深圳市沃通电子认证服务有限公司
中国深圳市南山区南海大道 1057 号科技大厦二期 A 栋 502
邮编：518067
总机：+86-755-8600 8688 传真：+86-755-33975112

WoSign
电子认证业务规则

版本：1.0
状态：最终审核通过
更新：2013 年 5 月 1 日

深圳市沃通电子认证服务有限公司
中国深圳市南山区南海大道 1057 号科技大厦二期 A 栋 502
邮编：518067
总机：+86-755-8600 8688 传真：+86-755-33975112

版本说明：

沃通认证业务规则版本控制表

名称及版本	主要修改说明	完成时间	修改人
沃通认证业务规则 1.0		2013 年 5 月	王高华/姬云鹏 符海燕/李国华
沃通认证业务规则 1.2			

一. 概括性描述

深圳市沃通电子认证服务有限公司（下称“WoSign”，或简称“沃通”），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。作为全球专注于电子认证服务的运营商，沃通依靠先进而实用的技术和优质的服务，为广大的、对通信和信息安全方面有各种各样需求的公众用户提供数字证书认证服务。

沃通运营和维护国内的数字证书公共认证体系，该体系的主 CA（WoSign Domestic CA, WOSIGN_DCA）由国家密码管理局根 CA 签发，由沃通拥有、并负责运营和维护。

本文档《电子认证业务规则》（Certification Practice Statement, CPS），根据 WOSIGN_DCA 体系证书策略（Certificate Policy, CP）的相关要求制定，阐明了沃通如何开展 WOSIGN_DCA 体系认证业务，包括批准、签发、管理、吊销和更新证书的业务方式和过程，以及相应的服务、法律和技术上的措施和保障，以供电子认证活动参与方了解和遵循。本 CPS 的总体条款结构符合信息产业主管部门所发布的《电子认证业务规则规范（试行）》，并在制定过程中参照《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务机构年度检查指引（试行）》及国家密码主管部门相关标准制定。在不改变《电子认证业务规则规范（试行）》总体框架的情况下，在制定本 CPS 时可能会对该框架进行扩充，以适应沃通认证业务的特定需求。

本 CPS（1.0 版本）的生效日期是 2013 年 5 月 1 日。

1.1 概述

本 CPS 适用于沃通运营管理的 WOSIGN_DCA 体系 CA，包括沃通主 CA、主 CA 之下的证书签发 CA、以及为机构客户创建并运营的客户子 CA。客户子 CA 托管在沃通、由沃通负责运营。机构客户在其客户子 CA 下签发证书时，必须遵从本 CPS 开展认证业务；机构客户也可以按照 WOSIGN_DCA CP 的相关要求制定自己的 CPS，并报沃通公司批准。机构客户自己制定的 CPS 不能与本 CPS 相冲突。为保证 WOSIGN_DCA 信任体系的一致性，沃通安全策略指导委员会将

对拥有客户子 CA 的机构客户的认证业务运营每年进行一次审计。

本 CPS 不适用于在沃通托管的私有体系证书。

沃通提供的 WOSIGN_DCA 体系证书，根据证书认证与绑定的主体及证书用途的不同，分为：

- 电子邮件证书(email certificate)
- 帐户证书(account certificate)
- 个人证书(individual certificate)
- 机构证书(organization certificate)
- 设备证书(device certificate)

1.1.1 电子邮件证书(email certificate)

电子邮件证书与电子邮件地址绑定，颁发给电子邮件地址的拥有者，用于电子邮件地址的鉴别。

1.1.2 帐户证书(account certificate)

帐户证书与订户在某个应用服务系统中的帐户绑定，用于该系统的用户登录。

1.1.3 个人证书(individual certificate)

个人证书包括个人用户证书(individual user certificate)，机构雇员证书(organization employee certificate)和各类管理员证书(administrator certificate)。个人用户证书颁发给个人用户，用于标识个人身份，它一般包括个人姓名、个人身份证件号码等身份识别信息，但通常不包括所属机构的信息。机构雇员证书颁发给机构内部人员（雇员），通常用于机构内部应用，它除了包括个人信息外，还包括个人所属机构名称、部门名称等信息。管理员证书颁发给沃通数字认证中心及其注册机构（Registration Authority，简称 RA）的管理员，用于证书服务和证书系统的管理，它一般包含个人姓名、所属机构名称、部门名称等信息。

1.1.4 机构证书(organization certificate)

机构证书包括机构单位证书（organization unit certificate）和机构代表人证书（organization representative certificate)。机构单位证书颁发给组织机构，用于标识机构身份，它一般包括机构法定名称和组织机构代码、税号等信息。机构代表人证书颁发给组织机构代表人，用于标识代表机构的人员的信息，它一般包括代表人姓名、身份证件号码等信息。

1.1.5 设备证书(device certificate)

设备证书包括服务器证书和运营设备证书。服务器证书颁发给服务器，用于标识服务器身份，它一般包括服务器主机名、域名、或 IP 地址，以及服务器所属机构名称等信息。运营设备证书颁发给沃通数字认证中心或其注册机构的运营设备，它一般包括运营设备名称、所属机构名称等信息。

当本 CPS 中的描述没特定指明证书类型，而一般性的提到的订户证书或最终用户证书时，有关证书是指沃通数字认证中心 CA 证书、运营设备证书以外的其他所有证书（包括管理员证书)。

1.2 文档名称与标识

本文档称为《沃通电子认证业务规则》（简称沃通 CPS)，该文档没有分配对象标识符。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构（CA）

