其他信息一起被鉴别和认证。

事件型证书的甄别名通常包含业务场景的相关数据信息，包括但不限于业务场景中的实体名称信息、笔迹信息、电子数据信息以及其他场景信息。

3.1.3 订户的匿名或伪名

沃通不接受任何匿名或者允许伪名，仅接受有明确意义的名称作为证书名称，能够明确标识订户的真实身份。

3.1.4 理解不同名称形式的规则

甄别名（DN）的内容一般由 CN 、OU 、O 、C 等部分组成，具体的命名规则详见本 CPS 7.1.3 名称形式。

3.1.5 名称的唯一性

在沃通的证书服务体系中，证书主体名称必须是唯一的。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 商标的承认、鉴别和角色

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 证明拥有私钥的方法

通过证书请求中所包含的电子签名来证明证书申请人持有与注册公钥对应的私钥。沃通在签发证书前，系统将自动使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断证书使用者拥有私钥。

3.2.2 个人身份的鉴别

对于个人订户身份的鉴别，沃通或授权的注册机构根据不同应用场景，支持不同的身份鉴别方式。鉴别审核批准后，沃通或授权的注册机构按照相关法律法规的要求妥善保存订户申请材料，沃通保存订户申请材料可以是纸质或电子数据形式。

本 CPS 简要说明了不同的个人身份鉴别方式。沃通公司保留根据最新国家政策法规的要求更新个人身份鉴别方法与流程的权利。

1） 订户身份实名鉴别

沃通或授权的注册机构对个人订户的实名身份信息进行核实鉴别，根据鉴别结果签发证书。实名鉴别的证明适用于各类数字证书应用场景，用于证明订户进行的身份认证和电子签名。

对于个人订户实名身份的鉴别，沃通或授权的注册机构将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。

鉴别方式可以采用面对面现场鉴别或远程鉴别。必要时，可以通过权威第三方数据库信息比对、手机短信验证等其他可靠的方式鉴别。

2） 订户身份简易鉴别

当业务场景需要时，沃通可以采取简易鉴别方式。简易鉴别方式下，沃通或授权的注册机构，仅登记订户提交的姓名与证件号码信息，为事后确认宜收集或记录订户的其他身份信息，如人像照片、指纹等。沃通根据登记结果签发证书。

简易鉴别方式下签发的证书，适用于对身份真实性证明和责任认定要求不高的应用场景。沃通或授权的注册机构应保证如实登记了订户提交的信息，保证所签发证书中记录的信息与订户提交的信息一致。订户应提供真实、完整和准确的身份信息，承担因信息有误导致沃通或依赖方遭受损失的赔偿责任。

沃通在证书甄别名（DN）中标识 OU=身份登记，以向依赖方明示此证书采取了身份登记式的简易鉴别。依赖方在依赖证书验证电子签名时，应参考自身的业务风险程度，评估是否应当信赖简易鉴别证书认证的身份信息。沃通不承担因订户过错导致损失的赔偿责任。

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需要鉴别：

1) 订户提交的组织身份信息。鉴别方法包括核对订户提交的组织有效身份证件或证件的具体信息。必要时可以通过权威第三方数据库对身份证件信息进行比对。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。
2) 组织授予经办人的授权证明。鉴别方法包括但不限于验证组织或组织的法定代表人授权给经办人办理证书事宜的授权文件或授权条款，也可以通过银行对公账户打款附言或法定代表人手机短信验证方式核实。
3) 经办人的个人身份证明材料。
4) 如该组织需申请服务器类型的证书，需域名使用权证明材料。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。

鉴别方式可以采用面对面现场鉴别或远程鉴别。当沃通或授权的注册机构认为有需要时，可以增加其他方式，包括但不限于鉴别组织的法定代表人身份或要求经办人提交法定代表人有效身份证件证明。

鉴别审核批准后，沃通或授权的注册机构按照相关法律法规的要求妥善保存订户申请材料，沃通保存订户申请材料可以是纸质或电子数据形式。

本 CPS 简要说明了如何进行组织身份鉴别。沃通公司保留根据最新国家政策法规的要求更新组织身份鉴别方法与流程的权利。

3.2.4 政府部门内设机构及个人的身份鉴别

沃通在给政府部门内设机构或公务人员发放证书时，沃通或授权的注册机构可以按政府部门及政务相关机构提供证书用户发放清单或提供证书发放用户库作为证书的申请依据，通过短信验证码、对公邮箱或公安部身份证库等辅助手段来验证用户身份真实性，并作出批准申请或拒绝申请的操作。

审核批准后，沃通或授权的注册机构按照相关法律法规的要求妥善保存该申请材料，同时确保电子数据具备不可篡改和抗抵赖性。

3.2.5 事件型证书订户身份的鉴别

事件型证书订户身份的鉴别参照个人或组织身份鉴别方法进行鉴别，也可以采取包括录音、录像、可信数据源等有效的身份核验方式进行自动鉴别。

3.2.6 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。

3.2.7 授权的确认

个人在沃通的数字证书申请表上写明代办人的身份信息并签名确认或采用其他安全有效方式体现申请人真实意愿的方式，则证明本人对代办人的授权确认。

代表组织获取数字证书，需要出具组织授权其该组织为办理 CA 数字证书事宜的授权文件。组织在沃通的数字证书申请表上加盖单位公章或采用其他安全有效方式体现申请机构真实意愿的方式，则证明本组织对办理人的授权确认。

