沃通电子认证服务有限公司 WoTrus CA Limited
中国深圳市南山区南海大道 1057 号蛇口科技大厦二期 A 座 502, 邮编：518067
总机：+86-755-8600 8688 传真：+86-755-33975112 https://www.wotrus.com

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：1.0

状态：最终审核通过

生效日期：2019 年 7 月 22 日

沃通电子认证服务有限公司

数字签名者:
沃通电子认证服务有限公司
日期:
2019.08.15 10:12:34 +08:00

www.wotrus.com

版本说明：

沃通电子政务电子认证业务规则版本控制表

版本	主要修改说明	修订时间	修改人	审核/批准人	生效时间
1.0	依据国家法律法规，遵循《电子政务电子认证业务规则》等规范要求，创建本《电子政务电子认证业务规则》。	2019年7月22日	覃丕军	安全策略管理委员会	2019年7月22日

目录

1. 概括性描述

1.1 概述

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 CPS》，CPS 为“Certificate Practice Statement”的缩写）由沃通电子认证服务有限公司按照国家密码管理局《电子政务电子认证服务管理办法》的要求，依据《电子政务电子认证业务规则规范》制定，并报国家密码管理局备案。

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”），成立于 2002 年 3 月 18 日，是同时获得国家密码管理局颁发的《电子认证服务使用密码许可证》以及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。作为国内领先和国际领先的服务器证书签发 CA，沃通自主研发国密证书全生态应用系统，并严格按照国际标准和国内标准为广大用户提供优质服务，为保障我国电子政务系统安全提供可靠可控的基于国密算法和国密证书数字证书认证服务和应用支持服务。

本《电子政务电子认证业务规则》详细阐述了沃通在实际工作中和运行中所遵循的各项规范。本《电子政务电子认证业务规则》适用于沃通及其员工、注册机构、证书申请人、证书持有者和依赖方，各参与方必须完整地理解和执行本《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 电子政务电子认证业务范围

电子政务电子认证业务规范包括面向政务部门的电子政务电子认证服务和面向企事业单位、社会团体、社会公众的电子政务电子认证服务。

1.3 电子政务电子认证活动参与者

1.3.1 电子政务认证机构

电子认证服务机构是受用户信任、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。沃通是根据《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》等规定依法设立的电子认证服务机构（简称“CA”）。

1.3.2 注册机构

注册机构（RA），作为电子认证服务机构授权委托的实体，负责对证书申请者（证书使用方）进行身份识别和鉴别，初始化或拒绝证书申请和撤销请求，代表CA批准更新证书或更新密钥的申请。沃通本身即是CA又是RA，沃通可授权建立多家外部RA。RA除了为最终用户证书申请者建立注册过程外，还要对最终用户提供服务。RA应遵循本CPS以及沃通的授权。

RA有责任妥善保存客户的数据的义务，不允许将客户的数据透露给与证书申请无关的任何单位或个人，不允许用作商业利益方面的用途。RA必须获得沃通及其操作子CA的授权，根据授权从事各类证书服务，并依据授权拓展相应的业务。各类政府机构、企事业单位等均可申请成为沃通认证服务体系架构内的注册机构。

沃通按照申请单位的性质、证书发展预期、场地、和人员情况等，经过合理的评估审计，合格后由沃通最终决定，对其发放授权委托书，授权其作为注册机构。

注册机构（RA）代表CA建立起证书注册过程，确认证书申请者（证书使用方）的身份，批准或拒绝证书申请，批准证书使用方的证书撤销请求或直接撤销证书，批准证书使用方的证书更新请求。

1.3.3 证书持有者

证书持有者，也称“证书使用方”，指从沃通获得证书的个人、组织机构，即最终用户。证书使用方通常需要同沃通，或其注册机构，或其授权机构签订合约获得证书，并承担作为证书使用方的责任。

“主体”（subject）特指证书标识的实体，或者被颁发证书的实体，也即证书中主体名字段（Subject Name）所标识的实体。

在有些情况下，证书使用方和证书主体是同一个实体，如个人证书、组织机构证书；但在有些情况下，证书使用方和主体不是同一实体，如设备证书(服务器证书)的证书使用方是设备所属机构，而证书主体是服务器IP地址或域名。

证书申请者指正在申请证书的证书使用方或其授权者。在有些情况下，证书申请者和证书使用方是同一个实体，如个人证书；但在有些情况下，他们是不同的实体，如组织机构证书的证书使用方是该组织机构，而申请者是往往其授权人。再比如，一个组织可能为其雇员申请证书，其雇员是真正的证书使用方（需要承担证书使用方的责任），而组织机构是其授权申请者。

1.3.4 依赖方

沃通信任域的依赖方是为某一应用而使用、信任沃通或其注册机构颁发的证书的个人或组织。依赖方可以是沃通的证书使用方，也可以不是证书使用方。

1.3.5 其他参与者

指为沃通的电子认证活动提供相关服务的其他实体。

1.3.6 各方主要责任

认证机构、注册机构、证书使用方、依赖方以及其他参与者的主要责任都在相关协议或条款中进行了明确和说明，具体可以参见本 CPS 和沃通官网(www.wotrus.com)。

1.4 电子政务电子认证策略管理

1.4.1 管理机构

沃通成立安全策略管理委员会，作为本机构电子政务电子认证服务业务规则的管理机构，对电子政务电子认证服务业务规则进行维护与管理，包括：

1) 确定本电子政务电子认证服务业务规则的制定和维护职责，建立合理、有效的修订和批准流程；

2) 定期对存在的业务风险进行评估，并及时对电子政务电子认证服务业务规则进行修订；

3) 按照《电子政务电子认证服务管理办法》规定，将发布的和修订后的电子政务电子认证服务业务规则及时报国家密码管理局备案，并在服务网站(www.wotrus.com)公开发布。

沃通安全策略管理委员会由公司 CEO 和各部门负责人组成。

1.4.2 联系方式

沃通公布以下对外的相关联系方式，任何有关沃通电子政务 CPS 的问题、建议、疑问等，均可按照下述

1）本 CPS 的发布地址：https://www.wotrus.com/ca/dca_cps.html

2）本机构网站地址：https://www.wotrus.com

3）电子邮箱：cps@wotrus.com

4）联系地址：广东省深圳市南山区南海大道 1057 号蛇口科技大厦 2 期 A 座 502#（518067）

5）联系部门：风控合规部

6）电话号码：+86-755-86008688

7）传真号码：+86-755-33975112

1.4.3 批准程序

沃通按照以下方式处理本电子政务 CPS 的起草制定、审批、发布、变更、备案等流程：

1）起草小组成立和 CPS 指定

沃通安全策略管理委员会指定相关部门和人员成立起草小组。沃通电子政务 CPS 起草小组根据《电子政务电子认证服务业务规则规范》编写本电子政务 CPS，在编写过程中应及时向沃通安全策略管理委员会汇报制定进展，并就有关问题召集相关人员讨论。

2）审批

本电子政务 CPS 由起草小组编写制定后，提交沃通安全策略管理委员会审核。沃通安全策略管理委员会议一致通过后，即作为正式版本。

3）发布

根据服务范围和服务对象要求，沃通采取如下的方式发布本电子政务 CPS：

（1）以电子的方式，在公司的官方网站发布。

（2）以书面的方式，客户服务部门可以根据需求提供。

4）变更

根据国家的政策法规、技术要求、标准的变化及业务发展情况等需要对本电子政务 CPS 进行修订，由起草小组编写修改建议报告，提交沃通安全策略管理委员会审核。经过批准通过后，按照前述方式进行对外发布。

5）备案

根据《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》的规定，沃通安全策略管理委员会在批准本电子政务 CPS 的制定或修订后，沃通将及时向国家密码管理局备案。

1.5 定义与缩写

1.5.1 定义

术语	定义
证书	是指一段信息，它至少包含了一个名字，标识特定的 CA 或标识特定的证书使用方，它包含了证书使用方的公钥、证书有效期、证书序列号，及 CA 数字签名。
证书申请	来自证书申请者的、要求 CA 颁发证书的请求
证书申请者	要求一个发证机构颁发证书的个人、组织机构或其授权代理者。
证书链	一个有序的证书列表，包含了最终用户的证书和发证机关的证书，该列表最顶级证书为根证书，最下级证书为最终用户的证书。
证书策略（CP）	是一个有关证书业务策略的主要说明。
证书撤销列表（CRL）	一个定期(或根据要求)发行的、并由发证机关数字签名的信息列表，用来识别在有效期内提前被撤销的证书。这个列表通常标明 CRL 发布者的名字，发布的日期，下一次 CRL 发布的日期，被撤销证书的序列号，撤销证书的时间和原因。
认证机构 (CA)	一个授权颁发、管理、撤销和更新证书的实体。
电子认证业务规则(CPS)	认证机构批准或拒绝证书申请、颁发、管理和撤销证书时必须遵守的业务规则的描述。
挑战语	证书申请者在注册一个证书时选择的秘密短语。当一个证书被颁发后，证书申请者成为了一个证书使用方，这时如果证书使用方要求撤销或更新这个证书使用方证书，CA 或 RA 可以使用挑战语识别证书使用方的身份。
一致性审计	一个认证机构或注册机构要定期经历的审计，通过该审计确定它是否满足有关的标准。
安全损害	对安全策略的违反（或怀疑违反），包括出现敏感信息未经授权的泄漏或失去对其的控制。对于私钥，安全损害是指丢失、失窃、公开、修改、未经授权的使用或私钥受到的其它安全危害威胁。
机密/私密信息	根据 CPS (9.3，9.4)要求需保密的信息。
服务器证书	用于支持浏览器和服务器之间的 SSL 会话加密。该证书用于标识组织机构的 Web 服务器的身份，将一个域名或 IP 地址与一台服务器绑定。

术语	定义
	该服务器证书确保服务器的拥有机构有权使用证书上的域名，确保当一个用户访问一个以该域名命名的 Web 服务器时，用户访问的 Web 服务器就是他要访问的服务器，而不是假冒的服务器，另外它可实现信息从客户端到服务器端的加密传输。
知识产权	在版权、专利、商业秘密、商标和其他知识产权下拥有的权利。
密钥生成规程参考指南	描述密钥生成规程要求和业务操作的文档。
密钥生成规程	CA 密钥对产生、其私钥被传送到密码模块、私钥备份和颁发它的公钥的过程。
未经验证的证书使用方信息	指证书申请者提交给 CA 或 RA、并被包含在证书中的信息，但该信息未经 CA 或 RA 证实，因此 CA 或 RA 除确认该信息是由证书申请者提出外，对其它信息不作确认。
抗抵赖	一种提供通信保护的属性，它可以防止通信一方否认信息的出处，否认它已经提交或传送了这些信息。否认出处包括否认某一通信与先前的一系列消息源来自同一地方，即使不知发送者是谁。（注：只有法院的判决、仲裁或其它的裁决才能够最终阻止抵赖。例如，合法、有效证书的数字签名是裁判所作出抗抵赖裁决的支持证据。）
在线证书状态查询协议 (OCSP)	为依赖方提供实时查询证书状态信息的协议。
操作期限	指从证书颁发日期和时间（或者证书上指定的一个较晚的日期和时间）开始，到证书过期或被撤销时的日期和时间为止的这段时间。
公钥基础设施(PKI)	所有支持基于证书的公开密钥系统实施和操作体系的组织机构、技术、业务和过程的总称。
注册机构 (RA)	CA 批准的一个实体，它帮助证书申请者申请证书，批准或拒绝证书申请，撤销证书或更新证书。
依赖方	信赖一个证书和/或一个数字签名的个人或组织机构。
依赖方协议	协议规定了一个组织机构或个人作为依赖方的条件和要求。
信息库	认证机构提供的、可在线访问的证书和其他证书有关信息的数据库。
秘密分割	根据秘密分割算法，将激活 CA 私钥需要的数据分割成多个部分，使用其中若干个分割可以恢复原激活数据。
安全套接层协议	由网景通信公司开发的、保护 Web 通信的一个工业标准。SSL 为一个 TCP/IP 连接提

术语	定义
(SSL)	供数据加密、服务器验证、信息完整性和可选的客户端验证等。
主体	与公钥对应的私钥的持有者。在组织机构证书中，主体指的是持有私钥的设备或装置或组织机构本身。一个主体只有唯一的、确切的命名。它和该主体证书中的公钥绑定在一起。
证书使用方	对于个人证书，证书使用方是指人，他是证书的主体；对于组织机构身份证书，证书使用方是指组织机构；对于组织机构代表人身份证书，证书使用方是组织机构授权的代表人；对于服务器证书，它是证书主体所对应设备的拥有者。一个证书使用方可以使用或被授权使用证书所含公钥对应的私钥。
证书使用方协议	一个 CA 或 RA 拟定的协议，规定一个人或组织机构作为证书使用方需要遵循的条款和条件。
可信人员	在认证机构的雇员、合同商或顾问，他们负责保证实体基础设施的可信性，以及管理产品、服务、设施和业务的可信性。
安全可信系统	是指能够有效地避免被入侵与滥用的，提供可靠的、可用的、有正确操作保障的、能够完成预定功能的、实施了适当的安全策略的计算机硬件、软件与程序。安全可信系统不一定是政府信息系统分级中所定义的“可信系统”。

1.5.2 缩写

缩写	全称
CA	认证机构
CP	证书策略
CPS	认证业务规则
CRL	证书撤销列表
OCSP	在线证书状态查询协议
LDAP	轻量目录访问协议
LRA	证书注册受理点
PIN	个人身份识别码
PKCS	公钥密码标准
PKI	公钥基础设施
RA	注册机构
RFC	请求评注标准(一种互联网建议标准)
SSL/TLS	加密套接层协议/传输层安全协议

1.6 策略发布与管理

1.6.1 策略的发布

沃通电子政务 CPS 可从沃通的官方网站（https://www.wotrus.com/ca/）获取；用户证书可从沃通的官方网站（https://www.wotrus.com/ca/dca_cert_search.html）获取证书的状态，包括证书的序列号、主题、生效日期、终止日期、证书类型、证书状态，以及可以下载证书的公钥。

1.6.2 策略发布的时间或频率

沃通电子政务 CPS 一旦批准，则及时发布到沃通官网，用户可通过官网 7X24 小时获得。

1.6.3 策略访问控制

沃通电子政务 CPS 是以只读的形式进行对外发布的。

沃通通过网络安全防护、系统安全设计、安全管理制度确保 CPS 只有授权人员才能修改和发布。

2. 身份标识与鉴别

2.1 数字证书命名与格式

2.1.1 证书命名

沃通严格按照《基于 SM2 密码算法的数字证书格式规范》（GM/T 0015）为电子政务数字证书命名。

2.1.2 证书版本

沃通签发的电子政务数字证书符合 X.509 V3 标准，甄别名格式遵守 X.501 标准。甄别名的命名规则由沃通定义。

根据证书主体类型不同，沃通颁发的证书的主体名字可以是人员姓名、组织机构名、部门名、域名等，命名符合 X.501 甄别名规定。

沃通 CA 证书的颁发者和主体域中包含 X.501 甄别名。沃通 CA 证书的主体甄别名由表 3 中的内容组成。

表 3- CA 证书主体甄别名属性

属性	值
国家 (C) =	CN
机构(O) =	机构名称
显示其他内容(OU) =	CA 证书中可以包含多个 OU 属性。这些属性可以包含但不限于下列内容： ➢ 单位部门名称 ➢ 其他描述文字
省 (S) =	所在省份
地区（L）=	所在城市
通用名(CN) =	对于 SSL 证书，一般为网站域名或 IP 地址；而对于代码签名证书则为申请单位名称；而对于客户端证书则为证书申请者的姓名等.