电子认证服务机构（Certification Authority，简称 CA）指所有得到授权能够颁发公钥证书的实体。沃通作为电子认证服务机构，运营并维护 WOSIGN_DCA 证书体系，向订户颁发包括电子邮件证书、个人证书、机构证书、设备证书在内的各类公钥证书。

与沃通建立起合同关系的第三方机构客户，可作为沃通 WOSIGN_DCA 体系下的一个下级认证机构，拥有 WOSIGN_DCA 下的子 CA 并开展其认证业务，但其子 CA 托管在沃通数字认证中心，由沃通负责维护和运营。

1.3.2 注册机构（RA）

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（订户）进行身份识别和鉴别，初始化或拒绝证书申请和吊销请求，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（订户）的身份，批准或拒绝证书申请，批准订户的证书吊销请求或直接吊销证书，批准订户的证书更新请求。

1.3.3 订户

“订户”指从沃通数字认证中心获得证书的个人、组织机构，即最终用户（end-user）。

订户通常需要同沃通数字认证中心，或其注册机构，或其授权机构签订合约获得证书，并承担作为证书订户的责任。

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

在有些情况下，证书订户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，证书订户和主体不是同一实体，如设备证书的订户是设备所属机构，而证书主体是设备。

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

证书持有者即证书订户或最终用户。

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签发的证书的个人或组织。依赖方可以是沃通的证书订户，也可以不是订户。

1.3.5 其他参与者

无规定。

1.4 证书应用

1.4.1 合适的应用

1.4.1.1 电子邮件证书

沃通签发的电子邮件证书与证书持有者的电子邮箱绑定，可用于电子邮件地址的鉴别、电子邮件内容的数字签名和加密，以实现邮件源发性证明、完整性保障及信息保密。

1.4.1.2 帐户证书

沃通签发的帐户证书与订户在某个应用服务系统中的特定帐户绑定，用于用户在该系统的登录（身份鉴别）。

1.4.1.3 个人证书

个人证书，包括个人用户证书和机构雇员证书，可用于需要区分、标识、鉴别个人身份的场合，还可用于数据加解密和信息签名，包括订单签名，以实现信息保密，提供信息源发性证明、完整性保障和抗抵赖。

1.4.1.4 机构证书

机构证书，包括机构单位证书和机构代表人证书，可用于需要区分、标识、鉴别机构身份的场合，还可用于数据加解密和信息签名，包括订单、合同签名，以实现信息保密，提供信息源发性证明、完整性保障和抗抵赖。

1.4.1.5 设备证书

设备证书用于标识服务器、运营设备，还可用于数据加解密和信息签名，以实现信息保密，及提供信息源发性证明、完整性保障。

1.4.2 受限的应用

沃通所颁发的某些证书在功能上是受到限制的，如个人证书只能用于个人订户的应用，而不能作为服务器证书或机构证书使用。机构证书只能用于代表组织机构的场合。 证书的密钥用法扩展项中限制了与证书中公钥对应私钥的使用目的（6.1.7.），如最终用户证书不能作为 CA 证书使用。这种限制是由基本限制扩展项缺省值确定的（7.1.2.5）。然而，基于扩展项的限制的有效性取决于软件，如果有关软件不遵守有关约定，其对证书的使用将超出本 CPS 限定的应用范围，将是不受保护的。

1.4.3 受禁的使用

沃通签发的证书禁止作以下用途

【i】任何要求降低安全防护的设施与系统：

- 核能设施
- 空中交通控制系统
- 民航导航系统
- 武器控制系统
- 任何其他系统故障可能导致人员伤亡或环境破坏的系统

【ii】任何法律禁止使用加密或使用数字证书的交易，或法律禁止的其他交易。

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的管理机构是沃通安全策略指导管理委员会，其联系地址如下：

深圳市沃通电子认证服务有限公司

中国深圳市南山区南海大道 1057 号科技大厦二期 A 栋 502

总机：+86-755-8600 8688

传真：+86-755-33975112

邮箱地址：Help@wosign.com

1.5.2 联系人

如果需要沃通策略文档请发邮件到信箱：Help@wosign.com ，或来信请寄：

深圳市沃通电子认证服务有限公司

中国深圳市南山区南海大道 1057 号科技大厦二期 A 栋 502

总机：+86-755-8600 8688

传真：+86-755-33975112

1.5.3 决定 CPS 符合策略的机构

沃通安全策略指导委员会。

1.5.4 CPS 批准程序

沃通有专门的策略管理机构——即安全策略指导委员会，负责 CPS 的管理。认证机构的 CPS 将会被提交到安全策略指导委员会，策略管理机构将负责评估 CPS 是否符合相关要求，如果符合，将批准 CPS。

1.6 定义与缩写

1.6.1 定义

表 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 或标识特定的订户，它包含了订户的公钥、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 签发证书的请求
证书申请者	要求一个发证机构签发证书的个人、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。
证书吊销列表（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吊销的证书。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，被吊销证书的序列号，吊销证书的时间和原因。
认证机构（CA）	一个授权签发、管理、吊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、签发、管理和吊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。当一个证书被签发后，证书申请者成为了一个订户，这时如果订户要求吊销或更新这个订户证书，CA 或 RA 可以使用挑战语识别订户的身份。
沃通公共认证体系	沃通建立的基于 PKI 的安全认证体系。
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 WOSIGN_DCA 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。该证书用于标识组织机构的 Web 服务器的身份，将一个域名与一台服务器绑定。 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保密传送。