3.2.8 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，在遵循本 CPS 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 密钥更新请求的身份标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

证书常规密钥更新中，证书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。

事件型证书没有密钥更新。

3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后的密钥更新等同于订户重新申请证书，其要求与本 CPS 3.2 相同。

3.3.3 证书变更的标识与鉴别

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。

证书变更的标识与鉴别使用初始身份验证相同的流程，其要求与本 CPS 3.2 相同。

事件型证书没有证书变更。

3.4 吊销请求的标识与鉴别

证书吊销请求的标识与鉴别使用初始身份验证相同的流程，其要求与本 CPS 3.2 相同。

如果是因为订户没有履行《沃通证书策略》和《沃通电子政务电子认证业务规则》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《沃通电子政务电子认证业务规则》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。沃通或授权的注册机构应明确告知证书用户所需承担的相关责任和义务，证书申请人表达申请证书的意愿后，沃通或授权的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。

1) **订户：**订户需要提供本 CPS 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 CPS 3.2 的要求对订户的身份信息进行采集、记录、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 CPS 3.2 的要求对订户的身份信息进行采集、记录、审核。通过鉴证后，授权的注册机构向沃通提交证书申请，由沃通向订户签发证书。授权的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。

证书申请人应当提供真实、完整和准确的信息，沃通或其授权的注册机构须按本 CPS 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。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

沃通或授权的注册机构按照《沃通电子政务电子认证业务规则》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 3.2 初始身份确认。

4.2.2 证书申请批准和拒绝

沃通或授权的注册机构根据《沃通电子政务电子认证业务规则》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《沃通电子政务电子认证业务规则》所规定的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，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。

在必要时沃通有权复核授权的注册机构提交的订户申请材料，并有权拒绝不符合本 CPS 的高风险申请。

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，一旦授权的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或授权的注册机构的管理要求。

事件型证书申请为即时处理。

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

沃通通过授权的注册机构对通用证书订户的通告有以下几种方式：

1) 通过面对面的方式，通知订户到授权的注册机构领取数字证书；授权的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。

对于事件型证书，订户成功完成电子签名，即视为沃通证书签发成功，沃通不再就证书签发向订户进行其他方式的通告。

4.4 证书接受

4.4.1 构成接受证书的行为

通用证书签发完成后，授权的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。

事件型证书签发完成后，将证书应用于对应的电子签名时起，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并提供查询服务。

对已发布的数字证书，沃通提供不同方式的证书相关信息查询服务，供订户和依赖方查询。查询方式包括但不限于用户在线自助或人工受理等，具体方式选择由沃通根据证书应用需求选择提供。

对于查询服务中可能涉及订户自身信息或其他个人信息的，沃通可以采取匿名化等方式处理，订户授权同意公开或法律、行政法规规定应当公开的除外。

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 订户私钥和证书的使用

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。

通用证书订户接受到数字证书，应妥善保存其证书对应的私钥。

事件型证书仅应用于订户对应的电子签名行为，订户只能在该次电子签名中使用私钥和证书。私钥将在完成本次电子签名数学运算后进行销毁，之后订户须停止使用该证书对应的私钥。

订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了相关证书之后才能使用对应的私钥，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。

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) 检验通用证书有效性，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。

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。

事件型证书仅用于业务场景的一次性的电子签名，不提供证书变更服务。

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 颁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。

事件型证书私钥在使用一次后即被销毁，不存在证书更新与密钥更新的情况。

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动，从而申请重新颁发一张新证书，并对原证书实施吊销措施。事件型证书不提供证书变更服务。

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、组织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 电子认证服务机构在颁发证书时对其他实体的通告

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《沃通电子政务电子认证业务规则》；

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. 与授权的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 CPS；

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。

事件型证书仅用于订户特定一次的电子签名行为，密钥在使用过一次后即销毁，不提供证书撤销和挂起服务。

4.9.2 请求证书吊销的实体

根据不同的情况下列实体能够要求撤销证书：

1) 订户、订户授权代表及订户证书费用垫付商；

2) 沃通或授权的注册机构；

3) 法院、政府主管部门及其他公权力部门。

只有沃通可以撤销根证书或者子 CA 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，并注明吊销原因；

2) 沃通或授权的注册机构根据本 CPS 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，授权的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；

强制吊销是指当沃通或授权的注册机构确认用户违反本 CPS 4.9.1 2)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、授权的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

授权的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。

4.9.9 吊销信息的其他发布形式

证书吊销信息通过 CRL 服务方式发布，予以公告。

沃通还可以采取官网通知的方式公告。

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。

事件型证书订购结束是指当订户使用数字证书完成电子签名后，该证书的服务时间结束。

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

通用证书（个人或机构)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。

通用证书（个人或机构）的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。

1) 订户密钥恢复：当订户的密钥损坏或丢失后，某些密文数据将无法还原，此时订户可申请密钥恢复。订户在沃通或授权的注册机构申请，经审核后，通过沃通向密钥管理中心请求；密钥恢复模块接受订户的恢复请求，恢复订户的密钥并下载于订户证书载体中。