最终用户证书的主体域中包含一个 X.501 甄别名，它由表 4 中的内容组成。

表 4–最终用户证书主体甄别名属性

属性	值
国家 (C) =	CN
机构(O) =	组织机构属性使用如下： ➢ 对于没有确定机构的个人用户证书。 ➢ 对于其他类型证书，是证书使用方所在机构的机构名。
显示其他内容(OU) =	CA 证书中可以包含多个 OU 属性。这些属性可以包含但不限于下列内容： ➢ 单位部门名称 ➢ 其他描述文字
省 (S) =	所在省份
地区（L）=	所在城市
通用名(CN) =	对于 SSL 证书，一般为网站域名；而对于代码签名证书则为申请单位名称；而对于客户端证书则为证书申请者的姓名等.
E-Mail 地址 (E) =	e-mail 地址（电子邮件证书，账户证书，个人证书，或机构证书）

运营设备证书的主体域中包含一个 X.501 甄别名，它的内容组成与服务器证书类似，只是其中的通用名(CN)对应的内容是设备的名称或 IP 地址，或者机构的名称。

2.1.3 证书扩展项

针对特别的用户，沃通颁发的证书有可能包含私有扩展项，不能识别私有扩展项的应用、依赖方可以忽略该扩展项。

沃通支持私有扩展项的类型包括：

- 个人身份证号码 Identify Card Number
- 企业营业执照（统一社会信用代码） IC Registration Number
- 企业组织机构代码 Organization Code
- 企业税号 Taxation Number

2.1.3.1 密钥用法（Key Usage）

该扩展项指定证书密钥对的用法，不同证书该扩展项的设置见 CPS 6.1.7。这个扩展项的 criticality 域通常设置为 TRUE。

2.1.3.2 证书策略扩展项（Certificate Policies）

证书策略扩展项中有沃通证书策略中对应证书类的 CP 对象标识符及策略限定符。这个扩展项的 criticality 域设置为 FALSE。

2.1.3.3 主体备用名（subjectAltName）

扩展项的使用符合 RFC 3280。此扩展项的 criticality 设为 FALSE。

2.1.3.4 基本限制扩展项（BasicConstraints）

沃通 CA 证书的基本限制扩展项中的主体类型被设为 CA。最终用户证书的基本限制扩展项的主体类型设为最终实体 (End-Entity)。这个扩展项的 criticality 域设置为 TRUE。

CA 证书的基本限制扩展项中的路径长度设定为在证书路径中该证书之后的 CA 级数。对于最终用户证书颁发 CA，其 CA 证书“pathLenConstraint”域的值设为 0，表示证书路径中仅有一个最终用户证书可以跟在这个 CA 证书后面。

2.1.3.5 扩展的密钥用法（Extended Key Usage）

对沃通不同的证书，扩展的密钥用法扩展项设定如下。

表 7 –可扩展的密钥用法扩展项的设置

		电子邮件证书	账户证书	服务器证书	个人证书
Criticality		非关键	非关键	非关键	非关键
	Server Auth 服务器认证	未设置	未设置	设置	未设置
	Client Auth 客户端认证	设置	设置	设置	设置
	CodeSigning 代码签名	未设置	未设置	未设置	未设置
	EmailProtection 邮件保护	设置	设置	未设置	设置
	TimeStamping 时间戳	未设置	未设置	未设置	未设置
	OCSP Signing OCSP 签名	未设置	未设置	未设置	未设置

2.1.3.6 CRL 的分发点（cRLDistributionPoints）

沃通颁发的证书中包含 CRL 的分发点扩展项，依赖方可根据该扩展项提供地址和协议下载 CRL。此扩展项的 criticality 项应设为 FALSE。

2.1.3.7 颁发 CA 密钥标识符

沃通最终用户证书及中级 CA 证书中有颁发 CA 密钥标识符扩展项，当证书颁发者包含主体密钥标识扩展项时，颁发 CA 密钥标识符由 160 位的颁发证书的 CA 的公钥进行 SHA-1 散列运算后的值构成；否则，它将包含颁发 CA 的主体 DN 和序列号。这个扩展项的 criticality 域设置为 FALSE。

2.1.3.8 主体密钥标识符

当证书包含主体密钥标识符扩展项时，该值由证书主体的公钥产生。使用该扩展项时，其扩展项的 criticality 域设为 FALSE。

2.2 身份标识与鉴别

2.2.1 证明拥有私钥的方法

沃通通过以下两个条件来证明证书持有者对私钥的持有：

1）通过证书请求中所包含的数字签名来证明证书持有者持有与公钥对应的私钥。

a）证书持有者在客户端生成签名密钥的公私钥对；

b) 证书持有者使用私钥对证书请求信息签名，并连同公钥一同提交 CA 系统；

c) CA 使用证书持有者公钥验证证书持有者签名。

2) 证书持有者必须妥善保管自己的私钥。

2.2.2 组织机构身份的鉴别

颁发机构证书、设备证书时，沃通或其注册机构按照鉴别操作规范的要求对组织机构进行身份鉴别，鉴别包括如下两方面内容：

- 确认组织机构是确实存在的、合法的实体。确认的方式可以是，政府颁发的组织机构成立的有效文件，如营业执照、组织机构代码证等，并通过权威的第三方数据库进行验证和确认。
- 确认该组织机构知晓并授权证书申请，即代表组织机构提交证书申请的人是经过授权的。确认的方式可以是：

使用从网络或其它常规途径获取验证电话号码，进行电话验证，获得组织机构有关申请及授权事宜的确认；或者由该机构提供加盖公章的授权书确认。

颁发服务器证书时，沃通或其注册机构按照鉴证规范要求对组织机构进行身份鉴别，鉴别包括如下三方面内容：

- 确认组织机构是确实存在的、合法的实体。确认的方式可以是，政府颁发的组织机构成立的有效文件，如营业执照、组织机构代码证等，同时通过权威的第三方数据库确认。
- 确认组织机构对域名有所有权或使用权。确认的方式可以是通过域名验证系统完成验证或人工确认域名所有者信息。
- 确认该组织机构知晓并授权证书申请，即代表组织机构提交证书申请的人是经过授权的。确

认的方式可以是：使用从其它常规途径获取验证电话号码，进行电话验证，获得组织机构有关申请及授权事宜的确认。

当沃通对外向有关机构（如注册机构或其他授权机构）颁发与运营有关的设备证书时，将通过电话或书面形式（包括传真、信函），向该机构的有关责任人确认设备证书申请者来自该机构，且有关申请获得了授权。

对于机构证书，沃通会验证单位信息的真实性和有效性，包括单位名称、注册地址、统一社会信用代码，如果包含单位邮箱的，则需要验证邮箱的有效性和控制权。如果包含域名的，则需要验证域名的有效性和控制权。沃通不对单位内部部门名称进行验证，虽然可能会显示在证书中。

2.2.3 个人身份鉴别

2.2.3.1 电子邮件证书和账户证书的个人身份鉴别

对于电子邮件证书的申请，沃通通过向证书申请中提交的、需要绑定的电子邮箱发送验证信息，申请人需要提供验证信息以确认电子邮箱地址是真实的、正确的，验证是邮箱拥有者本人在申请证书。

对于账户证书的申请，沃通通过一定的方式确认账户的有效性，并验证申请者（证书使用方）知晓或拥有该账户的秘密（如口令、或先前颁发的该账户的证书的私钥），以实现对用户身份的鉴别和验证。

为了完成账户证书的身份鉴别，沃通通常需要与维护该账户的应用服务系统的运营商进行合作。

对于电子邮件证书，沃通只验证证书中需要显示的电子邮件地址；对于账户证书，沃通只验证证书中需要显示的电子邮件地址和账户名称。

2.2.3.2 个人证书的个人身份的鉴别

颁发个人证书时，沃通或注册机构按照鉴别操作规范的要求对个人进行身份鉴别，鉴别包括如下两方面内容：

1) 确认证书申请者提交的身份信息确实存在且正确，具体方法包括：

- 采用沃通认可的、提供身份证实服务的数据库中的信息，如公安部门提供的个人身份数据库、主流的信用机构或其他可靠的信息源；或者，
- 对于授权承担注册机构职能的机构向与其相关的人员（如其员工、客户、合作伙伴）颁发证书的情形，可通过采用包含在该机构业务交易记录或数据库中的信息来完成鉴别。

2) 验证证书申请者是证书申请中所说的那个人，验证的方式包括：

- 验证申请者知晓或拥有通常只有真正的申请者才知晓或拥有的秘密，如通过证书使用方银行账户进行转帐验证；
- 通过授权承担注册机构职能的机构中的 RA 管理员验证、确认与该机构相关的证书申请者（如其员工、客户、合作伙伴）的身份及其证书申请行为，或者，其他安全可靠的方式，如面对面的验证、确认。

若个人证书的身份信息中包含有组织机构信息，则沃通认证机构或其注册机构还需要对该组织机构信息进行鉴别，其情形分为如下两种： 若申请者个人直接向沃通或其注册机构提交申请，则沃通或其注册机构，首先按“2.2.2 组织机构身份的鉴别”所述方法，确认组织机构信息的真实性；然后按“2.2.2 组织机构身份的鉴别”所述方法，确认申请者属于该组织机构的员工。 若证书申请通过沃通授权的承担注册机构职能的组织机构提交，且证书主体来自该组织机构，则在这种情形下，由组织机构负责确保有关信息的正确性。 沃通向承担注册机构角色的机构颁发与运营管理有关的管理员证书时，将通过电话或书面形式（包括传真、信函），向该机构的有关责任人确认该申请人来自该机构，且获得了有关申请的授权。

对于个人证书，沃通只验证在证书中需要显示的姓名、发放证件的所属辖区，如果包含电子邮件的，还需要验证电子邮件的控制权。对于个人证书中包含组织单位信息时，还必须按照组织机构身份鉴别的要求，对单位信息进行验证。沃通不对单位内部部门名称进行验证，虽然可能会显示在证书中。

2.2.4 政府部门个人身份鉴别

对于政府部门个人身份的鉴别，除了满足 2.2.3 个人身份鉴别的要求外，申请人还需要提交由所属政府部门签章的证明文件，明确组织、部门与证书中所列名称一致，并证明申请人属于该部门。

2.2.5 网站服务器身份鉴别

在把 SSL 证书签发给网站服务器时，除了必须完成组织机构身份的鉴别外，还需要验证服务器绑定的网站域名或 IP 地址。对服务器身份鉴别方式，可以采用如下三种方式之一：

(1) 网站控制权验证：在服务器指定目录下"/.well-known/pki-validation"放置一个由 CA 验证系统生成的与待验证的域名或 IP 地址相关的一次性有效的动态验证码，CA 验证系统自动读取此目录下的验证码后验证准确。此方法仅允许采用 80 或 443 端口访问读取验证码；

(2) 域名使用权验证：由 CA 验证系统给待验证的域名的如下邮箱：admin@, administrator@, webmaster@, hostmaster@, postmaster@ 发送一个与待验证的域名相关的一次性有效的动态验证码，用户在收到此验证码后提交到证书申请系统中并验证通知；

(3) 域名管理权验证：用户把 CA 验证系统生成的与待验证的域名相关的一次性有效的动态验证码作为一条域名解析记录设置好并通过 CA 验证系统验证，可用的域名解析记录有：CNAME、TXT 和 CAA。

沃通有一个独立的域名验证系统支持以上 3 种方法提供给用户完成网站服务器的控制权验证，证明用户有权申请绑定此域名或 IP 地址的服务器证书。

如果以上验证方法验证的是根域名，则子域名不再需要验证；如果验证的是子域名，则每个其他子域名或根域名还需要验证。域名完成验证后 1 年内无需再验证，CA 系统需绑定已验证的域名与已验证的组织机构的对应关系。

2.3 密钥更新请求的标识与鉴别

在证书使用方证书到期前，证书使用方需要获得新的证书以保持证书使用的连续性。沃通一般要求证书使用方产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。然而，在某些情况下，沃通允许证书使用方为一个现存的密钥对申请一个新证书，称作“证书更新”。对于密钥更新而言，证书使用方证书除公钥、有效期和序列号改变外，其他信息都没改变；对于证书更新而言，和密钥更新相比，证书使用方证书公钥也不改变。

密钥更新和证书更新与申请一个新证书在技术上是不同的。在申请一个新证书时，证书使用方需到沃通或其注册机构的证书服务站点申请注册，填写必要的申请信息；而对于密钥更新和证书更新，证书使用方虽然同样需要访问沃通或其注册机构的证书服务站点的相应服务网页，但用户无需填写申请信息，系统会自动获取证书使用方的有关信息。对于沃通的证书认证业务，在证书有效期到期前只能通过密钥更新或证书更新颁发具有相同颁发者、主体名和证书用途的证书。除非先将证书撤销，否则在证书有效期到期前，不能通过申请新证书的方法获得具有相同颁发者、主体名和证书用途的证书。

2.3.1 常规密钥更新的标识与鉴别

对于一般正常情况下的密钥更新，证书使用方访问沃通或其注册机构的证书服务站点相应的服务网页进行密钥更新申请，系统自动获取证书使用方原证书的相关信息，如证书使用方甄别名、证书序列号等，形成证书密钥更新申请信息，申请信息包含新公钥并由更新前的私钥签名（对于加密证书密钥更新而言，