术语	定义
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、私钥备份和签发它的公钥的过程。
未经验证的订户信息	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	指从证书签发日期和时间(或者证书上指定的一个较晚的日期和时间)开始，到证书过期或被吊销时的日期和时间为止的这段时间。
PKCS #10	公钥密码标准#10，由 RSA 安全公司制定，它定义了证书签名请求的结构。
PKCS #12	公钥密码标准#12，由 RSA 安全公司制定，它定义了私钥安全传送的方法。
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，吊销证书或更新证书。
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。
RSA	由 Rivest, Shamir and Adelman 发明的公钥密钥密码系统。
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(SSL)	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。
订户	对于个人证书，订户是指人，他是证书的主体；对于组织机构身份证书，订户是指组织机构；对于组织机构代表人身份证书，订户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

术语	定义
	有者。一个订户可以使用或被授权使用证书所含公钥对应的私钥。
订户协议	一个 CA 或 RA 拟定的协议，规定一个人或组织机构作为证书订户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”。

1.6.2 缩写

表 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	证书吊销列表
WOSIGN_DCA	沃通公共认证体系
OCSP	在线证书状态查询协议
OCA	运营 CA
DN	甄别名
LDAP	轻量目录访问协议
PCA	主认证机构
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	加密套接层协议

二. 信息发布与管理

2.1 信息库

沃通的 WWW 网站、认证系统的证书服务站点、LDAP、CRL 及 OCSP 服务器构成了沃通认证信息发布的信息库。另外，沃通授权的注册机构的证书服务站点也是认证信息发布的信息库。

2.2 认证信息的发布

沃通的认证业务规则可从沃通的 WWW 网站获取；用户证书可从沃通的 LDAP、证书服务站点获取；已被吊销了的证书的信息可从 CRL 站点、LDAP 查获，而证书的状态（有效、吊销、挂起）可通过 OCSP 获得。

2.3 发布的时间或频率

沃通的认证业务规则可通过信息库 7X24 获得。沃通签发的订户证书一经签发即发布到 LDAP 服务器供用户下载，同时订户可通过证书服务站点获得已签发的证书。通过 OCSP 对证书状态的查询是及时的。沃通对每个证书签发 CA 发布一个证书吊销列表，发布该 CA 签发的证书中的已吊销了的证书。证书吊销列表一般是每 24 小时、在午夜 0 点整更新。对于特殊的客户，沃通可为其专门定制吊销列表的更新频率。

沃通对于电子认证服务机构证书的证书撤销列表（CRL）每年至少一次进行签发。

2.4 信息库访问控制

对于 2.2 中所说的认证信息的查询、获取是公开的、没有限制的。沃通通过网络安全防护、系统安全设计、安全管理制度确保这些信息只有授权人员才能修改。

三. 身份标识与鉴证

3.1 命名

3.1.1 名称类型

根据证书主体类型不同，沃通签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 证书的签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 或者不用
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： ➢ CA 名 ➢ 证书服务类别名， ➢ 一个依赖方协议声明的引用，该依赖方协议明确了使用证书的条款。 ➢ 版权通告 ➢ 描述证书类型的文字
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.

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”或不用。
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，是证书订户所在机构的机构名。
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： ➢ CA 名 ➢ 证书服务类别名， ➢ 一个依赖方协议声明的引用，该依赖方协议明确了使用证书的条款。 ➢ 版权通告 ➢ 描述证书类型的文字
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，帐户证书，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。

3.1.2 对名称有意义的要求

对于电子邮件证书，电子邮件地址出现在证书主体甄别名的电子邮件地址字段(E 字段)，该信息作为标识订户的关键信息被鉴别、认证。电子邮件证书主体甄别名的通用名不作为标识订户的有效主体信息，不被鉴别和认证。

对于帐户证书，订户在相应应用系统中的帐户名通常出现在证书主体甄别名的通用名中，并作为标识订户的关键信息被鉴别、认证，而应用系统所属组织机构作为证书主体甄别名的一部分（出现在 O 字段）也被鉴别和认证。

个人证书主体甄别名中的通用名通常是个人的真实姓名，或者其他能唯一标识用户身份

的其他信息，如个人身份证号码等，它作为标识订户的关键信息被鉴别和认证。 机构单位证书主体甄别名的通用名通常是组织机构的名称，或者其他能唯一标识该机构的其他信息，如组织机构代码等，它作为标识订户的主要信息同其他信息一起被鉴别和认证。

机构代表人证书主体甄别名中的通用名通常是个人的真实姓名，或者其他能唯一标识用户身份的其他信息，如个人身份证号码等，它作为标识订户的主要信息同其他信息（如组织机构名称）一起被鉴别和认证。

设备证书主体甄别名中的通用名通常是该组织机构的设备名，如域名，它作为标识订户的主要信息同其他信息（如组织机构名称）一起被鉴别和认证。

3.1.3 订户的匿名或伪名

电子邮件证书和帐户证书可以使用匿名或伪名。

3.1.4 理解不同名称形式的规则

依 X.501 甄别名命名规则解释。

3.1.5 名称的唯一性

沃通签发给某个实体的证书，其主体甄别名，在该证书签发 CA 信任域内是唯一的，其中的例外是签发双证书时（一个签名证书、一个加密证书），属于同一实体的两个证书具有同样的主体甄别名，但证书的密钥用法扩展项不同。

3.1.6 商标的识别、鉴证和角色

证书申请者不应在其证书申请中使用侵害他人知识产权的名称，但沃通并不决定证书申请者是否具有相关知识产权，也无需判断、裁决或解决任何关于域名、名称、商标、服务标

的争端问题。当出现此类争端时，沃通有权拒绝或挂起证书申请，直到争端得到有效解决。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