2) 司法取证密钥恢复：司法取证人员在密钥管理中心申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

事件型证书的签名密钥由签名设备生成密钥并执行签名后，即时销毁。事件型证书的加密密钥对由密钥管理中心生成。

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

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按照下列标准实施：

1) GB 50174-93：《电子计算机机房设计规范》
2) GB 2887-89：《计算站场地技术条件》
3) GB 9361-88：《计算站场地安全要求》
4) GB 6650-1986：《计算机机房用活动地板技术条件》
5) GB 50034-1992：《工业企业照明设计标准》
6) GB 5054-95：《低压配电装置及线路设计规范》
7) GBJ 19-87：《采暖通风与空气调节设计规范》
8) GB 157：《建筑防雷设计规范》
9) GBJ 79-85：《工业企业通信接地设计规范》

CA 机房位于中国深圳市南山区南海大道 1057 号科技大厦二期 A 栋 502 内自建的 CA 机房，实行分层访问的安全管理。

CA 机房的功能区域划分为六个层次，四个区域。

六个层次由外到里分别是：入口、办公、敏感、数据中心、屏蔽机房、保密机柜。

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

为了保证机房系统的安全，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，能防止非法的进入。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、长时间不关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 机房的要求按照相关管理规定要求，并每年定期对物理系统的安全状态进行检查。

5.1.4 水患防治

机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

CA 机房的系统有充分保障，能够防止水侵蚀。

目前机房内无上下水系统，空调间做了严格防水处理，由漏水检测系统提供（7X24）实时检测。

5.1.5 火灾防护和保护

火灾预防和保护策略：

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水喷淋灭火装置。CA 机房内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室。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，吊顶的耐火极限不得低于 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。紧急出口门外部不能有门开启的装置，且紧急出口门须与门禁报警设备联动外，需装配独立的报警设备。
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。
8) 灭火系统采用电动，手动，紧急启动三种方式。
    a. 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，切断非消防电源（如：空调电源、照明电源等）。并送排风（烟），防火阀关闭。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。
    b. 手动方式：人员对钢瓶或药剂瓶直接开启操作。
    c. 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，介质存储地点和 CA 机房系统分开并且保证物理安

全，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的期限已满时，应当将这些数据进行销毁。写在纸张之上的，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。

5.1.8 异地备份

CA 主机房位于中国深圳市南山区南海大道 1057 号科技大厦二期 A 栋 502，异地备份位于北京市朝阳区酒仙桥路 6 号院电子城国际电子总部 B 座 4 层，主机房的电子认证数据实时传输到容灾备份中心，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、授权的注册机构、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。

可信角色包括但不仅限于以下几类：

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

证书业务管理员对授权的注册机构操作员进行管理，并对授权的注册机构业务进行管理。

5.2.2 每个角色的识别与鉴别

所有沃通的在职人员，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，进入系统需要使用数字证书进行身份鉴别。沃通将独立完整地记录其所有的操作行为。

5.2.3 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，即沃通的可信角色由不同的人担任。

至少两个人以上才能使用一项对参加操作人员保密的密钥分割和合成技术，来进行任何密钥恢复的操作。

5.3 人员控制

5.3.1 资格、经历和无过失要求

所有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，具体要求在人事管理制度中规定。沃通要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热忱度、无影响沃通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

沃通与有关的政府部门和调查机构合作，完成对沃通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 培训与考核要求

沃通对运营人员按照其岗位和角色安排不同的培训。培训有：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沃通组织培训与考核。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。

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，每年至少接受沃通组织的培训一次。

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，沃通将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

当沃通员工被怀疑，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，沃通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

对不属于沃通内部的工作人员，但从事 CA 有关业务的人员等独立签约者（如：授权的注册机构的工作人员），沃通的统一要求如下：

1） 正规劳务公司派遣人员；

2） 具有相关业务的工作经验；

3） 必须接受 CA 组织的岗前培训。

5.3.8 提供给员工的文档

为使得系统正常运行，沃通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

沃通记录与系统相关的事件，这些记录信息称为日志。对于这些日志，无论其载体是纸张还是电子文档的形式，必须包含事件发生的日期、事件的发生时间段、事件的内容和事件相关的实体等。

沃通还可能记录与系统不直接相关的事件，例如：物理通道参观记录、人事变动等。

5.4.2 处理或归档日志的周期

沃通建有 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。

5.4.3 审计日志的保存期限

对企事业单位、社会团体、社会公众的电子政务电子认证服务审计日志至少保存到证书失效后五年；对政务部门的电子政务电子认证服务审计日志至少保存到证书失效后十年，法律法规另有规定的，按照相关法律法规执行。

5.4.4 审计日志的保护

沃通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，按照策略进行备份。

5.4.6 审计日志收集系统

审计日志收集系统涉及证书受理过程中的各阶段业务处理日志信息以及 Web 服务程序、网络安全等信息日志记录。

沃通使用审计工具满足对上述日志信息审计的各项要求。

5.4.7 对导致事件实体的通告

沃通发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，沃通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。