申请信息不包含新公钥）。

沃通的证书认证系统将对密钥更新申请进行验证，包括验证申请签名，然后进行与新证书申请一样的鉴别。

2.3.2 撤销后密钥更新的标识与鉴别

沃通对撤销后证书不进行密钥更新。

2.4 撤销请求的标识与鉴别

在沃通的证书业务中，证书撤销请求可以来自证书使用方，也可以来自沃通或其注册机构。证书撤销的方式可以是证书使用方自己申请撤销，也可以由证书使用方要求沃通或其注册机构管理员撤销，沃通和其注册机构在认为必要的时候，有权发起撤销证书使用方证书。

在证书使用方自己申请撤销时，撤销请求的鉴别过程如下：

证书使用方在申请撤销证书时，需要提交撤销申请材料，个人证书的撤销申请材料必须要有本人的亲笔签名，机构证书必须要加盖单位的公章，鉴别人员会核实签名与公章，确认无误后，在系统中完成撤销申请。

证书使用方通过认证机构、注册机构撤销时，撤销请求的鉴别过程如下：

证书使用方通过一定的方式，如邮件、传真、电话等，向认证机构、注册机构提交请求，认证机构、注册机构通过与证书保障级别相应的通讯方式与证书使用方联系，确认要撤销证书的人或组织确实是证书使用方本人，或者其授权者。依据不同的环境，通讯方式可以采用下面的一种或几种：电话、传真、e-mail、邮寄或快递服务。

3. 数字证书服务操作规范

3.1 证书申请

3.1.1 证书申请流程

沃通在本电子政务 CPS 中阐述和说明了受理证书申请的所有流程及要求，并通过网站、书面告知、现

场咨询、电话、电子邮件等方式告知证书申请者及证书持有者所必须提交的材料和办理流程。

对于个人证书，申请者到沃通受理点填写或到沃通网站下载填写《个人数字证书申请表》，并提供个人身份证明文件及其复印件一份，例如：身份证、军官证、护照、警官证、士兵证、士官证、文职干部证、及其他法律法规和政府政策认可的证明文件等。

政府、机构部门中的个人申请证书时，还需提交个人所在单位许可授权证明（申请表加盖单位公章）及单位证明文件；如果是委托申请的，还需提供经办人被授权证明，证明代表他人提交证书申请的人是经过单位授权的。

对于机构证书，申请者填写《机构数字证书申请表》，并提供单位对经办人的授权委托证明，单位的企业法人营业执照、事业单位法人登记证、税务登记证、组织机构代码证、社会团体法人登记证、政府批文及其他有效证件，经办人的身份证和沃通可能需要的其他文件。

任何需要在各类应用中采用数字证书进行真实身份标识和鉴别，实现信息保密，并提供信息源发性证明、完整性保障和抗抵赖的个人或机构，都可以申请个人证书或机构证书。

组织机构申请机构证书时，由机构授权人员申请。

设备证书由域名或设备拥有机构，或获得域名或设备使用授权的机构中的授权人申请。申请者填写《设备数字证书申请表》，并提供申请个人或申请机构的身份证明文件及其复印件一份。身份证明文件参照个人证书和机构证书的要求。

3.1.2 证书申请实体

在证书申请的过程中，参与整个申请过程的实体主要包括:

- 1、证书申请者，包含个人、企事业单位和政府机构、社会团体、人民团体等各类组织机构。任何合法的组织、个人和有明确身份归属的其他网络主体均可申请数字证书，以保证网上交易和网上行政作业的安全和可靠。
- 2、沃通授权服务受理机构，包括 RA 以及证书代理商等，以及相应的系统、系统管理员、操作员等。
- 3、电子认证服务机构，包括沃通以及沃通授权的下级操作子 CA 等。
- 4、证书使用方，发证书构已经为其颁发证书，并不依赖于其是否已经接受证书。

3.1.3 注册过程与责任

证书申请者可到沃通的注册服务站点、或其授权注册机构的注册服务站点，申请各类证书。

对于电子邮件证书，注册时申请者须正确填写正确的电子邮件地址；对于账户证书，注册时申请者须正确填写正确的账户信息，如帐号名等。

对于机构证书，注册时申请者须正确填写以下信息：

1）机构的真实身份标识信息，如机构法定名称、组织机构代码、税号等；

2）机构授权的申请人信息，如姓名、电话、邮件地址等。

对于个人证书，注册时申请者须正确填写以下信息：

1）个人的真实身份标识信息，如个人真实姓名、身份证号码、所属机构（若需要）等；

2）其他信息，如邮件地址等。

对于服务器证书和运营设备证书，注册时申请者须正确填写以下信息：

1）服务器主机名、域名、IP 地址、或设备名称、及所有者信息等；

2）申请人信息，如姓名、电话、邮件地址等。

对于管理员证书，注册时申请者须正确填写以下信息：

1）个人的真实身份标识信息，如个人真实姓名、所属机构、身份证号码等；

2）其他信息，如邮件地址等。

根据《中华人民共和国电子签名法》的规定，申请者未向沃通提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、沃通造成损失的，承担相应的法律及赔偿责任。

3.2 证书申请处理

3.2.1 执行识别与鉴别功能

沃通和其授权的证书服务机构，有权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，证书审计表应记录鉴别人的姓名、签名、验证结果和验证日期。

在接到证书使用方的证书申请后，发证机构应完成以下鉴别工作，将其作为向该证书使用方颁发证书的先决条件：

- 确认证书申请者接受证书使用方协议中的各项条款。
- 根据证书申请者所申请的证书种类，按照各类证书的不同鉴别要求对证书申请者的身份进行验证。
- 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（可根据证书种类不同采用不同的确认方法，如要求证书使用方做出保证等方式）。
- 确认证书中包含的信息，都是准确的。
- 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。
- 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。

在颁发了证书后，除非被通知该证书发生了本 CPS 所述的安全损害情况，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。

沃通和其授权的证书服务机构的审核人员合理、审慎地进行申请者身份鉴别，并进行批准或拒绝的操作。

对于申请单位和个人提交给沃通及其授权的证书服务机构的所有申请材料，沃通及其授权的证书服务机构都必须确保申请材料的安全，必须由至少 2 人以上负责对申请材料的处理，包括但不限于：材料审核、调阅、归档保存、销毁等。

3.2.2 证书申请批准和拒绝

沃通及其授权的证书服务机构收到申请，对申请信息及身份信息进行完整性、有效性、可靠性和真实性的鉴别，准确无误后，将批准该申请。沃通及其授权的证书服务机构依照电子政务 CPS 的规定为申请者颁发一张证书以证明已经批准了申请者的证书申请。

- 该申请完全满足前面 2.2 条款关于证书使用方信息的标识和鉴别规定
- 该申请必须满足最新的相关要求。
- 申请者接受或者没有违反对证书使用方协议的内容和要求
- 申请者已经按照规定支付了相应的费用，另有协议规定的情况除外

当沃通及其授权的证书服务机构在进行鉴别程序时，如果申请者未能成功通过鉴别，沃通及其授权的证书服务机构将拒绝申请者的证书申请，并立即通知申请者鉴别失败。对于鉴别失败的原因，沃通有权拒绝解释，并且不需要通知申请者。法律法规对此有明确要求的除外。

3.2.3 处理证书申请的时间

沃通及注册机构将在合理时间内完成证书请求处理。在申请者提交资料齐全且符合要求的情况下，处理证书申请的时间不超过 2 个工作日。

3.2.4 告知证书申请的结果

依据鉴别的结果，沃通会及时向证书申请者做出接受或拒绝证书申请的决定，并通过面对面、电话、邮件或书面通知等方式通知证书申请者结果及相应的原因。如：无法完成鉴别和验证身份信息；用户没有提交所规定的文件；用户没有在规定时间内回复通知；未收到证书费用等等。

若沃通接受了证书申请并成功通过了鉴别，则沃通会妥善保管证书申请者提交的所有用于鉴别的材料。

3.3 证书颁发

3.3.1 证书颁发中注册机构和认证机构的行为

作为证书认证系统的运营者，沃通既是一个认证机构（CA），同时也承担了部分注册机构（RA）的职能（如负责设备证书的注册、审批等）。另外，沃通授权的机构也承担相应的注册机构职能，如接收、处理证书服务请求。

在证书颁发前 RA 管理员负责证书申请的鉴别，在证书申请通过鉴别后，RA 管理员将批准证书请求。在批准证书申请时，RA 管理员使用证书登录到 RA 系统，查询系统记录的有关请求并批准该请求。批准的信息将会发送到沃通的 CA 系统，CA 系统颁发证书并返回给 RA 系统供证书申请者下载。

3.3.2 认证机构和注册机构对用户的通告方式

如果证书申请获得批准并颁发，RA 将通过多种方式告诉证书申请者如何获取证书。

沃通对证书申请者的通告提供以下几种方式：

1) 电子或纸质的受理回执；
2) 电子邮件（e-mail）；
3) 通过面对面的方式，通知证书持有者（如申请者到受理点领取等方式）；
4) 其他沃通认为安全可行的方式。

3.3.3 证书获取方式

沃通对于已经签发的证书提供 3 种获取方式：

1、用户到沃通的受理点，通过身份鉴别后，由系统在 USB-Key 中产生密钥对，生成证书；

2、通过身份鉴别后，由沃通的鉴别人员，使用 USB-Key 产生密钥对并生成证书，然后通过邮寄或快递的方式将 USB-Key 交付给证书申请者；

3、由用户在安全可靠的环境中使用可以证明 CSR 是从 USB Key 中生成的有国密型号的 USB Key 生成私钥和 CSR 文件，并在沃通官网通过 HTTPS 提交，通过身份鉴别后，沃通将已签发的公钥证书文件通过 https 的方式传递给用户，由用户在安全可靠的环境中导入到原先生成 CSR 的 USB Key 中。

3.4 证书接受

3.4.1 构成接受证书的行为

沃通证书使用方接受证书的方式可以有如下几种：

对于由注册机构替证书使用方产生证书请求、证书密钥对、下载证书的情形，则证书使用方通过面对面的方式从注册机构（沃通或其注册机构）接受载有证书和私钥的介质的行为，即表明了用户接受了证书；当证书使用方获取含有证书和私钥的介质后，在约定的时间内未表示异议，即表明用户接受了证书。

证书使用方根据电子邮件中的获取证书的的指示信息，访问专门的证书下载服务站点将证书下载到本地存放介质，如本地计算机硬盘、USB Key、智能卡。系统记录证书使用方下载了证书即表明证书使用方接受了证书。

3.4.2 认证机构对证书的发布

沃通有基于 LDAP 协议的目录服务，除非与证书使用方之间有特别的约定，沃通通常将其颁发的证书发布到目录系统上。

3.5 密钥对和证书使用

密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用是不受相关法律和沃通策略保障的。

3.5.1 用户私钥和证书使用

对于签名证书，其私钥可用于对信息的签名。在可能的情况下，签名证书及信任链上的证书（根证书除外）应同被签名信息一起提交给依赖方。证书持有者使用私钥对信息签名时，应该被告知并确认签名的内容。对于具有身份鉴别用途的证书，其私钥可用于对鉴别方提交的挑战信息进行签名；在可能的情况下，具有身份鉴别用途的证书及信任链上的证书（根证书除外）应提交给验证方。对于加密证书，其私钥可用于对采用对应公钥加密的信息解密。证书持有者应妥善保管其证书私钥。

3.5.2 依赖方公钥和证书使用

当依赖方接受到经数字签名的信息后，应该：

(1) 获得数字签名对应的证书及信任链；

(2) 确认该签名对应的证书是依赖方信任的证书；

(3) 证书的用途适用于对应的签名。

(4) 使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

当依赖方需要发送加密信息给接收方时，须先通过适当的途径获得接收方的加密证书，后使用证书上的公钥对信息加密。依赖方应将加密证书连同加密信息一起发送给接收方。

3.6 密钥更新

3.6.1 密钥更新的情形

沃通证书密钥更新包括但不限于以下情形：

1、证书私钥泄露和撤销证书；

2、证书到期；

3、证书密钥到期；

4、基于证书、政策安全等原因，沃通要求证书密钥更新。

出现上述情况，除非证书持有者特别要求，沃通一般不建议证书持有者不进行证书密钥更新操作，而是撤销原有证书，重新申请新的证书。

3.6.2 证书更新的情形

对于沃通颁发的任何最终用户证书，证书到期前 30 天系统将会自动发邮件给证书使用方提醒用户证书将到期，如需继续使用可进行证书更新。到期前 30 天内，如果证书使用方原来的注册信息继续有效，证书使用方可访问沃通或注册机构的证书更新站点申请证书更新。申请证书更新时用户无需象初次申请那样填写注册信息，系统会自动获取所需的信息。证书更新可以更换密钥对，也可以使用原有密钥对，视更新的具体情形而定，关于证书更新与重新申请一个同样主体甄别名的新证书区别见本电子政务 CPS 2.3。

若用户需要改变注册信息，则不能更新证书，需按新证书申请流程进行。

证书到期或撤销后，将无法进行更新，只能按照初始流程重新申请证书。

3.6.3 更新申请的提交

证书持有者、证书持有者的授权代表（如机构证书等）或证书对应实体的拥有者（如设备证书等）在证书满足更新条件时，应按要求向沃通或其注册机构提出更新申请。更新申请可以采取面对面提交申请表或者在线提交带有证书持有者数字签名的更新申请。

3.6.4 更新申请的鉴别

对于不更换密钥的证书更新请求，用户提交的证书签名请求（PKCS#10）包含有原有证书的公钥，并由原证书私钥签名。 接收到用户的证书更新请求后，沃通会完成如下验证操作：

- 确认、验证申请对应的原证书存在并且由沃通认证机构颁发；
- 证书更新请求在允许的期限内；
- 用原证书上的证书使用方公钥对更新申请的签名进行验证。

若以上验证通过，则沃通或其注册机构根据证书种类的不同，分别按如下方式和过程完成证书更新请

求的鉴别、批准，及新证书的颁发。

对于机构证书（包括机构单位证书和机构代表人证书）和设备证书（包括服务器证书和运营设备证书）根据用户以前提交的注册信息，按与新证书申请一样的流程完成证书申请的鉴别，包括机构身份信息正确性、有效性的验证和确认，证书申请人及证书申请授权的确认等。在进行鉴别时，若机构用户以前提交的机构身份证明文件（如组织机构代码、营业执照）仍在其有效期内，则更新申请人无需重新提交有关的机构身份证明文件，但沃通或其注册机构仍会通过第三方数据库确认有关材料是否继续有效。完成以上鉴别后，批准更新请求，颁发新证书。