沃通通过使用经数字签名的 PKCS#10 格式的证书请求，验证证书申请者拥有私钥。

3.2.2 机构身份的鉴证

签发机构证书、设备证书时，沃通或其注册机构按照《沃通鉴证计划》的要求对组织机构进行身份鉴证，鉴证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，政府签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，或通过权威的第三方数据库确认。
- 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信函、传真确认。

签发服务器证书时，沃通或其注册机构按照《沃通鉴证计划》的要求对组织机构进行身份鉴证，鉴证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，政府签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，通过域名注册商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）签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。

3.2.3 个人身份的鉴证

3.2.3.1 电子邮件证书和帐户证书的个人身份鉴证

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确认信息，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，但沃通不确认、不担保签发的证书中除电子邮箱地址以外的其他身份信息是真实的、可靠的、属于申请者本人的。

对于帐户证书的申请，沃通通过一定的方式确认帐户的有效性，并验证申请者（订户）知晓或拥有该帐户的秘密（如口令、或先前签发的该帐户的证书的私钥），以实现对用户身份的鉴别和验证，但沃通不确认、不担保签发的证书中除帐户名、帐户所在应用系统及系统所属机构名以外的其他身份信息是真实的、可靠的、属于申请者本人的。

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

3.2.3.2 个人证书的个人身份的鉴证

签发个人证书时，沃通或注册机构按照《沃通鉴证计划》的要求对个人进行身份鉴证，鉴证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，如通过订户银行帐户进行转帐验证；
- 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证，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“3.2.2 机构身份的鉴证”所述方法，确认组织机构信息的真实性；然后按“3.2.2 机构身份的鉴证”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签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。

3.2.4 没有验证的订户信息

通常，除了该类型证书所必须要求的身份信息需要得到明确、可靠的验证以外，下列信息是在申请时可以不被要求验证：

- 个人和单位身份证文件中联系用的电子邮件地址
- 证书中任何其它不被要求验证的信息

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

对于机构证书和设备证书，沃通在签发前，将确认证书申请获得正当授权。确认的方式有多种，如 CPS 3.2.2 中对机构授权证书申请者的确认方式。

3.2.6 互操作准则

不在此规定。

3.3 密钥更新请求的标识与鉴证

在订户证书到期前，订户需要获得新的证书以保持证书使用的连续性。沃通一般要求订户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，沃通允许订户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，订户证书除公钥、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，订户证书公钥也不改变。

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，证书订户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，订户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，系统会自动获取订户的有关信息。 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签发具有相同签发者、主体名和证书用途的证书。除非先将证书吊销，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签发者、主体名和证书用途的证书。

3.3.1 常规的密钥更新的标识与鉴证

对于一般正常情况下的密钥更新，订户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，系统自动获取订户原证书的相关信息，如订户甄别名、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证。

3.3.2 吊销之后的密钥更新的标识与鉴证

沃通对吊销后证书不进行密钥更新。

3.4 吊销请求的标识与鉴证

在沃通的证书业务中，证书吊销请求可以来自订户，也可以来自沃通或其注册机构。证书吊销的方式可以是订户自己吊销，也可以由订户要求沃通或其注册机构管理员吊销，沃通和其注册机构在认为必要的时候，有权发起吊销订户证书。

在订户自己吊销时，吊销请求的鉴别过程如下：

订户在申请证书需提交一挑战语，在订户吊销证书时提交挑战语，如果挑战语匹配，证书吊销自动完成。 订户通过认证机构、注册机构吊销时，吊销请求的鉴别过程如下：

订户通过一定的方式，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订户联系，确认要吊销证书的人或组织确实是订户本人，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。

四. 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

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、企业单位事业单位政府机构、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 以及证书垫付商等，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. 订户，发证书构已经为其签发证书，并不依赖于其是否已经接受证书。
- 5. 密钥生成器，包括电子认证服务机构和用户自己选择的密钥生成器，包括但不限于 USB Key IC 卡、加密卡、加密机等硬件提供者和 IE 等。
- 6. 主管部门，包括《中华人民共和国电子签名法》《电子认证服务管理办法》、《电子认证服务密码管理办法》等规定的各娄主管部门。

4.1.2 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；对于帐户证书，注册时申请者须正确填写正确的帐户信息，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、实名登记的电话号码、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、实名登记的电话号码等；

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。

4.2 证书申请处理

4.2.1 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。

在接到订户的证书申请后，发证机构应完成以下鉴别工作，将其作为向该订户签发证书的先决条件：

- 确认证书申请者接受订户协议中的各项条款。
- 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，如要求订户作出保证等方式)。
- 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。
- 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。

在签发了证书后，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。

4.2.2 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 CPS 的规定为申请者签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 3.2 条款关于订户信息的标识和鉴别规定
- 该申请必须满足《证书鉴证流程》的相关要求。
- 申请者接受或者没有违反对订户协议的内容和要求
- 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。

4.2.3 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 5 个工作日。

4.3 证书签发

4.3.1 证书签发中 RA 和 CA 的行为

作为证书认证系统的运营者，沃通既是一个 CA，同时也承担了部分 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 RA 职能，如接收、处理证书服务请求。

在证书签发前 RA 管理员负责证书申请的鉴证，在证书申请通过鉴证后，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 系统签发证书并返回给 RA 系统供证书申请者下载。

4.3.2 CA 和 RA 对订户的通知

无论是拒绝还是批准订户的证书申请，RA 系统会通过邮件自动通知订户。如果证书申请获得批准，邮件中包含有获取证书的信息。

4.4 证书接受

4.4.1 构成接受证书的行为

沃通订户接受证书的方式可以有如下几种：

对于由注册机构替证书订户产生证书请求、证书密钥对、下载证书的情形，则订户通过

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；当订户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。