沃通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

沃通每年对系统进行漏洞扫描和渗透测试等脆弱性评估，以降低系统运行的风险。

5.5 记录归档

5.5.1 归档记录的类型

归档记录包括但不仅限于所有审计数据、员工资料、证书系统建设和升级文档、证书申请信息、与证书申请相关的信息等。

5.5.2 归档记录的保存期限

不同归档记录的保留期限是不同的。根据法律法规的要求、业务需要和运营服务的实际情况，不同归档记录的保留期限如下：

1） 对企事业单位、社会团体、社会公众的电子政务电子认证服务归档记录的保存期为证书失效后五

年；

2) 对政务部门的电子政务电子认证服务归档记录的保存期为证书失效后十年；

3) CA、子 CA 证书和密钥，及相关生成记录，自证书到期或撤销后保留不少于 10 年；

4) 物理访问记录，保留不少于 2 年；

5) 系统操作和管理记录，保留不少于 2 年；

6) 外部评估记录和内部年度评估审计记录，保留不少于 5 年；

7) 业务管理类记录，保留不少于 5 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。沃通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，还在异地保存其备份。存档的数据库一般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。沃通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。

对于书面的归档资料，不需要进行备份，但需要采取严格的措施保证其安全性。

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。但是该时间信息不采用数字时间戳这种基于密码的方式进行。

5.5.6 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。沃通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 根密钥由密码机产生，有效期为 30 年，更替办法为：
   a. 使用旧的私钥对新的公钥及信息签名生成证书；
   b. 使用新的私钥对旧的公钥及信息签名生成证书；
   c. 使用新的私钥对新的公钥及信息签名生成证书。
   d. 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，沃通将采取以下方式更替：
   a. 沃通将在 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”）；
   b. 产生新的密钥对，签发新的 CA 证书；
   c. 在“停止签发日期”之后，沃通将采用新的 CA 密钥签发下级证书。
   d. 密钥更替时直接把当前 CA 证书吊销，签发到 ARL 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) 沃通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 损害和灾难恢复

5.7.1 事故和损害处理程序

发生故障时，沃通将按照灾难恢复计划实施恢复。

5.7.2 计算机资源、软件和/或数据的损坏

沃通遭到攻击，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，沃通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

当 CA 根证书被作废时，沃通通知订户。

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

5.7.4 灾难后的业务存续能力

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，沃通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，沃通需要终止运营时，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。

沃通在终止服务六十个工作日前，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 授权的注册机构和订户等。

在终止服务四十五个工作日前向国家密码管理局报告，按照相关法律规定的步骤进操作。

沃通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) 管理 CA 系统管理员和安全官员；
7) 通知与 CA 终止运营相关的实体。

根据沃通与授权的注册机构签订的运营协议终止授权的注册机构的业务。

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

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，采取五选三方式，密钥管理员凭借智能 IC 卡对密钥进行控制。

通用证书的签名密钥对由订户的密码产品（如：智能 USB KEY 或智能 IC 卡等）生成，加密密钥对由密钥管理中心生成。

事件型证书的签名密钥对由签名设备生成，加密密钥对由密钥管理中心生成。

6.1.2 私钥传送给订户

通用证书的签名密钥对由订户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。

事件型证书的签名密钥对由签名设备生成并保管。加密密钥对由密钥管理中心产生，通过安全通道传递给证书申请方。

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，采用国家密码管理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管理部门的规定。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理部门许可的密码设备或密码模块生成。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管理部门要求。

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或密码模块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。

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 私钥在密码模块中的存储

CA 系统采用国家密码管理部门认可的密码设备，这些设备内置的协议、算法等均符合国家密码行业的标准要求。

订户私钥在密码设备或密码模块中加密保存。

6.2.8 激活私钥的方法

CA 私钥存放在硬件密码设备中，具有激活私钥权限的管理员使用含有自己的身份的智能 IC 卡登录，启

动密钥管理程序，进行激活私钥的操作，需要超过半数以上的管理员同时在场。

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 CA 机构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：智能密码钥匙 USB-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管理部门鉴定，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

CA 签发的证书符合 X.509 V3 格式。遵循 RFC5280 标准。

7.1.1 版本号

X.509 V3。

7.1.2 算法对象标识符

符合国家密码管理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 5 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；

   e. 事件型证书中代表签名行为业务场景的相关信息，分 2 种：

      - 当订户是电子签名人时，CN 中的内容是订户的名称；
      - 当订户是申请对签名行为业务场景相关信息进行固化的实体时，CN 中的内容可以是实体名称，也可以是需要固化的签名行为相关信息。

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。

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

CA 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。

7.2.2 CRL 和 CRL 条目扩展项

CRL 扩展项：颁发机构密钥标识符 Authority Key Identifier。

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

7.3.1 版本号

不适用。

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、确认沃通是否按照《沃通电子政务电子认证业务规则》及其业务规范、管理制度和安全策略开展业务，发现存在的可能风险。审计分内部审计和外部审计。