对于电子邮件证书，其更新请求的鉴别、批准，更新证书的颁发与新证书申请完全相同。

对于账户证书的更新，则只需完成如下确认就可批准更新请求，颁发新证书：

1）该证书对应的账户依然有效；

2）该账户被允许更新证书。

以上过程可以是自动或手动。

对于个人用户证书的更新，若包含在证书中的需鉴别的信息不包含该证书用户所属组织机构，则只要该证书用户履行了应尽的责任（如支付了有关费用），则证书更新请求将获得批准，新证书将获得颁发。以上过程可以是自动或手动的。若包含在证书中的需鉴别的信息包含该证书用户所属组织机构，则在批准更新请求、颁发新证书前，需要确认该证书用户仍然是所属机构的人员。

对于机构雇员证书的更新，则在完成如下确认后，批准证书更新请求，颁发新证书：

1）该证书用户仍然是对应机构的雇员；

2）该用户的证书更新获得了该机构的许可。

对于更换密钥的证书更新，参见 3.7.3。

3.6.5 密钥更新方式

沃通提供的密钥更新方式包括但不限以下方式：

1、到沃通或其受理点进行面对面的更新方式；

2、通过系统提交申请，在线的自动更新方式。

3.6.6 通知证书持有者密钥更新

同本电子政务 CPS 3.3.2。

3.6.7 构成接受密钥更新的行为

同本电子政务 CPS 3.4.1。

3.6.8 认证机构对密钥更新的发布

同本电子政务 3.4.2。

3.7 证书变更

3.7.1 证书变更的情形

证书变更是指在证书未到期之前，更改除公钥及有效期之外的其他信息。沃通的认证业务不直接支持证书变更。证书使用方要变更证书中的内容时，视为申请一张新证书，需要先将原有证书撤销，才能申请新证书，且证书的申请及处理流程与申请新证书一致。

3.7.2 证书变更的申请

同本电子政务 CPS 3.6.3。

3.7.3 证书变更的辨别

同本电子政务 CPS 3.6.4。

3.7.4 证书变更的受理方式

同本电子政务 CPS 3.6.5。

3.7.5 通知证书持有者证书变更

同本电子政务 CPS 3.6.6。

3.7.6 构成接受证书变更的行为

同本电子政务 CPS 3.6.7。

3.7.7 认证机构对变更证书的发布

同本电子政务 CPS 3.6.8。

3.8 证书撤销

3.8.1 证书撤销的情形

出现以下情况，最终用户证书必须撤销：

- 沃通、注册机构或证书使用方有理由相信或强烈的怀疑一个证书使用方的私钥安全已经受到损害。
- 沃通或其注册机构有理由相信证书使用方违背了证书使用方协议下的义务、陈述或担保。
- 沃通或其注册机构和证书使用方达成的证书使用方协议已经终止。
- 沃通或其注册机构有理由相信证书颁发时没有依据 CP、CPS 规定的有关程序，证书颁发给了非证书主体的人员或机构或没有鉴别该人员或机构在证书主体中的命名就颁发了证书）。
- 沃通或其注册机构有理由相信证书申请中的信息有违背事实的错误。
- 沃通或其注册机构确定证书颁发的一个必要前提条件既没有满足又没有豁免。
- 除了未经鉴别的证书使用方信息外，包含在证书中的信息不正确或已经改变。
- 证书使用方请求撤销证书。

3.8.2 可以发起请求撤销证书的实体

以下实体可以请求撤销一个最终用户证书：

- 沃通、注册机构或证书使用方可以在 3.8.1 所述情形下要求撤销一个最终用户证书。
- 对于电子邮件证书、账户证书、个人证书，证书使用方可以随时根据自己的意愿请求撤销自己的证书。
- 对于机构证书，组织机构授权的代表有资格请求撤销颁发给组织机构的证书。
- 对于设备证书，拥有该设备证书的组织机构授权的代表有资格请求撤销已经颁发的证书。
- 司法取证人员

3.8.3 证书撤销的申请

当沃通或其注册机构有充分的理由相信需要撤销证书使用方的证书时，沃通或其注册机构的有关人员可以通过内部确定的流程提请撤销证书。在证书撤销后，沃通或其注册机构将通过适当的方式，包括邮件、传真等，通知证书使用方证书已被撤销及被撤销的理由。

证书使用方可以通过以下方式要求撤销自己的证书：

- 直接提交撤销申请材料。
- 通过电子邮件、传真、特快专递等可靠的方式告知沃通或其注册机构。

3.8.4 证书撤销的鉴别

同本电子政务 CPS 3.6.4。

3.8.5 证书撤销受理方式

同本电子政务 CPS 3.6.5。

3.8.6 认证机构处理撤销请求时限

沃通或注册机构从接到撤销请求到完成处理请求的时间如下：

- 对于电子邮件证书和账户证书不能超过 24 小时。
- 对于个人证书不能超过 8 小时。
- 对于机构证书和设备证书不能超过 4 小时。

3.8.7 通知证书持有者证书撤销

同本电子政务 CPS 3.6.6。

3.8.8 构成接受证书撤销的行为

同本电子政务 CPS 3.6.7。

3.8.9 认证机构对证书撤销的发布

证书被吊销后，系统会将证书信息写入 CRL 中，并每 24 小时对外发布一次 CRL。依赖方可以通过查 CRL 列表来获得证书吊销情况。

3.8.10 CRL 发布频率

沃通每 24 小时发布一次 CRL，特殊紧急情况下可以立即签发 CRL。

3.8.11 CRL 发布的最大滞后时间

一个证书从它被撤销到它被发布到 CRL 上的滞后时间不超过 24 小时。

3.8.12 在线状态查询的可用性

沃通提供证书状态的在线查询服务，该服务 7X24 小时可获得。

3.8.13 在线状态查询要求

依赖方应检查证书的撤销状态。如果依赖方未通过 CRL 方式查询，则应通过在线存储库的方式查询。

3.9 密钥生成、备份与恢复

证书使用方加密证书密钥对可以由沃通的密钥管理中心系统集中安全产生和保存，密钥恢复是一种严格受控的过程，只有在如下情况下才允许进行密钥恢复：

1）证书持有者提出申请；

2）注册机构提出申请，并有充分的理由；

3）国家执法、司法机构因执法、司法的需要；

4）国家其他管理部门管理需要。

密钥恢复只有在必须的情况下才进行，并且申请要提出充分的理由和提供有关文件、材料。

3.9.1 证书持有者密钥恢复

当证书持有者的密钥损坏或丢失后，某些密文数据将无法还原，此时证书持有者可申请密钥恢复。证书持有者向认证机构提交申请，经审核后，通过认证机构向密钥管理基础设施发送请求；密钥恢复模块接受证书持有者的恢复请求，恢复证书持有者的密钥并下载于证书持有者证书载体中。

3.9.2 问责取证密钥恢复

问责取证人员向密钥管理基础设施提交申请，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。

4. 应用集成支持与信息服务操作规则

4.1 服务策略和流程

沃通根据自身的实际情况，制定了服务策略和流程，具体如下：

1、制定证书应用实施的管理策略和流程，对业务系统进行充分调研，指导或参与业务系统证书应用部分的开发和实施；

2、制定项目管理制度，规范系统和程序开发行为；

3、制定安全控制流程，明确人员职责；

4、实施证书软件发布版本管理，并进行证书应用环境控制；

5、对项目开发程序和文档等资料进行妥善归档保存。

4.2 应用接口

沃通提供应用接口程序供应用系统集成和调用。证书应用接口程序符合《电子政务数字证书应用接口规范》，包括证书环境设置、证书解析、随机数生成、签名验证、加解密、时间戳以及数据服务接口等功能。

沃通提供的证书应用接口程序支持 Windows、AIX、Solaris、Linux 等多种系统平台，并提供 C、C#、Java 等多种接口形态，可通过 com 组件、java 组件、ActiveX 控件、Applet 插件等多种形态提供服务。

4.2.1 密码设备调用接口

沃通提供服务器端密码设备的底层应用接口和客户端证书介质（如：USB Key）的底层应用接口。并且服务器端密码设备的底层应用接口应符合 GM/T 0018 的要求；客户端证书介质的底层应用接口应符合 GM/T 0016 和 GM/T 0017 的要求。

4.2.2 密码模块安全技术接口

沃通正积极研究 GM/T 0028 和 GM/T 0054 的要求，采用新模式与新技术密码模块安全技术接口来提供服务。

4.2.3 通用密码服务接口

沃通使用符合 GM/T 0019 的要求的通用密码服务接口，从而为各类密码服务层和应用层提供统一的通用密码服务接口。

4.3 集成内容

沃通具备面向各类应用的证书应用接口集成能力，并能够达到以下要求：

1、具备在多种应用环境下进行系统集成的技术能力，包括基于 B/S 应用模式（支持 Java、.NET asp 等开发语言）以及基于 C/S 应用模式（支持 C、VC 等开发语言）的系统集成能力。

2、提供满足不同应用系统平台的证书应用接口组件包，包括 com 组件、java 组件、ActiveX 控件、Applet 插件等。

3、提供集成辅助服务，包括接口说明、集成手册、测试证书、集成示例、演示 DEMO 等。

4.4 信息服务内容

4.4.1 证书信息服务

沃通 CA 系统中签发、更新的数字证书，可实时或定时与电子政务信息系统进行数据同步，实现将证书信息同步到电子政务信息系统中。沃通提交的数据包括业务类型、认证机构身份标识、用户基本信息、用户证书信息等。

4.4.2 CRL 信息服务

沃通在证书持有者证书吊销时，系统自动将该证书吊销信息公布，CRL 发布周期为 24 小时，即在 24 小时内发布最新 CRL。

4.4.3 服务支持信息服务

沃通以页面和服务的形式提供查询服务，接口符合《电子政务数字证书应用接口规范》的要求。

4.4.4 决策支持信息服务

沃通面向电子政务应用单位、政府监管机构提供决策支持信息，包括用户档案信息、投诉处理信息、客户满意度信息、服务效率信息等。

4.5 信息服务管理规则

沃通在提供信息服务时，做好相关信息的隐私保障机制，实现信息保护对用户的承诺。沃通对技术、客服等凡是能够接触用户信息的工作人员进行保密培训，并签署保密协议，严禁泄露或私自使用用户信息和业务信息。

1、私有信息类型的敏感度

对于以下信息，沃通按照日常安全保密制度严格执行：

1) 企业、政府主管单位、政府办公人员等的隐私信息；

2) 集成商、应用系统开发商、合作伙伴等的商业秘密；

3) 政府部门的敏感信息和工作秘密。

证书发行过程中涉及的用户申请信息都是敏感信息，而发布的证书和 CRL 信息不属于敏感信息。

2、允许的私有信息收集

沃通仅允许在证书发行和管理时才能收集私有信息，且只收集对发行和使用证书有用的私有信息。除了有特殊要求外，沃通不收集更多的私有信息。

3、允许的私有信息使用

沃通承诺只使用在 CA 或 RA 中收集的私有信息。若在某项业务中开展证书应用而获得的私有信息，在使用时，必须获得该业务应用单位的许可。

4. 允许的个人信息发布

沃通和注册机构仅能面向证书应用单位发布与之相关的私有信息，以协助证书应用单位进行证书业务管理。在特别紧急的情况下，沃通经管理机构授权可发布私有信息。任何特定的私有信息发布应遵循相关法律和政策执行。

5. 所有者纠正私有信息的机会

沃通允许用户在其证书生命周期内对其私有信息进行更正。

6. 对司法及监管机构发布私有信息

沃通或注册机构在以下情况下，可执行将私有信息发给获得相应授权的人员：

1) 根据国家相关法律法规，为司法机关提供私有信息；

2) 在私有信息所有者同意的情况下，可将私有信息提供给相应授权的人员；

3) 按照明确的法定权限的要求或许可。

4.6 信息服务方式

4.6.1 证书信息同步服务

沃通采用 API 接口技术实现 CA 系统与电子政务信息系统的证书应用同步。电子政务信息系统通过部署统一的接口，认证机构的 CA 系统通过调用统一的同步接口，实现 CA 系统向电子政务信息系统进行证书信息的自动同步功能。同时，为了保证数据传输的安全性，通过对通信数据添加数字签名，以防止数据在传输中被篡改或损坏。

4.6.2 CRL 信息同步服务

将 CA 系统与电子政务信息系统的 CRL 同步。CA 系统主动调用该接口，实时将最新的 CRL 文件同步到电子政务信息系统中。

为了提高 CRL 文件传输的安全性，对发送的 CRL 数据进行数字签名，电子政务信息系统只需要根据认证机构身份标识找到对应的根证书链，验证 CRL 签名的有效性即可确定 CRL 的有效性。

CRL 发布周期为每 24 小时一次。

4.6.3 服务支持信息服务

1、沃通通过 WEB 网站等面向电子政务用户发布如下信息：

（1）电子政务电子认证服务业务规则；

（2）证书生命周期服务流程及相关费用；

（3）证书用户操作手册；

（4）证书常见问题解答（FAQ）；

（5）获得证书帮助联系方式（用户服务方式、办公地址、邮政编码、投诉电话等）；

（6）其他应该发布的相关信息。

2、沃通通过 WEB 网站面向电子政务应用系统集成商发布如下信息：

（1）数字证书应用接口软件包；

（2）数字证书应用接口实施指南；

（3）证书常见问题解答（FAQ）；

（4）获得证书帮助联系方式（用户服务方式、办公地址、邮政编码、投诉电话等）；

（5）其他应该发布的相关信息。

3、沃通通过 WEB 网站面向电子政务应用系统发布如下信息：

（1）时间戳服务数据接口；

（2）HTTP 协议的 CRL 发布服务接口；

（3）LDAP 协议的证书发布接口。

4.6.4 决策支持信息服务

沃通面向证书应用单位以接口等方式提供如下信息服务：

（1）用户档案信息：分业务、地域、时段等要素提供用户信息的统计分析服务；

（2）投诉处理信息：提供特定业务、时间、特定用户群、问题类型等的投诉处理汇总信息及分析；

（3）用户满意度信息：提供面向业务的用户满意度调查信息；

（4）服务效率信息：提供面向业务的服务效率分析信息，如处理时间、服务接通率等。

5. 使用支持服务操作规则

5.1 服务内容

使用支持服务是沃通面向证书使用用户（即证书申请者、证书持用者）及证书应用单位提供的一系列售后服务及技术支持工作。

服务内容包括：数字证书管理、数字证书使用、证书存储介质硬件设备使用、电子认证服务支撑平台使用，以及各类数字证书应用（如证书登录、证书加密、数字签名）等贯穿证书使用和应用过程中的所有问题。