订户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。系统记录订户下载了证书即表明订户接受了证书。

4.4.2 CA 对证书的发布

沃通有基于 LDAP 协议的目录服务，除非与证书订户间有特别的约定，沃通通常将其签发的证书发布到目录系统上。

4.4.3 CA 对其他实体的通告

对于其签发的证书，沃通及其注册机构不通知其他实体。

4.5 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。

4.5.1 订户私钥和证书使用

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。证书持有者应按 6.1，6.2，6.4 妥善保管其证书私钥。

4.5.2 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。

4.6 证书更新

4.6.1 证书更新的情形

对于沃通签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订户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，如果订户原来的注册信息继续有效，订户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 CPS 3.3。

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。

证书到期或吊销后，将无法进行更新，只能按照初始流程重新申请证书。

4.6.2 请求证书更新的实体

同 CPS 4.1.1。

4.6.3 证书更新请求的处理

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，沃通认证系统会自动完成如下验证操作：

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

若以上自动验证通过，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证、批准，及新证书的签发。

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证，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。在进行鉴证时，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。完成以上鉴证后，批准更新请求，签发新证书。

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

对于帐户证书的更新，则只需完成如下确认就可批准更新请求，签发新证书：

1）该证书对应的帐户依然有效；

2）该帐户被允许更新证书。

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，新证书将获得签发。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、签发新证书前，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，签发新证书：

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。

以上过程可以是自动或手动。

对于更换密钥的证书更新，参见 4.7.3。

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 CA 对更新证书的发布

同 4.4.2。

4.6.7 CA 对其他实体的通告

同 4.4.3。

4.7 证书密钥更新

沃通对证书密钥不进行更新服务。

4.8 证书变更

4.8.1 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。订户要变更证书中的内容时，视为申请一张新证书，需要先将原有证书吊销，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。

4.8.2 请求证书变更的实体

原证书订户。

4.8.3 证书变更请求的处理

同 4.2。

4.8.4 签发新证书时对订户的通告

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 CA 对变更证书的发布

同 4.4.2。

4.8.7 CA 对其他实体的通告

同 4.4.3。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

出现以下情况，最终用户证书必须吊销：

- 沃通、注册机构或订户有理由相信或强烈的怀疑一个订户的私钥安全已经受到损害。
- 沃通或其注册机构有理由相信订户违背了订户协议下的义务、陈述或担保。
- 沃通或其注册机构和订户达成的订户协议已经终止。
- 沃通或其注册机构有理由相信证书签发时没有依据 CP、CPS 规定的有关程序，证书签发给了非证书主体的人员或机构或没有鉴证该人员或机构在证书主体中的命名就签发了证书）。
- 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签发的一个必要前提条件既没有满足又没有豁免。
- 除了未经鉴证的订户信息外，包含在证书中的信息不正确或已经改变。
- 订户请求吊销证书。

4.9.2 请求证书吊销的实体

以下实体可以请求吊销一个最终用户证书：

- 沃通、注册机构或证书订户可以在 4.9.1 所述情形下要求吊销一个最终用户证书。

- 对于电子邮件证书、帐户证书、个人证书，证书订户可以随时根据自己的意愿请求吊销自己的证书。
- 对于机构证书，组织机构授权的代表有资格请求吊销签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吊销已经签发的证书。
- 法院、政府主管部门及其他公权力部门。

4.9.3 吊销请求的流程

当沃通或其注册机构有充分的理由相信需要吊销订户的证书时，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吊销证书。在证书吊销后，沃通或其注册机构将通过适当的方式，包括邮件、传真等，通知订户证书已被吊销及被吊销的理由。

订户可以通过以下方式要求吊销自己的证书：

- 直接访问沃通或注册机构提供的证书服务网页。在订户提交吊销请求时，需同时提供证书申请时提供的挑战语作为身份鉴别的信息。这种方式适用于所有类别的证书。
- 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。

4.9.4 吊销请求宽限期

当订户发现出现 4.9.1 中的情况时，应该尽快提出吊销请求，从发现需要吊销证书到向沃通或其注册机构提出吊销请求的时间间隔的要求如下：

- 对于电子邮件证书和帐户证书不能超过 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。

4.9.5 CA 处理吊销请求的时限

沃通或注册机构从接到吊销请求到完成处理请求的时间如下：

- 对于电子邮件证书和帐户证书不能超过 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。

4.9.6 依赖方检查证书吊销的要求

依赖方应当检查他们所信任的证书是否被吊销。检查方式是通过查询沃通发布的 CRL 完成。

4.9.7 CRL 发布频率

沃通的认证系统每天零时为证书签发 CA 产生证书吊销列表。对于特别的证书签发 CA，沃通可定制证书吊销列表产生的频率。

4.9.8 CRL 发布的最大滞后时间

一个证书从它被吊销到它被发布到 CRL 上的滞后时间不超过 24 小时。

4.9.9 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（OCSP），该服务 7X24 小时可获得。