内部审计是由沃通自己组织内部人员进行的审计，审计的结果可供沃通改进、完善业务，内部审计结果不需要公开。

外部审计由沃通委托第三方审计机构来承担，审计的依据包括沃通所有与业务有关的安全策略、《沃通电子政务电子认证业务规则》、业务规范、管理制度，以及国家或行业的相关标准。

8.2 评估者的资质

内部审计人员的选择一般包括：

1) CA 的安全负责人及安全管理人员；

2) CA 业务负责人；

3) 认证系统及信息系统负责人；

4) 人事负责人；

5) 其他需要的人员。

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：

1) 人事审查；

2) 物理环境建设及安全运营管理规范审查；

3) 系统结构及其运行审查；

4) 密钥管理审查；

5) 客户服务及证书处理流程审查。

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。

对沃通关联方，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

9.1 费用

9.1.1 证书签发和更新费用

根据市场和管理部门的规定自行决定。

9.1.2 证书查询的费用

在证书有效期内，对该证书信息进行查询，沃通不收取查询费用。

9.1.3 证书吊销或状态信息的查询费用

查询证书是否吊销，沃通不收取信息访问费用。

对于在线证书状态查询（OCSP），由沃通与依赖方或订户在协议中约定。

9.1.4 其他服务费用

沃通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，沃通遵守并保持严格的操作程序和策略。一旦订户接受数字证书，沃通将不办理退证、退款手续。

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

9.2 财务责任

沃通保证其具有维持其运作和履行其责任的财务能力。它应该有能力承担对订户、依赖方等造成的责任风险，并依据本 CPS 规定，进行赔偿担保。

9.3 业务信息保密

9.3.1 保密信息范围

保密的业务信息包括但不限于以下方面：

1) 在双方披露时标明为保密（或有类似标记)的；
2) 在保密情况下由双方披露的或知悉的；
3) 双方根据合理的商业判断应理解为保密数据和信息的；
4) 以其他书面或有形形式确认为保密信息的；
5) 或从上述信息中衍生出的信息。

对于沃通来说，保密信息包括但不限于以下方面：

1) 最终用户的私人签名密钥都是保密的；
2) 保存在审计记录中的信息；
3) 年度审计结果也同样视为保密；
4) 除非有法律要求，由沃通掌握的，除作为证书、CRL 、认证策略被清楚发布之外的个人、公司和政府机构的信息需要保密。

沃通不保存任何证书应用系统的交易信息。

除非法律明文规定，沃通没有义务公布或透露订户数字证书以外的信息。

9.3.2 不属于保密的信息

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是公开的。沃通在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

订户数字证书的相关信息可以通过沃通目录服务等方式向外公布，但沃通认为涉及订户保密信息的除外。

9.3.3 保护保密信息的责任

各方有保护自己和其他人员或单位的机密信息的并保证不泄露给第三方的责任。不将机密数据和信息（也不会促使或允许他人将机密数据和信息)用于协议项下活动目的之外的其他用途，包括但不限于将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；在披露当时，如果已明确表示机密数据和信息不得复印、复制或储存于任何数据存储或检索系统，接受方不得复印、复制或储存机密数据和信息。

当沃通在任何法律、法规或规章的要求下，或在法院的要求下必须提供《沃通电子政务电子认证业务规则》中具有保密性质的信息时，沃通应按照要求，向执法部门公布相关的保密信息，沃通无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4 用户隐私保护

依据相关法律、法规，沃通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：姓名、联系方式、身份证号、地址和身份证（原件及/或任何形式的复本）等个人隐私信息。《沃通电电子政务子认证业务规则》有关用户个人信息保护条款的完整内容见沃通公司网站公布的《个人信息保护政策》。沃通针对用户隐私信息提供如下保障措施。

9.4.1 隐私保密方案

在数字证书生命周期中，沃通应在用户个人隐私信息的收集、使用、存储环节中，采取有效手段，保护个人隐私信息。

沃通应保护证书申请人所提供的、证明其身份的资料。沃通应采取必要的安全措施防止证书申请人资

料被遗失、盗用与篡改。

沃通将实施信息安全管理制度以及行业通行的安全技术和程序来确保用户的个人信息不被丢失、泄露、篡改、毁损或滥用。

9.4.2 作为隐私处理的信息

证书申请人提供的不构成数字证书内容的资料被视为隐私信息。

9.4.3 不被视为隐私的信息

证书申请人提供的用来构成数字证书内容的资料，通常不认为是隐私信息，法律或行政法规另有规定的除外。

9.4.4 用户个人信息的收集

根据《电子签名法》第二十条规定，沃通作为合法的第三方电子认证企业，在受理用户（含自然人个人以及公司法人与非法人组织）申请数字证书时有权对用户的身份进行核实。沃通要求用户即证书申请人申请证书时通过纸质申请表、电子申请表、证书服务系统等方式提供其能够证明其真实身份的证明材料。沃通在证书申请表等相关协议中，已明确告知用户沃通对用户包含但不限于用户个人的姓名、性别、年龄、身份证号码、家庭住址、联系方式等信息进行收集。