5.1.1 面向证书持有者的服务支持

数字证书管理：包括数字证书的导入、导出，以及客户端证书管理工具的安装、使用、卸载等。

数字证书应用：基于数字证书的身份认证、电子签名、加解密等应用过程中出现的各种异常问题，如：证书无法读取、签名失败、证书验证失败等。

证书存储介质硬件设备使用：包括证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等。

电子认证服务支撑平台使用：为用户提供在沃通的数字证书在线服务平台中使用的各类问题，如：证书更新失败、下载异常、无法提交撤销申请等。

5.1.2 面向应用提供方的服务支持

电子认证软件系统使用：提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等系统的使用

支持问题，如证书信息无法查询、数据同步失败、服务无响应等。

电子签名服务中间件的应用：解决服务中间件在集成时出现的各种情况，如客户端平台适用性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

5.2 服务方式

沃通提供多种服务方式，包括坐席服务、在线服务、现场服务等在沃通官网上可查询相应的服务方式。

沃通建立了完善的服务保障体系，包括建立专业的服务队伍、服务规范、知识库、服务跟踪系统、满意度调查、投诉受理等。服务保障体系应根据服务业务的变化及时更新。

5.2.1 坐席服务

用户拨打沃通 24 小时服务热线，客服人员和值班人员根据用户的问题请求，协助用户处理。

5.2.2 在线服务

在线服务通过提供网络实时通讯系统、远程终端协助系统，以及在线帮助与传统模式的结合，满足用户多种服务帮助的需求。

网络实时通讯系统：用户通过在线帮助网站远程发起支持请求，网站客服人员能够第一时间同登陆网站的访客取得联系，进行交流。

远程终端协助系统：用户通过安装远程终端软件，可以通过互联网或者局域网向客户服务人员发起协助请求。由服务人员通过远程终端控制功能，实时检测用户的软件硬件环境，通过同屏显示指导、帮助用户解决应用故障。

在线帮助与传统模式的结合：将在线服务系统与电话服务结合，方便客户既可以打电话、也可以自助上网，随时查询自己的服务记录、请求处理状态、产品配置信息等等。

5.2.3 现场服务

根据用户的实际需求，由技术支持工程师上门现场为用户处理数字证书应用中存在的问题。

5.2.4 满意度调查

通过多种用户可接受的调查方式进行客户回访，包括电话、WEB 网站、邮件系统、短信、传真等。对用户进行回访，并进行满意度调查。并将用户回访中产生的相关文档进行归档、保存。

5.2.5 投诉受理

向用户公布电子政务电子认证服务监管部门的投诉受理方式。可通过电话、网站平台、电子邮件、即时通讯工具等方式及时接受客户投诉，投诉受理过程中应记录投诉问题，并将结果及时反馈给用户。将投诉受理中产生的相关文档进行归档、保存。

5.2.6 培训

培训方式由沃通与客户双方约定的形式开展。

培训内容主要包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答、操作手册等。

5.3 服务质量

沃通坐席服务、在线服务、现场服务时间做到充分满足各类用户的需要。服务时间至少是 5 天*8 小时，热线电话服务时间是 7 天*24 小时不间断服务。沃通设有专门的投诉受理热线，承诺在 1 个工作日内进行投诉处理；沃通制定了用户培训意见反馈表，对培训效果进行评估，并做出相应处理，保证优质的客户服务质量。沃通对技术问题和技术故障按照一般事件、严重事件、重大事件进行分类，制定响应处理流程和机制，以确保服务的及时性和连续性。

6. 认证机构设施、管理和操作控制

6.1 物理控制

6.1.1 场地位置与建筑

沃通认证中心的运营场地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#。

沃通认证业务的运营场地是按照相关规范进行构建的，整体建筑由能够阻止物理穿透的材料建成。建筑物的外墙、地板和天花板都属于永久性建造，并互相联结，可以阻止未经过授权的进入、穿透。敏感区域及以上区域的墙壁，在其双层干饰面内墙之间，采用镀钢夹层。敏感区域只设置一个门作为的常规入口。根据消防要求置了消防紧急出口。敏感区域及以上区域没有窗口。通风孔、管道口或任何类似的通向敏感区域的孔口都采用了硬金属条进行加固。

运营场地位的物理安全是基于物理层级的保护，每一物理层就是一个屏障，设置了可以控制进出的带锁的门来控制每个人进出每一个区域。每一层区域有非常严格的控制方法防止未经授权的物理访问，而且每一个物理安全层在物理上完全包含下一个物理安全层，内部的安全层不与外部的安全层使用一样外部墙体，最外层的安全层是整个建筑物的外墙。

沃通认证机构的运营场地能达到以下安全和控制风险要求：

- 防止物理非法进入

七层物理结构及完善的安全管理体系保护沃通的运营设施安全。

- 防止未经过授权的物理访问

确保未经过授权的人，或仅被授权访问有限物理区域的人员，不得访问沃通认证机构内的受限制区域。

- 维护CA服务的完整性、可用性

保障提供CA服务的系统、设施不受到破坏，保证认证服务不被中断。

6.1.2 物理访问控制

沃通的物理设施的访问控制系统是与控制各层门进出的门禁系统相结合的，并实现了以下安全功能：

- 进出每一道门都有记录作为审计依据；
- 系统采用身份识别卡和生物识别鉴定的控制方法，控制关键的进出门；

- 所有关键区域的门都设有强行开门报警。
- 整套访问控制系统配有断电保护装置，还配有 UPS 提供紧急用电；

与门禁系统配合使用的还有录像监控系统，所有的录像资料根据安全审计要求保留一段时间。

6.1.3 电力与空调

沃通有安全、可靠的电力供电系统及电力备用系统以确保系统 7X24 小时正常供电及在出现供电系统出现供电中断是能够提供正常的服务。另外，对于机房中的各个区域，均使用了单独的空调进行温度控制，同时，核心区还加装了通风装置，以确保温度和湿度符合规范要求。

6.1.4 水患防治

沃通机房四周的墙体均没有水管穿过，服务器和网络设备等都采用了离地机架部署，地面没有部署强电和弱电，并且地面都采用了防水处理措施，以确保机房不会遭受水患威胁。

6.1.5 火灾预防和保护

6.1.5.1 结构防火

沃通认证机构的运营中心耐火等级符合 GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级，防护方法应符合当地管理部门或机构的安全要求。

6.1.5.2 火灾报警及消防设施

- 沃通认证机构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。
- 敏感区及高敏区配置了独立的气体灭火装置。

6.1.5.3 紧急出口

根据国家的有关消防要求、规定和标准，在非敏感区及敏感区的办公区域内，设置了紧急出口，紧急出口设有消防门。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。紧急出口门外部没有

门开启的装置，且紧急出口门与门禁报警设备联动外。非紧急避险状态下，紧急出口门不能被内部人员任意打开。

6.1.6 介质存储

沃通认证机构对储存产品软件和数据、归档、审计或备份信息的介质保存在安全设施中，这些设施受到适当的物理和逻辑访问控制的保护，只允许授权人员的访问，并防止这些介质受到意外损坏（如水、火灾和电磁）。

6.1.7 废物处理

沃通对敏感的文件和材料在处理之前将其使用碎纸机进行粉碎处理，使信息无法恢复。密码设备在作废处置前根据制造商的指南将其物理销毁或初始化。其他存储介质（硬盘、USB Key、智能卡）作废处理将进行物理性粉碎。

6.1.8 异地备份

沃通认证机构对关键系统数据、审计日志数据和其他敏感信息进行日常备份，这些备份信息保存在沃通北京机房的安全的地方。

6.1.9 入侵侦测报警系统

机房区域安装了入侵侦测报警系统，进行安全布防。机房区域、办公区域、公共区域等各区域安装了高清摄像头，并启用了移动侦测报警功能。

6.2 操作过程控制

6.2.1 可信角色

在沃通提供的电子政务电子认证服务过程中，能从本质上影响证书的颁发、使用、管理和撤销等涉及密钥操作的职位都被沃通视为可信角色。这些角色包括但不限于：密钥和密码设备的管理员、系统管理员、

安全审计人员、业务管理人员及业务操作人员等，具体岗位名称和要求以沃通的岗位说明书为准。

6.2.2 角色的识别与鉴别

所有沃通的在职人员，必须通过认证后，根据岗位性质和职位权限的需要，发放系统操作卡、门禁卡、登录密码、操作证书、系统账号等安全令牌。对于使用安全令牌的员工，沃通系统将独立完整地记录其所有的操作行为。

所有沃通职位人员必须确保：

1) 根据岗位安全等级的不同，进行不同程度层次的身份识别和鉴别措施；
2) 基本的身份审查措施，确保符合岗位可信资格；
3) 赋予可信员工相应的权限区分，为其发放安全令牌；
4) 发放的安全令牌直接属于个人或组织所有；
5) 发放的安全令牌不允许共享。沃通的系统和程序通过识别不同的令牌，对操作者进行权限控制。

6.2.3 角色职责分离设置

所谓职责分离，是指如果一个人担任了完成某一职能的角色，就不能再担任完成另一特定职能的角色。沃通对如下人员进行了职责分割：

- 业务管理员
- 模板管理员
- 业务制证员
- 超级管理员
- 系统管理员
- 审计管理员

6.3 人员控制

6.3.1 可信人员要求

在沃通中担任一定角色、执行一定功能、完成一定工作的人员，其所受教育、培训及工作经历应足够胜任其工作。

沃通客户服务人员必须受过专门的客户服务技能培训，通过 PKI 及相关应用基本知识培训，熟悉有关证书业务，考试通过后方能进行有关工作。这些培训和考试由沃通负责。 沃通安全管理人员必须熟悉、掌握有关的安全知识和安全管理，熟悉沃通安全要求，熟悉沃通安全与审计指南，有很强的责任感。为了达到此要求，沃通将对安全管理人员进行培训。

沃通密钥与密码设备管理人员必须熟悉 PKI 基本知识，熟悉 CA 证书和密钥相关的证书，如 CA 证书的产生、颁发、更新、密钥更新等，熟悉有关密码设备操作使用。 沃通所有的可信人员必须符合清白要求：没有伪造教育、工作经历，没有违法犯罪记录，工作中没有严重的不诚实行为。

6.3.2 可信人员背景审查

为了确保担任可信角色的人员能够胜任有关工作，沃通将按照《员工手册》《安全策略》等对雇佣的人员先进行背景调查。在成为沃通的可信人员前，有关人员必须提交相关材料，以证明他们能够胜任预期的工作。沃通依据有关材料进行背景调查，在调查过程中，沃通将为有关人员保密，保护其隐私。

背景调查时如果出现提交材料与事实不符或证明提交材料为伪造时，沃通将拒绝可信职位候选人获得有关职位或取消其可信人员的资格。

6.3.3 人员培训及再培训

为了使有关人员能胜任其承担的工作，沃通对所有入职员工制定有专门的培训计划，培训内容包括：

- 本人工作职责。
- 安全管理要求及制度。
- 事故和安全威胁的报告和处理。

对于销售、服务和支持还包括：

- PKI 及应用。
- 沃通的产品与服务。
- 客户服务流程与要求（客户服务）。
- 安全操作流程（系统、密钥）。

根据沃通策略调整、系统更新等情况，沃通将对员工进行继续培训，以适应新的变化。

6.3.4 工作岗位轮换周期和顺序

根据实际情况进行内部安排，至少每年轮换一次。

6.3.5 违规行为处罚

沃通对于未授权行为或其他违反公司安全策略和程序的行为制定有相应的处罚措施，包括警告、罚款直至辞退，情节严重的将依法追究刑事责任。

6.3.6 外包服务人员及要求

沃通不允许外包服务人员担任可信职位。任何外包服务人员在某一职务的职能和安全标准应与相应职位的内部雇员一样。

外包服务人员进入敏感区时，只能在认证机构人员的陪同和直接监督下访问认证机构的安全设施，完成有关的工作。

6.3.7 提供给员工的文档及保密策略

提供给员工的文档通常包括员工培训资料及员工工作手册等，这些资料通常是不公开的。机密文档用证书加密，仅限于公司办公电脑阅读。

6.4 审计日志程序

6.4.1 审计日志定义

本电子政务 CPS 中所述的审计日志，是指在整个电子政务电子认证业务过程中，涉及证书生命周期管理、加密设备生命周期管理、密钥生命周期管理以及用户资料管理等过程所有产生的所有操作记录，这些记录可能会以纸质或电子的形式存在。

6.4.2 审计日志安全检查与风险评估

内部审计人员需要定期对所有的审计日志进行审查，评估安全策略和操作流程的执行情况，从而对运

营风险进行评估。

6.4.3 审计日志记录要求

沃通能够准确完整地记录电子政务电子认证所涉及运营条件和环境、密钥和证书生命周期管理的日志和事件。

6.4.4 审计日志处理或归档周期

沃通所记录的各类日志、安全事件的记录都在安全和公正的情况下以自动或手动方式产生，并定期归档。只有被授权的安全管理人员才能定期检阅记录和跟进有关事项。

6.4.5 审计日志检测系统

沃通在系统层面就已经做了访问控制，从而确保不会发生非授权的访问行为。

6.5 规定事件记录的类型

沃通对以下事件进行记录，记录以纸质或者电子等形式进行：

1、注册系统和证书受理操作的相关授权记录及管理记录；

2、密钥生成、备份、存储、撤销、归档和销毁管理；

3、密码设备生命周期管理；

4、证书申请、密钥更新、证书变更和证书撤销管理；

5、证书签发和 CRL 列表生成；

6、PKI 系统访问；

7、操作 PKI 系统和其他安全系统的行为；

8、安全配置文件变更；

9、系统崩溃、硬件故障和其他异常；

10、防火墙和路由器的工作情况，机房进出访问等等。

6.6 规定事件记录的内容

对于每类事件，记录的内容包括但不限于以下内容：

1. 事件类型；
2. 事件相关内容；
3. 事件发生的时间日期；
4. 数字签名审核程序时成功或失败的指示符；
5. 证书撤销时成功或失败的指示符；
6. 引起事件发生的实体或操作员身份。