4.9.10 在线状态查询要求

依赖方应检查证书的吊销状态。如果依赖方未通过 CRL 方式查询，则应通过 OCSP 在线方式查询。

4.9.11 吊销信息的其他发布形式

除了通过 LDAP 目录服务发布 CRL，或通过 OCSP 服务器提供证书状态查询外，沃通所发布的 CRL 也可通过沃通的相关服务网站获得。

4.9.12 密钥损害的特别要求

无论是订户还是沃通、注册机构，发现证书密钥受到安全损害时应立即吊销证书。

4.9.13 证书挂起的情形

出现以下情况，可将最终用户证书暂时挂起：

- 沃通、注册机构或订户怀疑证书的私钥安全可能已经受到损害。
- 沃通或其注册机构怀疑证书申请中的信息可能存在违背事实的陈述。
- 沃通或其注册机构有理由相信订户未履行订户协议下的义务、陈述或保证。
- 订户请求挂起证书。

4.9.14 请求证书挂起的实体

以下实体可以请求挂起一个最终用户证书：

- 沃通、注册机构或证书订户可以在 4.9.13 所述情形下要求挂起一个最终用户证书。
- 对于电子邮件证书、帐户证书、个人证书，证书订户可以随时根据自己的意愿请求挂起自己的证书。
- 对于机构证书，组织机构授权的代表有资格请求挂起签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挂起已经签发的证书。
- 法院、政府主管部门及其他公权力部门。

4.9.15 挂起请求的流程

当沃通或其注册机构有充分的理由相信需要挂起订户的证书时，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挂起证书。在证书挂起后，沃通或其注册机构将通过适当的方式，包括邮件、传真等，通知订户证书已被挂起及被挂起的理由。

订户可以通过以下方式要求挂起自己的证书：

- 接访问沃通或注册机构提供的证书服务网页。在订户提交挂起请求时，需同时提供证书申请时提供的挑战语作为身份鉴别的信息。这种方式适用于所有类别的证书。
- 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。

4.9.16 挂起的期限限制

订户证书一旦被挂起将处于挂起状态：

- 提出挂起的一方认为挂起的理由已不存在，提出恢复证书有效状态，恢复证书状态的请求过程与申请挂起的过程相同；
- 沃通、注册机构或证书订户将挂起的证书吊销，对挂起证书的申请吊销过程与 4.9.3 相同；
- 被挂起证书已到期。

4.10 证书状态服务

沃通通过网站 CRL、OCSP、LDAP 提供证书状态服务。

对于被吊销证书，其状态将同时在 CRL、OCSP 反映；对于被挂起证书，其信息将不出现在 CRL，但通过 OCSP 可查询其挂起状态。

4.10.1 操作特征

沃通提供的证书状态查询以网络服务的形式：

- CRL 通过 80 端口采用 HTTP 协议提供；
- OCSP 符合 RFC2560，反映证书的当前状态；
- 证书目录 LDAP 符合 LDAP V3（RFC3377，2251-2256，2829-2830）。

4.10.2 服务可用性

沃通的 CRL、OCSP 证书状态服务均保证 7X24 可用，并且采用了冗余技术。

4.10.3 可选特征

无。

4.11 订购结束

订购结束是指证书用户终止使用沃通的服务，它包含以下两种情况：

1. 证书到期时终止与沃通的服务

当证书到期时，证书订户不再延长证书使用期或者不再重新申请证书时，证书使用者可以提出服务终止。

2. 证书未到期时中止与沃通的服务

在证书的有效期内，由于证书订户的原因而单方面要求终止证书服务。沃通将根据证书用户的要求挂起或吊销证书。证书用户与沃通的服务终止。

所有订购结束的用户，申请时使用的数据都将妥善保管，以防丢失泄密。并将遵守《中华人民共和国电子签名法》 “第二十四条 电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期限至少为电子签名认证证书失效后五年。”的相关要求，对订户申请相关材料保存不少于七年。对于超过七年的数据进行彻底删除销毁。

4.12 密钥托管与恢复

沃通依国家密码管理部门的相关规定，提供加密证书密钥的集中产生、保存和恢复。

4.12.1 密钥托管与恢复的策略与行为

订户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。

4.12.2 会话密钥的封装与恢复的策略与行为

会话密钥是指用户在使用证书建立加密通道时临时生成的加密密钥，该密钥由应用环境来决定使用，沃通不对其进行保存和恢复。

五. 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

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《沃通物理场地建设规范》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。

5.1.2 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。

5.1.3 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，沃通认证机构还具有加热/通风/空调系统控制运营设施中的温度和湿度。

5.1.4 水患防治

沃通数据中心有专门的技术措施，防止、检测漏水的出现，并能够在出现漏水时最大程度地减小漏水对认证系统的影响。

5.1.5 火灾防护

5.1.5.1 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。

5.1.5.2 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。

5.1.5.3 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。

5.1.6 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）。

5.1.7 废物处理

沃通对敏感的文件和材料在处理之前将其切成碎片，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。

5.1.8 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建筑物以外的安全的地方。

5.1.9 注册机构物理控制

沃通注册机构的物理场地有足够的安全措施，保证只有授权的人员才能进入，只有授权

的人员才能接触系统进行证书管理。

5.2 程序控制

5.2.1 可信角色

沃通的可信人员包括：

- 网络管理员
- 模板管理员
- 系统管理员
- 超级管理员
- 业务管理员
- 业务操作员
- 业务录入员
- 业务审核员
- 业务制证员
- 司法取证员
- 审计管理员

5.2.2 每项任务需要的人数

沃通有严格策略和控制程序，以保障基于工作性质的职责分离。最敏感的操作要求多名可信人员共同参与完成。

- 鉴证和签发机构证书和管理员证书，要求 2 个可信人员的参与。
- 访问 CA 密钥离线生成室和 CA 密钥离线存放室，至少两名有访问权限的人员。
- 掌管 CA 私钥激活数据分割份额的秘密持有人员，至少 3 人。
- 操作存放有 CA 密钥的密码设备，包括密钥生成、分配、备份、销毁等，至少需
- 要 3 个秘密持有人，一个密钥管理员，一个见证人。