与沃通建立证书服务合作的合作方，沃通要求合作方建立收集用户个人信息的管理制度，要求合作方在开展业务过程中遵守合法、正当、必要的原则，以书面形式明确告知用户收集个人信息的目的、方式和范围，并征得用户书面同意。

沃通不会以非公司名义或授权员工个人收集用户个人信息；亦不会对与电子认证业务无关及非必要的个人信息进行收集。

9.4.5 个人信息的存储

沃通将收集到的用户个人信息统一录入证书用户管理系统。沃通建立独立的机房设备存储已收集到的用户个人信息，采取严格的技术手段对存储的数据信息进行加密处理，确保用户个人信息不被窃取、泄露，但该等措施并不排除在沃通的数据信息存储系统受到恶意黑客入侵等特殊情况及地震、洪水等不可抗力的自然因素而可能发生数据信息泄露的风险。

9.4.6 用户个人信息的使用

沃通不会在与用户自身使用证书服务及应用无关的系统或场合使用证书用户个人信息。发生下列情形之一的，沃通将依法提供用户个人相关信息：

1) 基于国家法律、行政法规、规章的规定而提供的；

2) 经过用户本人书面授权或同意提供的。

除上述情形外，沃通不会向任何第三方提供用户的个人信息，不会将用户个人信息用于其他用途。

9.4.7 用户个人信息的共享

沃通不会以商业目的或未取得用户自身同意或授权的情况下与其他组织或个人共享证书用户的个人信息。

在遵守国家相关法律法规前提下，沃通经过用户本人书面授权或同意提供的用户个人信息，并有义务要求接收方采取有效手段保护上述信息。

9.4.8 CA 对于用户个人信息的管理

沃通通过以下措施规范用户个人信息的内部管理：

1) 沃通遵循法律法规的要求及行业规范要求采取对个人信息安全保护措施；

2) 沃通内部建立严格的用户个人信息收集、查阅、使用、处理等管理制度；

3) 沃通通过加强内部员工关于个人信息保护的培训，要求员工参加学习培训；

4) 沃通要求授权的注册机构建立不能低于沃通对用户个人信息的保护级别的用户个人信息保护制度，并提交沃通备案。

9.4.9 个人信息的查询

用户如需查阅及浏览自身的个人信息，可按沃通公司官方网站公布的联系方式联系沃通查询。

9.4.10 个人信息的删除和更改

1) 个人信息的删除

按照法律法规要求或与用户证书服务协议的约定，沃通有权对证书用户个人信息进行删除。

2) 个人信息的更改

用户在使用 CA 证书服务过程中，个人信息发生变更的，应当自个人信息变更之日起 2 日内通过沃通公司官方网站公布的联系方式提出；由于用户自身原因未及时将变更信息通知沃通的，由此发生的风险由用户自身承担。

9.5 知识产权

除非额外声明，沃通享有并保留对证书以及沃通提供的全部软件的一切知识产权，包括但不限于所有权、名称权、著作权、专利权和利益分享权等。沃通有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统的兼容和互通。

按《沃通电子政务电子认证业务规则》的规定，所有由沃通签发的证书和提供的软件中使用、体现和相关的一切版权、商标和其他知识产权均属于沃通公司所有，这些知识产权包括所有相关的文件和使用手册。授权的注册机构应征得沃通的同意使用相关的文件和手册，并有责任和义务提出修改意见。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

沃通在提供电子认证服务活动过程中的承诺如下：

1) 沃通遵守《中华人民共和国电子签名法》、《中华人民共和国密码法》及相关法律的规定，接受国家密码管理部门的领导，对签发的数字证书承担相应的法律责任。
2) 沃通保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定。
3) ）除非已通过沃通证书库发出了 CA 的私钥被破坏或被盗的通知，CA 机构保证其私钥是安全的。
4) 沃通签发给订户的证书符合沃通的 CPS 的所有实质性要求。
5) 沃通将向证书订户通报任何已知的、将在本质上影响订户的证书的有效性和可靠性事件，通报的有效形式包括但不限于邮件通知、官网公告。
6) 沃通将及时吊销证书。
7) 沃通拒绝签发证书后，将立即向证书申请人归还所付的全部费用。
8) ）证书公开发布后，沃通向证书依赖方证明，数字证书中载明的订户信息都是准确的。

9.6.2 注册机构的陈述与担保

沃通授权的注册机构在参与电子认证服务过程中的承诺如下：

1) 提供给证书订户的注册过程完全符合沃通的 CPS 的所有实质性要求。
2) 在沃通生成证书时，不会因为授权的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。
3) 授权的注册机构将按 CPS 的规定，及时向沃通提交证书申请、吊销、更新等服务请求。
4) 授权的注册机构有义务通知订户阅读《沃通通用证书策略》、《沃通事件型证书策略》和本 CPS 以及相关用户协议。