6.7 记录归档要求

6.7.1 记录归档的保存期限

对于不同的归档记录，其保留期限是不同的。对于系统操作事件和系统安全事件记录，其归档应保留到完成安全脆弱性评估或一致性审计。

- 对证书使用方证书生命周期内的管理事件的归档，保留一年以上。
- 对 CA 证书和密钥生命周期内的管理事件的归档，其保留期限不少于 CA 证书和密钥生命周期。
- 证书使用方证书的归档保留期限不少于证书失效后 5 年。
- CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，额外保留 5 年。

6.7.2 记录归档的保存措施

沃通对各种电子、纸质形式的归档文件，都有安全的物理和逻辑保护措施和严格的管理程序，确保归档了的文件不会被损坏，防止非授权的访问、修改、删除或其它的篡改行为。

6.7.3 记录归档的备份程序

沃通对归档文件定期进行备份，分为增量备份和全备份。增量备份每天进行，全备份每周进行。备份文件将在异地（北京机房）进行保存。

6.7.4 记录归档时间戳要求

沃通对每项日志有时间记录。对于纸质记录，有操作人员手工记录；对于电子记录，由系统自动增加时间，但这些时间未采用时间戳技术。

6.7.5 记录归档收集系统

沃通的档案收集系统由人工操作和自动操作两部分组成。

6.7.6 记录归档检验机制

只有被授权人员才可以查看和获得归档信息，这些信息被归还时必须得到检验。

6.8 认证机构密钥更替

在证书到期以前，沃通将按照证书策略的规定对根密钥进行更换，生成新的证书。在进行密钥的生成时，严格按照沃通关于密钥管理的规范。认证机构密钥更替必须循序以下原则：

1、在下级证书生命周期结束前停止颁发新的下级证书，确保在认证机构的证书到期时所有下级证书也全部到期；

2、在停止颁发新的下级证书后至证书到期时，继续使用认证机构私钥签发 CRL，直到最后一张下级证书过期；

3、生成和管理认证机构密钥对时，严格遵守密钥规范；

4、及时发布新的认证机构证书；

5、确保整个过渡过程安全、顺利，不出现信任真空期。

密钥更换时，沃通需要颁发 3 张新证书：

1、新私钥签名的包含新公钥的沃通证书；

2、新私钥签名的包含旧公钥的沃通证书；

3、旧私钥签名的包含新公钥的沃通证书。

6.9 数据备份

6.9.1 数据备份计划

沃通建立数据备份管理机制，采用本地备份、定时备份、本地冷备和异地定时备份相结合的方式备份重要数据库的数据。对关键系统数据，包括证书数据、系统配置数据、用户数据、审计日志数据和其他敏感信息进行异地备份，并确保其处于安全的设施。

数据备份采用磁盘阵列、光盘等多种方式备份数据，具备快速恢复能力，保证系统数据和服务的连续性，减少对业务运营的影响。

1、备份内容

（1）主机操作系统；

（2）系统应用软件，如 Web 服务程序、数据库系统等；

（3）认证系统软件；

（4）系统配置；

（5）数据库用户数据。

2、备份策略

（1）采用专门的备份服务器对整个运营系统的软件及数据进行备份，备份数据保存在硬盘上；

（2）备份策略采用冷备方式，备份保存于本地硬盘系统及光盘；

（3）备份策略保证没有数据丢失或数据丢失不会造成实质性的影响；

（4）在系统出现故障、灾难时，备份方案能够在最短的时间内从备份数据中恢复出原系统及数据；

（5）选择的备份介质能保证数据的长期可靠；

（6）对备份数据收集、保管、恢复进行管控，确保备份数据的安全，防止泄露和未经授权使用；

（7）定期检查备份系统和设备的可靠性和可用性，定期检查备份介质可靠性和数据完整性；

（8）定期对系统数据备份进行测试检查，确保其可用性，定期对备份数据库可用性恢复测试检查，确保系统备份数据库可用性。

6.9.2 异地备份中心

为了确保备份数据的安全，沃通除了在本地对所有系统和数据进行备份外，还在北京机房异地备份中心进行了备份，由专人进行保管和定期检查，以确保备份数据的安全和可用。

异地机房备份中心地址：北京市朝阳区酒仙桥路 6 号院 360 大厦 B 座 4 层。异地备份中心的安全等级与主机房的安全等级完全相同。

6.10 损害与灾难恢复

6.10.1 事件和损害的列表

沃通根据实际运营的情况，总结了以下有关事件及其损害列表

损害	事件	影响大小
物理损坏	火灾	小
	水灾	小
	污染	小
	重大事故	小
	设备或介质损坏	中
	灰尘、腐蚀、严寒	小
自然灾难	气候气象现象	小
	地震现象	小
	火山现象	小
	洪水	小
基础服务失效	空调系统失效	大
	电源失效	大
	通讯设备故障	大
辐射干扰	电磁辐射	小
	热辐射	小
	电子脉冲	小
信息的损害	截取损害干扰信号	小
	远程间谍	小
	偷取介质或文件	小
	偷取设备	小
	获取循环利用或废弃的介质	小
	泄密	中
	来自非信任源的数据	中
	损坏硬件	中
	损坏软件	中
	位置检测	小
技术故障	设备失效	大
	设备故障	大
	饱和的信息系统	中
	软件故障	中

未经授权的活动	设备的未经授权的使用	小
	非法的软件拷贝	小
	使用盗版软件	小
	破坏数据	小
	非法处理数据	小
功能受损	误用	小
	滥用权限	小
	盗用权限	小
	拒绝服务	小

6.10.2 计算机资源、软件或数据的损坏

沃通对业务系统及其他重要系统的资源、软件和/或数据进行了备份，并制定了相应的应急处理流程，当出现计算机资源、软件和/或数据的损坏时在最短的时间内恢复被损害的资源、软件和/或数据。

对备用设备、设施、数据，每月进行可用性检测，确保在应急恢复过程时设备、设施、数据的可用性。

6.10.3 实体私钥损害处理程序

沃通的根私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，沃通应该：

1） 立即向国家主管机关：国家密码管理局和工信部进行通报。

2） 立即通过网站和其它公共媒体对证书使用方进行通告，采取措施保证用户利益不受损失。

3） 立即撤销所有已经被颁发的证书，更新 CRL 和 OCSP 信息，供证书使用方和依赖方查询。同时沃通立即向国家密码管理局申请生成新的密钥对，并颁发新的根证书。

4） 新的根证书颁发以后，按照本 CPS 关于证书颁发的规定，重新颁发下级证书和下级操作子 CA 证书。

5） 沃通新的根证书颁发以后，将会立即通过沃通信息库的方式进行发布。

沃通的子 CA 私钥出现遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，操作 CA 应该：

1) 立即向沃通进行汇报并生成新的密钥对和证书请求，向沃通申请颁发新的证书。

2) 沃通立即通过网站和其它公共媒体对证书使用方进行通告，采取措施保证用户利益不受损失。

3) 立即撤销所有由该子 CA 颁发的证书，更新 CRL 和 OCSP 信息，供证书使用方和依赖方查询。

4) 新的子 CA 证书颁发以后，按照本 CPS 关于证书颁发的规定，重新颁发证书使用方证书。

5) 新的证书颁发以后，将会立即通过沃通信息库、目录服务器、HTTPS 等方式进行发布。

证书使用方的私钥出现遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，证书使用方应该按照本 CPS 的规定，首先申请证书撤销，并按照规定重新申请新的证书。

6.10.4 灾难后的业务存续能力

沃通在异地建立了容灾系统，一旦物理场地出现了重大灾难，沃通能够根据业务连续性计划在最短时间内恢复其业务。

6.10.5 业务连续性计划

沃通根据实际情况制定了业务连续计划，并从以下几个方面确保业务连续性计划的可用性：

1、每年对业务连续性计划进行检查和更新，确保其持续有效。

2、对 CA 系统中的重要部件制订完善的灾难恢复流程，并定期进行演练，确保流程操作的有效性。

3、建立重要系统、数据、软件的备份，并存放在安全的环境中，只有合理授权人员才可接触备份。

4、定期测试备份设备、设施、后备电源等，确保其可用性。

5、建立当 CA 签名密钥可信性受威胁时的应变计划。

6、制订相关流程，对终止电子政务电子认证服务时的告知及业务承接做出计划。

6.11 认证机构或注册机构的终止

当沃通及其注册机构因各种情况，需要停止其业务时，将会严格按照《电子政务电子认证服务管理办法》及相关法规中对认证机构中止业务的规定要求进行有关工作。

7 认证系统技术安全控制规则

7.1 密钥对的生成和安装

7.1.1 密钥对的生成

7.1.1.1 CA 密钥对的产生

对于沃通 CA 密钥对，沃通专门的密钥管理员及若干名接受过相关培训的可信雇员在沃通安全设施中的密钥生成室按照沃通的密钥管理策略中规定的密钥生成流程进行产生。沃通密钥生成流程规定了 CA 密钥产生的流程控制及参加人员。沃通 CA 的密钥对使用符合国家密码主管部门的要求的密码硬件产生。

7.1.1.2 证书使用方密钥对的产生

对于电子邮件证书、账户证书、个人证书和机构证书，证书使用方使用国家密码管理部门许可的密码模块（如 USB Key，智能卡）生成密钥对。

对于服务器证书，证书使用方使用服务器程序使用的密码模块提供的密钥生成功能生成密钥对。

对于运营设备证书，沃通或其注册机构将使用专门的程序软件在国家密码管理部门许可的密码模块（如加密卡或加密机）中生成密钥对。

对于管理员证书，私钥使用国家密码管理部门许可的客户端密码模块（如 USB Key）产生。

7.1.2 私钥传送给证书使用方

沃通各类 CA 证书密钥对由沃通在其安全运营场地产生，私钥由沃通自身持有和保存，不存在私钥的传送问题。

沃通各种运营设备证书的密钥对由沃通或其注册机构在设备所在地产生，并在本地保存，不存在私钥的传送问题。

对于沃通颁发的其他最终用户证书，通常的情况下密钥对在证书使用方本地的密码模块（如 USB Key）中产生，私钥由最终用户保存在本地密码模块中，不存在私钥的传送问题。但在一些特别的安排下，沃通或其注册机构可能会代最终用户在约定的密码硬件中（如 USB Key）产生证书密钥对，且私钥保存在密码硬

件中。在这种情形下，沃通或其注册机构将通过安全的途径将保存有证书私钥的密码硬件传送到最终用户手中，并确保在传送过程中私钥不会被非授权的使用、被泄露或被损坏。

7.1.3 公钥传送给证书颁发机构

需要沃通认证的证书公钥，证书使用方通过 PKCS#10 格式的证书签名请求信息文件包格式，以电子的方式将公钥提交给沃通认证中心（或通过其注册机构提交），这些请求通过网络传送时使用安全套接层协议（SSL）和其他安全协议。

7.1.4 认证机构公钥传送给依赖方

对于沃通的主 CA 公钥，通过如下方式传输给依赖方：

1）依赖方访问沃通的证书服务站点下载 CA 证书，该站点受到服务器证书的保护；

2）依赖方访问沃通的目录系统；

3）沃通、注册机构或其合作伙伴到依赖方业务系统现场将 CA 证书安装到业务系统；

4）沃通、注册机构或其合作伙伴通过签名电子邮件将 CA 证书传输给依赖方；

5）沃通、注册机构或其合作伙伴分发给依赖方的软件中绑定、包含有 CA 证书。

对于沃通的其他 CA 公钥，除了上面所述的方式传输给依赖方外，当证书使用方获取证书时沃通通过 PKCS#7 格式将除根证书外的证书链传递给证书使用方。

7.1.5 密钥的算法

为了保证加密/解密的安全性，沃通所使用的 SM2 算法密钥对长度为 256 位。如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，沃通将会完全遵从。

7.1.6 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。

7.1.7 密钥使用目的

在沃通证书服务体系中的密钥用途和证书类型紧密相关，被分为签名和加密两大类。

沃通的 CA 签名密钥用于签发用户证书和证书撤销列表（CRL）；

证书持有者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。

7.2 私钥保护和密码模块工程控制

7.2.1 在 CA 私钥保护方面的要求

沃通使用国家密码管理部门认可、批准的硬件密码模块生成主 CA、证书颁发 CA 和其他 CA 密钥对，并存储 CA 私钥。

沃通制定有专门密码管理策略，在从运送、验收、初始化、离线存放、在线使用到销毁的整个密码设备生命周期内，对密码模块进行管理和控制。CA 密码模块离线存放在 CA 密钥离线存放区中，CA 密码模块在线放置在屏蔽机房或机柜中。

沃通运营设备证书使用的密码模块的标准及控制同 CA 密钥密码模块。 最终用户证书使用国家密码管理部门认可的密码模块，并妥善保护、保管其密码模块，防止其失窃、丢失、损坏及被非授权的使用。

7.2.1.1 私钥多人控制（m/n）

沃通的各类 CA 私钥存放在硬件加密卡中，该加密卡启动的秘密（如激活数据）被分割保存在 3 张 IC 卡中（称为秘密分割份额，或简称秘密分割），这 3 张 IC 卡由沃通 3 名可信雇员持有（称为秘密分管者），保存沃通内部保险柜中。当要激活 CA 私钥时，需要 2 名秘密分管者提供他们的秘密分割 IC 卡才能完成。

并且所有操作 CA 根私钥的行为都必须在 CA 屏蔽机房内完成。

7.2.1.2 私钥托管

沃通所有 CA（包括主 CA 和运营 CA）的私钥均未在其他地方托管。

沃通根据国家密码管理部门的要求对证书使用方加密证书的私钥进行托管。

7.2.1.3 私钥备份

沃通对 CA 私钥通过专门的备份加密卡进行备份，这些备份分别作为本地常规备份和异地灾难恢复备份。对备份加密卡的保护符合 CPS 6.2.4 的要求。

对于认证机构运营设备证书，沃通或其注册机构通常不进行私钥备份，因为这种备份是不需要的；但对某些特别的运营设备证书，如时间戳服务证书，沃通会对其私钥进行备份。

对于最终用户证书，如果存放证书私钥的密码模块允许私钥备份，沃通建议证书使用方对私钥进行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改或泄露。