5.2.3 每个角色的识别与鉴别

对于物理访问控制，沃通通过门禁磁卡、指纹识别鉴别不同人员，并确定相应的权限。

对于进行证书生命周期管理的沃通、注册机构证书管理员，他们使用相应的数字证书访问认证系统、注册机构系统，完成证书管理工作。

对于系统维护人员，他们使用安全的身份鉴别机制进入认证系统进行维护工作。

5.2.4 需要职责分割的角色

所谓职责分割，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

5.3 人员控制

5.3.1 资格、经历和无过失要求

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、签发、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。

5.3.2 背景审查程序

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捏造时，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。

5.3.3 培训要求

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）。

5.3.4 再培训周期和要求

沃通根据业务需要安排。

5.3.5 工作岗位轮换周期和顺序

内部安排。

5.3.6 未授权行为的处罚

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。

5.3.7 独立合约人的要求

在有限制的情况下，独立合约人或顾问可以担任可信职位。任何合约人或顾问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。

担任可信角色的独立合约人和顾问需要通过 5.3.2 中所述的背景调查程序，否则，他们不能担任可信角色，当进入敏感区时，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。

5.3.8 提供给员工的文档

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。

5.4 审计日志程序

5.4.1 记录事件的类型

沃通对如下几类事件进行记录：

- CA 密钥生命周期内的管理事件，包括：

1) 密钥生成，备份，存储，恢复，归档和销毁。

2) 密码设备生命周期的管理事件，例如接收、使用、卸载和弃用。

这些记录都是密钥管理员完成的纸质记录。

- CA 和订户证书生命周期内的管理事件，包括：

1) 证书的申请、批准、更新、吊销等。

2) 成功或失败的证书操作。

这些记录由认证系统自动记录，保存在数据库。

- 系统安全事件，包括：

1) 成功或不成功访问 CA 系统的活动。

2) 对于 CA 系统网络的非授权访问及访问企图。

3) 对于系统文件的非授权的访问及访问企图。

4) 安全、敏感的文件或记录的读、写或删除。

5) 系统崩溃，硬件故障和其他异常。

6) 防火墙和路由器记录的安全事件。

这些记录由操作系统自动完成，沃通的系统维护人员会定期检查系统日志。

- 系统操作事件，包括：

1) 系统启动和关闭。

2) 系统权限的创建、删除、设置或修改密码。

这些记录由操作系统自动完成，沃通的系统维护人员会定期检查系统日志。

- 沃通物理设施的访问记录，包括：

1) 授权人员进出。

2) 非授权人员进出及陪同人。

3) 安全存储设施（离线密钥）的访问。

授权人员进出物理设施由沃通物理场地的访问控制系统自动记录。非授权人员进出由陪同人员作纸质记录。

- 可信人员管理记录，包括且不限于：

1) 网络权限的帐号申请记录

2) 系统权限的申请、变更、创建申请记录

3) 人员情况变化

日志记录包括如下信息：

- 每个日志记录的日期和时间。
- 对于自动日志记录，登记的序列号或序号。
- 做日志记录的实体的身份。
- 日志记录的种类。

5.4.2 处理日志的周期

对于 CA 和订户证书生命周期内的管理事件日志，沃通将一个季度进行一次内部检查、审计。

系统安全事件和系统操作事件日志沃通将每周进行一次检查、处理。

沃通物理设施的访问日志沃通将每月进行一次检查、处理。

5.4.3 审计日志保存期限

与证书相关的审计日志，在证书失效后至少保留 5 年。

5.4.4 审计日志的保护

沃通采取了物理和逻辑的访问控制方法，防止未经授权而浏览、修改、删除或其他方式篡改电子或纸质审计日志文件。

5.4.5 审计日志备份程序

对于认证系统的日志，沃通定期进行备份。

5.4.6 审计收集系统

对于电子审计信息，沃通设置了专门的审计信息存储系统，自动或人工完成审计信息的收集。对于纸质的审计信息，则有专门的文件管理柜来实现审计信息的收集。

每季度对相关记录进行分析、审计、检查。

5.4.7 对导致事件主体的通知

当审计记录报告一个事件时，沃通会立即通知引起该事件的个人、组织机构。

5.4.8 脆弱性评估

根据审计记录，沃通定期进行系统、物理场地、运营管理、人事管理等方面的安全脆弱性评估，并根据评估报告采取措施。

每季度对相关系统、物理场地、运营管理、人事管理进行安全检查。

5.5 记录归档

5.5.1 归档记录的类型

沃通对 5.4.1 所述记录类型进行归档。

5.5.2 归档记录的保存期限

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。

- 对订户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。
- 订户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。

5.5.3 归档文件的保护

沃通对各种电子、磁带、纸资形式的归档文件，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。

5.5.4 归档文件的备份程序

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（北京公司办公室机房）进行保存。

5.5.5 记录时间戳要求

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。

5.5.6 归档收集系统

沃通有专门的电子归档记录存放系统。

5.5.7 获得和检验归档信息的程序

只有可信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。

5.6 CA 密钥变更

当 CA 密钥对的累计寿命超过 CPS 6.3.2 中规定的最大生命期，沃通将启动密钥更新流程，替换已经过期的 CA 密钥对。沃通密钥变更按如下方式进行：

- 一个上级 CA 将在其私钥到期时间小于下级 CA 的生命期之前停止签发新的下级 CA 证书（“停止签发日期”）。
- 产生新的密钥对，签发新的上级 CA 证书。
- 在“停止签发证书的日期”之后，对于批准的下级 CA 或最终用户证书请求，将采用新的 CA 密钥签发证书。
- 上级 CA 继续利用原来的 CA 私钥签发 CRL 直到利用原私钥签发的最后的证书过期为止。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