9.6.3 订户的陈述与担保

订户一旦接受沃通签发的证书，就被视为向沃通、授权的注册机构及信赖证书的有关当事人作出以下承诺：

1) 订户需熟悉《沃通电子政务电子认证业务规则》的条款和与其证书相关的证书政策，还需遵守证书持有人证书使用方面的有关限制。
2) 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，可供沃通或授权的注册机构检查和核实。
3) 订户应当妥善保管私钥，采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件的发生。
4) 私钥为订户本身访问和使用，订户对使用私钥的行为负责。
5) 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知沃通和授权的注册机构，申请采取吊销等处理措施。
6) 订户已知其证书被冒用、破解或被他人非法使用时，应及时通知沃通吊销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉《沃通电子政务电子认证业务规则》的条款以及和订户数字证书相关的证书政策，并确保本身的证书用于申请时预定的目的。

依赖方在信赖订户的数字证书前，必须采取合理步骤，查证订户数字证书及电子签名的有效性。

所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解《沃通电子政务电子认证业务规则》

的有关条款。

9.6.5 其他参与者的陈述与担保

其他参与者的陈述与担保同 9.6.4。

9.7 赔偿责任限制

9.7.1 赔偿责任范围

如出现下述情形，沃通承担相应有限赔偿责任：

1) 在订户提交信息或资料真实、完整、准确的情况下，沃通签发的证书含有错误信息，导致订户或依赖方由此遭受损失；

2) 由于沃通原因致使证书私钥被破译、窃取、泄露，导致订户或依赖方遭受损失；

3) 对于订户申请吊销的证书，沃通未能及时吊销证书由此导致依赖方遭受损失。

沃通只在证书有效期限内承担损失赔偿责任。在证书有效期内产生的损失，订户或依赖方应在知道或应当知道损失发生之日起三年内向沃通书面提出索赔。

9.7.2 赔偿责任限额

沃通对所有当事实体（包括但不限于订户、申请人或信赖方）的合计责任不超过该特定证书适用的赔偿责任上限。对于一份证书产生的所有数字签名和交易处理，沃通对于任何实体有关该特定证书赔偿的合计责任应该限制在一个不超出下述赔偿责任上限的范围内。这种赔偿上限可以由沃通根据情况重新制定 ，CA 机构会将重新制定后的 CPS 公布于沃通网站以通知相关当事人。如在本 CPS 公布修订的 1 个月后继续使用沃通提供的数字证书服务，即表明同意接受此等修订的约束。如果不予接受本 CPS 中的约束，订户可以停止使用证书或在上述期限内以书面形式向沃通申请吊销证书。

沃通所颁发数字证书的赔偿责任上限如下:

个人证书：800 元人民币。

机构证书：4000 元人民币。

设备证书：12000 元人民币。

事件型证书：800 元人民币。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的责任均有上限而不考虑电子签名和交易处理等有关的其他索赔的数量。当超过责任上限时，可用的责任上限将首先分配给最早得到索赔解决的一方。沃通没有责任为每份证书支付高出责任上限的赔偿，而不管责任上限的总量在索赔提出者之间如何分配的。

9.7.3 责任免除

有下列情况之一的，应当免除沃通之责任。

1） **订户在申请和使用沃通数字证书时，有违反如下义务之一的：**

a. 订户有义务提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息。如已提供的关键材料或信息有变更，可能影响证书使用的，订户应当及时通知沃通。如因材料或信息变更未及时通知沃通，给订户本人或第三方造成的损失，沃通不承担责任；

b. 订户应当妥善保管沃通所签发的数字证书载体、私钥、保护密码 PIN 的安全，不得泄漏或随意交付他人；

c. 订户在应用自己的密钥或使用数字证书时，应当使用可依赖、安全的系统；

d. 订户知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知沃通及相关各方，并终止使用该电子签名制作数据；

e. 订户在使用数字证书时必须遵守国家的法律、法规和行政规章制度。不得将数字证书用于沃通规定使用范围外的其他任何用途使用；

f. 订户必须在证书有效期内使用该证书；不得使用已失密或可能失密、 已过有效期、被冻结、被吊销的数字证书；

g. 订户有义务根据规定按时向沃通交纳服务费用。

2） **由于下列依赖方的原因造成的损失，沃通不承担任何赔偿责任，由依赖方自行承担。**

a. 依赖方未经检验证书的状态即决定信赖证书的；

b. 依赖方明知或者应当知道证书存在超范围使用、超期限使用、被人窃取或者信息错误等情况，仍然信赖该证书并从事有关活动的。

3） **外部授权的注册机构或其他合作方依据协议约定或实际上承担履行证书受理与审核、订户身份鉴别、证书交付等工作的，因其违反协议约定或存在过错（包括但不限于未尽审核与鉴别义务、未妥善交付证书、未经授权处理订户私钥等行为），导致订户、依赖方或自身遭受损失的，订户或依赖方可以追究授权的注册机构或合作方的责任，沃通给予配合，但沃通不承担赔偿或补偿责任。**

4) **由于客观意外或其他不可抗力事件原因而导致数字证书签发错误、延迟、 中断、无法签发，或暂停、终止全部或部分证书服务的。关于不可抗力的描述参见本 CPS 9.15.4。**