7.2.1.4 私钥归档

当沃通的 CA 密钥对超过使用期后，这些 CA 密钥对将归档保存至少 5 年。归档 CA 密钥对保存在 CPS 6.2.1 所述的硬件密码模块中，并且沃通的密钥管理策略和流程阻止归档 CA 密钥对返回到产品系统中。对归档私钥到了归档保存期，沃通将按 CPS 6.2.10 销毁。

对于认证机构运营设备证书，沃通或其注册机构通常不进行私钥归档，因为这种归档是不需要的；但对某些特别的运营设备证书，如时间戳服务证书，沃通会对其私钥进行归档，其归档过程和要求同 CA 密钥对。

沃通或其注册机构不对最终用户证书的私钥进行归档，但如果证书使用方存放证书私钥的密码模块允许私钥备份，沃通建议证书使用方对私钥进行归档，并对归档的私钥采用口令或其他访问控制机制保护，防止非授权的泄露。

7.1.2.5 私钥导入、导出密码模块

沃通的 CA 密钥对在硬件密码模块上生成，保存和使用。此外，为了常规恢复和灾难恢复，沃通对 CA 密钥进行复制。当 CA 密钥对从一个硬件密码模块复制到另一个硬件密码模块上时，被复制的密钥对以加密

的形式在模块之间传送，并且在传递前要进行模块间的相互身份鉴别。另外沃通还有严格的密钥管理流程对 CA 密钥对复制进行控制。所有这些有效防止了 CA 私钥的丢失、失窃、修改、非授权的泄露、非授权的使用等。

沃通运营设备证书私钥的导入、导出控制同 CA 私钥。

沃通注册机构的运营设备证书私钥通常是不允许导入、导出的，若在特定的情况下确实需要导出、导入，则必须由沃通的可信人员进行相关的操作。沃通在进行导出、导入时，将确保导出的证书私钥不以明文形式存在（如由具有足够强度的口令保护），并在完成导出、导入后立即、彻底地销毁导出的私钥。

对于各类最终用户证书，若使用的密码模块（软件或硬件）支持私钥的导出、导入，则沃通要求最终对导出、导入的私钥必须使用足够安全的口令进行保护，且最终用户需要确保导出的私钥不被丢失、失窃、修改、非授权的泄露、非授权的使用等。

7.2.1.6 私钥在密码模块的存储

沃通 CA 私钥以加密的形式存放在符合国家密码主管部门的要求硬件密码模块中，且私钥的使用也在硬件密码模块中进行。

沃通运营设备证书私钥的存储同 CA 私钥。

对于个人证书和机构证书，最终用户须将私钥保存在其可控制、国家密码主管部门的认可的密码模块中（如 USB Key），私钥在密码模块中须以加密形式存储，且私钥的使用受口令或指纹等安全措施保护。最终用户须采取必要的措施防止其他人员对私钥的非授权访问、获取和使用。

对于服务器证书，最终用户需将私钥保存在国家密码主管部门认可的密码模块中（包括 SSL 加速卡），且存放私钥的密码模块必须在最终用户其可控制的范围内，并最终用户要采取相应的安全手段防止对私钥的非授权访问、获取和使用，使用的手段包括私钥的使用受口令保护，服务器及密码模块位于安全可控的物理环境等。

7.2.1.7 激活私钥的方法

1、最终用户证书私钥

保存在密码模块中的最终用户证书私钥需在用户输入口令（或 PIN 码）或指纹等密钥保护信息（激活数据）后才被激活，才能能够被使用。

2、运营设备证书私钥

对于沃通的运营设备证书私钥的激活同 CA 私钥的激活；对于沃通注册机构的运营设备证书私钥，需要专门的安全管理人员输入保护口令后才能激活。

3、CA 私钥

沃通的 CA 私钥存放在硬件密码模块中，并且其激活数据按 CPS 6.2.2 进行分割。当需要使用 CA 私钥时（在线或离线），需要沃通 CA 私钥 5 个秘密分管者中的至少 2 人和密钥管理员同时到场，由 2 个秘密分管者输入秘密分割（激活数据 2）后才能激活。

7.2.1.8 解除私钥激活状态的方法

对于个人证书和机构证书，当应用软件向密码模块发出设备关闭指令，或密码模块被下载（如硬件密码模块从读卡器中取出）、或用户通过密码管理软件从密码设备登出（logout）、或计算机断电时，私钥被解除激活状态，不能再被使用。

对于服务器证书，当服务程序关闭、系统注销或系统断电后私钥即进入非激活状态。

对于沃通及其注册机构的运营设备证书的私钥，当 CA 或 RA 系统向密码模块发出登出（logout）或密码管理软件向密码模块发出关闭（close）指令，或存放私钥的密码模块断电,，私钥进入非激活状态。

对于沃通 CA 私钥，当 CA 系统向密码模块发出登出（logout）或密码管理软件向密码模块发出关闭（close）指令，或存放私钥的硬件密码模块断电,，私钥进入非激活状态。

7.2.1.9 销毁私钥的方法

对于沃通的最终用户证书私钥，若不再使用，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。若私钥撤销、到期作废后，还需要用于信息解密的，最终用户应该妥善保存一定期限，以便于解开加密信息。若私钥无需再保存，则将通过私钥的删除、系统或密码模块的初始化来销毁。

在沃通 CA 私钥生命周期结束后，沃通将 CA 私钥继续保存在一个备份硬件密码模块中，并进行归档，其他的 CA 私钥备份被安全销毁。归档的 CA 私钥在其归档期限结束后，需在多名可信人员参与的情况下安全销毁。CA 私钥的销毁将确保 CA 私钥从硬件密码模块中彻底删除，不留有任何残余信息。

沃通不再使用的运营设备证书私钥，按 CA 私钥销毁相同的方法进行销毁，对无需归档而不再使用的运营设备私钥将立即销毁。

沃通注册机构不再使用的运营设备证书私钥，将通过私钥的删除、系统或密码模块的初始化来销毁。

7.2.1.10 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。

7.2.1.11 离职、换岗人员私钥处置

对于离职人员的私钥处置：

沃通人员离职时，需安全策略管理委员会移交 USB Key 等系统相关的凭证，并进行相关的工作交接。沃通在移交后 1 小时内修改更换 PIN 等，确保信息不会泄露；

对于换岗人员的私钥处置：

沃通人员换岗时，需安全策略管理委员会移交 USB Key 等系统相关的凭证，并进行相关的工作交接。沃通在移交后 1 小时内修改更换 PIN 等，确保信息不会泄露；

7.2.2 用户私钥保护方面的要求

沃通确保，在电子政务的证书应用，数字证书对应私钥的生成、存储和使用能够得到有效的安全保护；

签名密钥对为证书持有者专有，生成、存储和使用受证书持有者安全管控；沃通不保存证书持有者的签名密钥。

加密密钥对由国家密码管理局和省部密码管理部门规划建设的密钥管理基础设施提供密钥管理服务。

7.3 密钥对管理的其他方面

7.3.1 公钥归档

对于生命周期外的 CA 和最终用户证书，沃通将进行归档，归档的证书存放在归档数据库中。

7.3.2 证书操作期和密钥对使用期限

公钥和私钥的使用期限与证书的有效期相关但却有所不同。

对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期

限以外，直到私钥受到损害或密钥对存在被破解的风险，如加密算法被破解。当私钥受到损害或密钥对存在被破解的风险后，签名证书的公钥在技术上仍然可以用于验证数字签名，但这种验证在法律上不一定是有效的。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。 当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。 另外无论是证书使用方证书还是 CA 证书，有效期到了后，在保证安全的情况下，允许证书进行更新而密钥对不变。但是密钥对不能无限期使用。

7.4 激活数据

7.4.1 激活数据的产生和安装

沃通 CA 私钥的激活数据由硬件加密卡内部产生，并分割保存在 5 个 IC 卡中，需通过专门的读卡设备和软件读取。沃通 CA 私钥激活数据的产生过程，按沃通密钥生成规程参考指南中的规定进行。所有秘密分割的创建和分发有相应的记录，包括产生时间、持有人等信息。

沃通运营设备证书私钥的激活数据的产生和安装，同 CA 私钥。

沃通注册机构运营设备证书私钥的激活数据，由注册机构的安全管理员根据所用密码系统提供的功能相应产生。若激活数据是口令，则对口令的安全要求不低于证书使用方证书私钥保护口令的要求。

如果证书使用方证书私钥的激活数据是口令，这些口令必须：

- 至少 8 位字符或数字；
- 至少包含一个字符和一个数字；
- 不能包含很多相同的字符；
- 不能和操作员的名字相同；
- 不能包含用户名信息中的较长的子字符串。

沃通还建议证书使用方使用双因素机制（如硬件+密码，生物识别设备+密码等）来控制私钥的激活。

7.4.2 激活数据的保护

保存有沃通 CA 私钥及运营设备证书私钥的激活数据秘密分割的 3 个 IC 卡，由沃通 3 个不同的可信人员持有，而且持有人员必须符合职责分割的要求，签署协议确认他们知悉秘密分管者责任。秘密分割由秘密持有人分别存放在沃通认证中高安全保护的保险柜中各自的保险盒中。

沃通注册机构的运营设备证书私钥的激活数据，由注册机构的管理员负责安全保护。

如果证书使用方使用口令或 PIN 码保护私钥，证书使用方应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书使用方使用生物特征保护私钥，证书使用方也应注意防止其生物特征被人非法获取。

7.4.3 激活数据的其他方面

7.4.3.1 激活数据的传送

存有沃通 CA 私钥、运营设备证书私钥的激活数据的 IC 卡，通常保存在沃通的安全设施中，不能携带外出或传送。如因某种特殊情况确实需要传送时，其传送过程需在沃通安全管理人员和密钥管理人员的监督下进行。

沃通注册机构的运营设备证书私钥的激活数据由注册机构的安全管理员产生、保管，不得向外传送。

通常情况下证书使用方证书私钥的激活数据由证书使用方自己产生、保管，不应传送给其他人员，若私钥激活数据因特别的原因需要进行传送时，证书使用方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。

在某些特别的安排下，沃通认证中心或其注册机构，有可能代证书使用方在特定的密码硬件（如 USB Key）中产生私钥并产生相应的激活数据，在这种情况下，沃通或其注册机构，或者通过面对面的方式，或者通过电话、电子邮件等方式，将激活数据传送给证书使用方。在非面对面的传送方式下，私钥激活数据的传送路径、方式同存有私钥的密码硬件的传送路径、方式将是不同的，分开的。在这种安排下，证书使用方在接收到存有私钥的密码硬件和获得激活数据后，必须尽快改变私钥的激活数据。

7.4.3.2 激活数据的销毁

存有沃通 CA 私钥、运营设备证书私钥的激活数据分割的 IC 卡，其销毁所采取的方法包括将 IC 卡初始化，或者彻底销毁 IC 卡，无论采取何种方式，都将保证不会残留有任何秘密信息。CA 私钥激活数据的销毁

是在沃通安全管理人员和密钥管理人员的监督下进行。

沃通注册机构的运营设备证书私钥的激活数据不再使用时，注册机构掌管激活数据的安全管理员需要销毁有关数据，确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

当证书使用方证书私钥的激活数据不需要时应该销毁，证书使用方应该确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

7.5 系统安全控制

7.5.1 安全技术要求

沃通的证书认证系统主机实现了自主访问控制（DAC），进行了安全漏洞扫描和安全优化，安装了防病毒系统，确保了包含 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。此外，根据沃通的安全策略，只允许有工作需求的必要人员访问生产系统的服务器，一般的应用用户在生产系统服务器上没有账户。

沃通的电子认证生产系统网络与其它部分逻辑分离，并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，且只有沃通系统运营管理组中的、必要的可信人员可以直接访问认证系统数据库。

7.5.2 安全技术措施

沃通的 CA 系统及其运营环境通过了国家权威机构的安全测评、评审，并获得了相应资质。

7.6 生命周期技术控制

7.6.1 CA 系统运行管理

1、CA 系统的操作流程采用文档化并进行维护。

2、CA 系统（包括软件、网络等方面）的变更经管理层批准，经批准的变更实行前通过测试，并进行记录。

3、可能对系统的安全性有影响的改动必须事先进行风险评估，改动前进行备份并得到管理层的明确批

准。

4、CA 中心的测试系统、运营系统、网络设施等，都由专门的操作维护人员，并有相应明确的授权。

5、操作维护人员定期检查系统及网络的稳定性、安全性及容量，确定符合服务水平。

6、建立了检测和防护控制来防止病毒和恶意软件，并提供适当的报警信息。

7、建立了监控流程，确保记录并报告发现的或怀疑的、对系统或服务有威胁的安全缺陷。建立并执行系统故障报告、处理流程。

8、建立了相应制度，对 CA 系统相关的媒介（包括设备、证书介质、文档等）进行妥善保管，避免非授权的访问。

7.6.2 CA 系统访问管理

设置关键岗位和职责分工，对于 CA 系统的访问权限进行严格限制，未授权人员不得访问 CA 系统。

1、制定了 CA 系统的访问策略，内容包括：访问角色及相关权限，认证及鉴别的方法，分权机制，特殊 CA 操作的人数（密钥生成时 3 of 5 规则）等。

2、制定了 CA 系统访问人员角色职能定义，确保合理的职责分割和权限控制，并明确授权及取消授权的操作流程和策略。

3、制定了网络安全策略，并制定了访问网络的控制策略。

4、制定了操作系统及 CA 软件的安全访问的策略。

5、建立了对各种对 CA 系统访问的审计措施。

7.6.3 CA 系统的开发和维护

原则上不对 CA 系统进行技术开发和直接调用其数据，仅将 LDAP 和 RA 系统对外提供查询和访问服务。

1、建立了 CA 系统软件修订控制流程，对系统新增或修改进行管理。

2、严格控制对 CA 系统的源代码及测试数据的访问。

3、操作系统升级变更时，对应用系统软件重新测试。

4、在 CA 系统中，购买、使用或修改的软件，需要进行严格检查，避免“特洛伊木马”等攻击。

7.7 网络的安全控制

沃通证书认证系统网络进行安全漏洞扫描和安全优化，部署了防火墙、入侵检测系统，并在系统通信

过程中使用加密和数字签名进行保护。

7.8 时间戳

沃通 CA 系统的各种系统日志、操作日志都有对应的记录时间。这些时间标识未采用基于密码的数字时间戳技术。

8. 法律责任和其他业务条款

8.1 费用

8.1.1 免费或收费策略

沃通可根据提供的电子政务电子认证相关服务向本机构的证书持有者收取费用，具体收费标准根据国家有关物价管理部门的批复文件执行。在收费标准范围内，即不超过收费标准的情况下，沃通有权根据市场状况，针对不同用户群体推出不同的收费策略或优惠措施。

8.1.2 证书签发和密钥更新费用

沃通在官网公布了证书签发等费用，具体地址为：https://www.wotrus.com/ca/dca_cert_price.html。

8.1.3 其他服务费用

沃通将根据具体的项目情况，适当的收取服务费用，具体的费用将以实际项目合同为准。

8.2 财务责任

8.2.1 责任担保范围

沃通向证书使用方提供证书使用保障。如果由于沃通原因造成用户使用证书过程中遭受损失，沃通公司将向证书使用方、依赖方提供赔偿（具体情形参见 9.9）。

8.2.2 责任赔付声明

沃通具备国家信息产业主管部门所规定的资金实力，具备承担赔偿责任的条件。

8.3 业务信息保密

沃通有专门的信息保密制度，保护自身和客户的敏感信息、商业秘密。

8.3.1 保密信息范围

沃通保密的信息包括但不限于：

- 系统方面

1) 认证系统结构、配置，包括系统、网络、数据库等；
2) 认证系统安全策略和方案；
3) 系统操作、维护记录；
4) 各类系统操作口令。

- 运营管理方面

1) 物理安全策略与实施方案，包括场地、访问控制、入侵检测等实施方案；
2) 密钥管理策略与操作记录；
3) CA 或 RA 批准或拒绝的申请纪录；
4) 可信人员名单；
5) 内部安全管理策略与制度。

- 客户信息

1) 客户的注册信息；
2) 客户系统、应用访问 CRL、OCSP 的记录（时间、频度）；
3) 客户与认证机构、注册机构签订的协议；

8.3.2 不属于保密的信息

证书、证书状态信息及信息库中的信息，都是不需保密的信息。

8.3.3 保护保密信息的责任

沃通有各种严格的管理制度、流程和技术手段保护自身的商业秘密，每个员工都必须接受信息保密方面的培训，并与公司签订保密协议。任何参与方有责任保证不泄露保密信息。

8.4 个人隐私保密

8.4.1 保护隐私的责任

除非执法、司法方面的强制需要，沃通及其注册机构在没有获得客户授权的情况下，不会将客户隐私信息透露给第三方。

8.4.2 使用隐私信息的告知与同意

沃通或其注册机构如果需要将客户隐私信息用于双方约定的用途以外的目的，则需要事先告知客户并获得客户同意和授权，用户同意和授权信息以下列方式之一传送给沃通或其注册机构：

1）有手写签名的同意和授权文件，并将文件邮寄、快递到沃通或其注册机构；

2）将手写签名的同意和授权文件传真到沃通；

3）以签名电子邮件的形式同意并授权。

8.4.3 依法律或行政程序的隐私信息的使用

当沃通在法律、法规或规章条款有要求时，或在司法机关的要求下必须披露本电子政务电子认证服务业务规则中具有保密性质的信息时，沃通可以按照法律、法规或规章条款以及司法机关的要求，向执法部门公布相关的保密信息。这种披露不视为违反了保密的要求和义务。

8.4.4 不被视为隐私的信息

不被认为是隐私信息包括，要出现在证书中的信息、证书及证书状态信息。

8.5 知识产权

沃通拥有对本电子政务 CPS 的所有知识产权。沃通保留其签发的证书和证书撤销信息的所有知识产权。任何人可以免费地复制、分发证书和证书撤销列表，只要他们进行完整复制并且证书和证书撤销列表的使用符合相应的依赖方协议。证书申请者拥有证书申请中包含的申请者拥有的商标、服务标志或商业名称以及签发给该证书申请者的证书中的可辨识名的所有权利。证书所有者拥有其证书相关的密钥对的知识产权。

8.6 陈述与担保

8.6.1 认证机构的陈述与担保

证书使用方同意沃通证书使用方协议是证书使用方注册申请沃通证书的一个条件，在证书使用方成功完全证书申请注册前，证书使用方必须以下列两种方式之一接受证书使用方协议：

1）对证书使用方协议文件签名并提交给沃通或其注册机构；

2）阅读注册页面上证书使用方协议，并点击同意证书使用方协议。

依赖方决定信赖沃通颁发的证书前需阅读沃通依赖方协议，用户接受证书及状态信息即表明其接受了依赖方协议。

沃通不负责评估证书是否被恰当使用。证书使用方和依赖方必须依证书使用方协议和依赖方协议确保证书用于允许使的目的。

沃通、注册机构和证书使用方之间的担保、免责和有限责任由他们之间的协议规定约束。

沃通对证书使用方做出如下担保：

- 证书中不存在批准证书申请或颁发证书时沃通已知的对事实的实质性错误描述；
- 批准证书申请或颁发证书时，不会因为工作疏忽将错误信息包含到了证书中；
- 证书满足沃通证书策略所有实质性的要求；
- 撤销服务和信息库的使用在所有方面符合沃通证书策略的要求。

沃通对证书依赖方做出如下担保：

- 除了未经鉴别、验证的证书使用方信息外，包含在证书中的所有信息都是准确的。
- 在沃通信息库中发布的证书已经颁发给了个人或组织机构（它们的名字包含在证书中），证书使用方已经根据 CPS 4.4 接收了该证书。
- 批准证书申请或颁发证书的实体颁发证书时完全遵守了 CPS 的规定。
- 沃通所采纳的与证书服务有关的技术，基于目前的技术发展与评估是安全的、可靠的。
- 沃通已通过技术的、物理的防护及流程控制，确保服务系统、设备和设施的安全、可靠。

8.6.2 注册机构的陈述与担保

沃通认证机构的注册机构做出如下担保：

RA 在批准证书前，完成了所有必要的鉴别工作，并且确认了信息是正确的、准确的。

8.6.3 用户的陈述与担保

作为获得证书的一个条件，证书申请者在证书申请时已阅读了证书使用方协议并且同意证书使用方协议，并且：

- 在证书申请时，证书使用方的所有陈述都是对的；
- 证书使用方提供的，特别是包含在证书中的需要鉴别、验证的信息是真实的、准确的。

在证书的保存和使用过程中，证书使用方同意做到：

- 按照沃通 CP、CPS 将证书用于规定的使用目的，不将证书用于证书使用目的以外的场合；
- 利用与证书中的公钥相对应的私钥产生的数字签名是证书使用方的数字签名，证书使用方知晓要签名的内容，产生数字签名时，证书使用方已经接受了证书，且该证书没有过期或撤销。
- 证书使用方对自己的私钥进行了有效的保护，其他人员无法使用证书使用方的私钥。

8.6.4 依赖方的陈述与担保

依赖方确认，在任何信赖行为发生之前，阅读了依赖方协议，并评估了在特定应用中信赖证书的适当性，不在证书适用目的以外的应用中信任证书。

8.6.5 其他参与者的陈述与担保

为沃通提供客户身份验证服务的第三方已向沃通做出如下承诺：

- 是合法的、获得授权的组织机构信息服务提供商；
- 提供的信息权威性的；
- 在其能够管理与控制范围内，其提供的数据是真实的、准确的；
- 其保存的组织机构信息在最短的时间内获得了更新。

8.7 担保免责

沃通不对其颁发的证书适用于其规定的目的以外的任何应用承担任何担保，对证书在其规定的目的以外的应用不承担任何责任。对由不可抗力，如战争、地震、洪灾、爆炸、恐怖活动等，造成的服务中断并由此造成的客户损失，沃通及注册机构不承担责任。

8.8 偿付责任限制

对于由于沃通自身原因，如没有严格按业务流程进行证书审批导致证书的错误颁发、假冒，或管理上的疏忽导致 CA 私钥泄漏、盗用等，造成了证书使用方、依赖方的损失，沃通将承担相应的赔偿责任，但这种责任是有限的。

沃通对于证书提供的保障级别分为：恢复证书使用、撤销（错误）证书、经济赔偿。

对于电子邮件证书、账户证书、以及设备不涉及经济赔偿，只涉及恢复证书使用、撤销（错误）证书等方式的保障。对于个人证书和机构证书，在包括上述保障方式外，增加经济补偿的保障方式，见表 10。

表 10 – 责任赔偿

证书级别	责任赔偿
个人证书	最高人民币 800 元
机构证书	最高人民币 2000 元
设备证书	最高人民币 4000 元

沃通只对由于自身原因造成的用户直接损失承担责任，对间接的损失不承担责任。

8.9 赔偿责任

有下列情形之一的，沃通承担有限的赔偿责任：

- 沃通将证书错误的颁发给证书使用方以外的第三方，导致证书使用方或者依赖方遭受损失的；
- 证书使用方提交的注册信息或者资料真实、完整、准确，但沃通颁发了有错误信息的证书，导致证书使用方或者依赖方遭受损失的；
- 证书使用方提供了虚假的注册信息或者资料，而沃通将有关信息作为已鉴别与验证信息包含在颁发的证书中，从而导致依赖方遭受损失的；
- 由于沃通的原因导致证书私钥被破译、窃取，致使证书使用方或者依赖方遭受损失的；

证书使用方有下列情形之一，给沃通、依赖方造成损失的，应当承担赔偿责任：

- 提供的资料或者信息不真实、不完整或者不准确的；
- 证书中的信息有变更，未终止使用该证书并通知各方的；
- 证书使用方没有使用可信系统保护私钥，或者没有采取必要的注意防止证书使用方私钥的安全损害、丢失、泄漏、修改或非授权的使用；
- 知悉证书私钥已经丢失或者可能已经丢失时，未终止使用该证书并通知各方的；
- 证书使用方使用的名字（包括但不限于通用名、域名和 e-mail 地址）破坏了第三方的知识产权的；
- 超过证书的有效期限使用证书的；
- 使用证书用于违法、犯罪活动的。

在如下情况，依赖方对自身原因造成的沃通损失承担责任：

- 依赖方没有执行依赖方职责义务；
- 依赖方在不合理的环境下信赖一个证书；
- 而依赖方没有检查证书状态确定证书是否过期或撤销。

有下列情形之一的，沃通不承担赔付责任：

- 因证书使用方原因致使依赖方遭受损失的；
- 依赖方未经检验证书的状态即决定信赖证书的；
- 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；

- 因不可抗力原因导致证书使用方或者依赖方遭受损失的。

8.10 有效期限与终止

8.10.1 有效期限

除非沃通特别声明 CPS 提前终止，在沃通颁布新版本 CPS 之前，本 CPS 一直有效。

8.10.2 终止

当沃通终止业务时，沃通 CPS 终止。在终止服务六十日前向电子认证服务主管部门报告，并作出妥善安排。

8.10.3 效力的终止与保留

沃通 CPS 的终止（而非更新），意味着沃通认证业务的终止。沃通终止认证业务的过程将按国家有关主管部门的规定进行，并根据规定对受影响的客户进行安排，保证客户的利益不受影响或将受影响的程度减少到最小。

当由于某种原因，如内容修改、与适用法律相冲突， CPS、证书使用方协议、依赖方协议和其他协议中的某些条款失效后，不影响文件中其他条款的法律效力。

8.11 对参与者个别通告与沟通

沃通及其注册机构在必要的情况下，如在主动撤销证书使用方证书、发现证书使用方将证书用于规定外用途及证书使用方其他违反证书使用方协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知证书使用方、依赖方。

8.12 修订

8.12.1 修订程序

本认证业务规则将尽量避免不必要的修改。但不定期地，沃通将对本 CPS 进行检查、评估，当沃通认为应该对本 CPS 做出修改时，CPS 起草小组将对本 CPS 及其他相关文档、协议提出修改建议，获得沃通管理层批准后，由沃通安全策略管理委员会指定专人负责组织有关文档、文件的修改。修改后的 CPS 及其他相关文档、协议经沃通安全策略管理委员会批准后正式发布，并报国家密码管理局备案。

8.12.2 通知机制与期限

沃通将修改了的 CPS 通过沃通信息库更新通告栏发布，其地址为：https://www.wotrus.com/ca/。在认为有必要时，沃通将通过电子邮件、信件、媒体等方式通知有关各方。

修改后的 CPS 经批准后将立即在沃通信息库更新通告栏发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，沃通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面受到的影响最小。

8.12.3 必须修改业务规则的情形

由沃通安全策略管理委员会根据公司业务情况决定。

8.13 争议处理

当沃通、证书使用方和依赖方之间出现争议时，有关方面可依据协议通过协商解决，协商解决不了的，可通过法律解决。沃通证书使用方协议、依赖方协议和其他证书使用方协议已包括该项内容。

8.14 管辖法律

本规则在各方面服从《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》等中华人民共和国法律、规则、规章、法令和政令的约束和解释。沃通的任何业务活动受有关法律、法规的制约，任何业务和法律文件、合同的解释、执行不能同有关法律、法规相冲突。

8.15 与适用法律的符合性

沃通的所有业务、活动、合同、协议符合中华人民共和国法律、法规，包括但不限于，公司法、合同法、消费者权益保护法等，主要有：

1、《中华人民共和国电子签名法》

2、《中华人民共和国网络安全法》

3、《商用密码管理条例》

4、《电子认证服务密码管理办法》

5、《电子政务电子认证服务管理办法》

8.16 一般条款

8.16.1 完整协议条款

CPS、证书使用方协议及依赖方协议及其补充协议将构成沃通信任域参与者之间的完整协议。

8.16.2 转让条款

沃通、注册机构、证书使用方及依赖方之间的责任、义务不能通过任何形式转让给其他方。

8.16.3 分割性条款

法律允许的范围内，在沃通证书使用方协议、依赖方协议和其他证书使用方协议内出现可以同其他条款分割的条款时，协议中的可分割条款的无效不应该影响协议中其他条款效力。

8.16.4 强制执行条款

在沃通、注册机构、证书使用方和依赖方之间出现纠纷、诉讼时，胜讼可以要求对方支付有关诉讼费作为对其补偿的一部分。免除一方对某次合同违约的赔偿不意味着免除对其他合同违约的赔偿。

8.16.5 不可抗力条款

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、法律或行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。

在电子政务电子认证活动中，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（如证书持有者）不得提出异议或者申请任何补偿。

8.17 其他条款

沃通对本《电子政务电子认证业务规则》具有最终解释权。