5) **因沃通的设备或网络故障等技术故障而导致数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“技术故障”引起原因包括但不限于：**

a. 不可抗力；

b. 关联单位如电力、电信、通讯部门而致；

c. 黑客攻击；

d. 设备或网络故障。

6) **如果沃通能够证明其提供的服务是符合法律、行政法规相关规定实施的，沃通将不对订户或依赖方承担任何赔偿或补偿责任。**

9.7.4 有限责任

1) **沃通所有的赔偿义务不得高于本 CPS 9.7.2 规定的赔偿责任上限。**

2) **沃通根据判决或裁定应当承担赔偿或补偿责任的，沃通将按照法院的判决、仲裁机构的裁定承担相应的赔偿或补偿责任。**

3) **无论本 CPS 是否有相反或不同规定，就以下损失或损害，沃通不承担任何赔偿和/或补偿责任：**

a. 订户和/或依赖方的任何间接损失、直接或间接的利润或收入损失、信誉或商誉损害、任何商机或契机损失、失去项目、以及失去或无法使用任何数据、无法使用任何设备、无法使用任何软件；

b. 由上述第“a”项所述的损失相应生成或附带引起的损失或损害；

c. 非沃通的行为而导致的损失；

d. 因不可抗力而导致的损失，如罢工、战争、灾害、恶意代码病毒等。

9.8 赔偿

沃通按照《沃通电子政务电子认证业务规则》9.7 条款承担赔偿责任。

证书订户和依赖方在使用或信赖证书时，若有任何行为或疏漏而导致沃通和授权的注册机构产生损失，订户和依赖方应承担赔偿责任。

订户接受证书就表示同意在以下情况下承担赔偿责任。

1) 未向沃通提供真实、完整和准确的信息，而导致沃通或有关各方损失。

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。

3) 在知悉证书密钥已经失密或者可能失密时，未及时告知沃通，并未终止使用该证书，而导致沃通或有关各方损失。

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电子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，即违反沃通对证书使用的规定，造成了沃通或有关各方的利益受到损失。

6) 如订户在证书的申请、使用过程中存在的其他违反本 CPS 、服务协议、相关法律、法规的规定的行为，给沃通造成损失的。

9.9 有效期限与终止

9.9.1 有效期限

《沃通电子政务电子认证业务规则》自发布之日起正式生效。

《沃通电子政务电子认证业务规则》中将详细注明版本号及发布日期。

9.9.2 终止

当新版本的《沃通电子政务电子认证业务规则》正式发布生效时，旧版本的《沃通电子政务电子认证业务规则》自动终止。

9.9.3 效力的终止与保留

《沃通电子政务电子认证业务规则》的某些条款在终止后继续有效，如知识产权承认和保密条款。另外，各参与方应返还保密信息到其拥有者。

9.10 对参与者个别通告与沟通

认证活动的某一参与方与另一参与方进行通信时必须使用安全通道，以使其通信过程在法律上有效。

9.11 修订

9.11.1 修订程序

当《沃通电子政务电子认证业务规则》不适用时，由沃通安全策略管理委员会组织 CPS 编写小组进行修订。

修订完成后，沃通安全策略管理委员会进行审批，审批通过后将在沃通公司的网站上发布新的《沃通电子政务电子认证业务规则》。

《沃通电子政务电子认证业务规则》将进行严格的版本控制。

9.11.2 通知机制和期限

《沃通电子政务电子认证业务规则》在沃通公司的网站上发布。版本更新时，最新版本的《沃通电子政务电子认证业务规则》在沃通公司的网站发布，对具体个人不做另行通知。

9.11.3 必须修改业务规则的情形

当管辖法律、适用标准及操作规范等有重大改变时，必须修改《沃通电子政务电子认证业务规则》。

9.12 争议处理

沃通、证书订户、依赖方等实体在电子认证活动中产生争端可按照以下步骤解决：

1) 当事人首先通知沃通，根据《沃通电子政务电子认证业务规则》中的规定，明确责任方；
2) 由沃通相关部门负责与当事人协调；
3) 协调不成，当事人因与沃通或授权机构在电子认证活动中产生的任何争端及或对《沃通电子政务电子认证业务规则》所产生的任何争议，均应提请深圳仲裁委员会按照其仲裁规则在深圳进行仲裁。仲裁裁决是终局的，对双方均有约束力。

9.13 管辖法律

《沃通电子政务电子认证业务规则》在各方面服从中国法律和法规的管制和解释，包括但不限于《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》等。

9.14 与适用法律的符合性

无论在任何情况下，《沃通电子政务电子认证业务规则》的执行、解释、翻译和有效性均适用中华人民共和国大陆地区的法律。

9.15 一般条款

9.15.1 完整规定

《沃通电子政务电子认证业务规则》将替代先前的、与主题相关的书面或口头解释。

9.15.2 分割性

当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。

9.15.3 强制执行

免除一方对合同某一项的违反应该承担的责任，不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。

9.15.4 不可抗力

不可抗力是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。

在数字证书认证活动中，沃通由于不可抗力因素而暂停或终止全部或部分证书服务的，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方（如订户）不得提出异议或者申请任何补偿。

9.16 其他条款

沃通公司对《沃通电子政务电子认证业务规则》拥有最终解释权。