沃通已制定各种应急处理方案，规定了相应的事故和损害处理程序，这些应急处理方案有：

1) 认证系统应急方案；
2) 电力系统应急方案；
3) 消防应急方案；
4) 网络与信息系统应急方案；
5) 安全事故应急处理方案等。

5.7.2 计算机资源、软件和/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。

5.7.3 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） 立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其它公共媒体对订户进行通告，采取措施保证用户利益不受损失。

2） 立即吊销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。同时沃通立即生成新的密钥对，并自签发新的根证书。

3） 新的根证书签发以后，按照本 CPS 关于证书签发的规定，重新签发下级证书和下级操作子 CA 证书。

4） 沃通新的根证书签发以后，将会立即通过沃通信息库、目录服务器、HTTP 等方式进行发布。

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，向沃通申请签发新的证书。

2） 沃通立即向电子认证服务管理办公室和其他政府管理部门汇报，通过网站和其它公共媒体对订户进行通告，采取措施保证用户利益不受损失。

3） 立即吊销所有由该子 CA 签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。

4） 新的子 CA 证书签发以后，按照本 CPS 关于证书签发的规定，重新签发订户证书。

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

证书订户的私钥出现遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，订户应该按照本 CPS 的规定，首先申请证书吊销，并按照规定重新申请新的证书。

5.7.4 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。

5.8 CA 或 RA 的终止

当沃通及其注册机构需要停止其业务时，将会严格按照《中华人民共和国电子签名法》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。

六. 技术安全控制

6.1 密钥对的产生和安装

6.1.1 密钥对的产生

6.1.1.1 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规程进行产生。沃通密钥生成规程规定了 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。

6.1.1.2 订户密钥对的产生

对于电子邮件证书、帐户证书、个人证书和机构证书，订户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，订户使用服务器程序使用的密码模块（包括 SSL 硬件加速卡）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。

6.1.2 私钥传送给订户

沃通各类 CA 证书密钥对由沃通数字认证中心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。

对于沃通签发的其他最终用户证书，通常的情况下密钥对在订户本地的密码模块（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。

6.1.3 公钥传送给证书签发机关

需要沃通认证的证书公钥，订户通过 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。

6.1.4 CA 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，当证书订户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订户。

6.1.5 密钥的长度

沃通 CA 和订户密钥对至少是 1024 位 RSA。

6.1.6 公钥参数的生成和质量检查

符合国家密码管理部门的要求。

6.1.7 密钥使用目的

主 CA 的密钥用于签发运营 CA 的证书及 CRL，运营 CA 的密钥用于签发订户证书。订户证书的使用目的需满足证书策略的要求，证书中的密钥用法扩展项按表 5 所示设定：

表 5 - 密钥用法扩展项的设置

		CA 证书	帐户 证书	机构 证书	个人 证书	服务器 证书	运营设备证书	电子邮件证书
Criticality		非关键	非关键	非关键	非关键	非关键	非关键	非关键
0	Digital Signature 数字签名	未设置	设置	设置	设置	设置	设置	设置
1	Non Repudiation 不可抵赖性	未设置	未设置	设置	设置	未设置	未设置	未设置
2	Key Encipherment 密钥加密	未设置	设置	设置	设置	设置	设置	设置
3	Data Encipherment 数据加密	未设置	未设置	未设置	未设置	设置	未设置	未设置
4	Key Agreement 关键协议	未设置	未设置	未设置	未设置	设置	未设置	未设置
5	Key Cert Sign 主要证书登录	设置	未设置	未设置	未设置	未设置	未设置	未设置

6	CRL Sign CRL 登录	设置	未设置	未设置	未设置	未设置	未设置	未设置
7	Encipher Only 只加密	未设置	未设置	未设置	未设置	未设置	未设置	未设置
8	Decipher Only 只解密	未设置	未设置	未设置	未设置	未设置	未设置	未设置

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、证书签发 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。

6.2.2 私钥多人控制（m 选 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。

6.2.3 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订户加密证书的私钥进行托管。

6.2.4 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，沃通数字认证中心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，沃通建议订户对私钥进行备份，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。

6.2.5 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，沃通数字认证中心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，但如果订户存放证书私钥的密码模块允许私钥备份，沃通建议订户对私钥进行归档，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。

6.2.6 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。

沃通数字认证中心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。

6.2.7 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。

6.2.8 激活私钥的方法

6.2.8.1 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。

6.2.8.2 运营设备证书私钥

对于沃通数字认证中心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。

6.2.8.3 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。

6.2.9 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。

6.2.10 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。若私钥吊销、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。

6.2.11 密码模块的评估

由国家密码管理部门负责。

6.2.12 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；

6.3 密钥对管理的其他方面

6.3.1 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。

6.3.2 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。 另外无论是订户证书还是 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。对于不同的证书，密钥对通过证书更新允许的最长使用期限如下：

- 对于 1024 位主 CA 证书，其密钥对的最长允许使用年限是 30 年。
- 对于 1024 位其他 CA 证书，其密钥对的最长允许使用年限是 15 年。
- 对于 1024 位最终用户证书，其密钥对的最长允许使用年限是 2 年。

6.4 激活数据

6.4.1 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。

沃通数字认证中心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订户证书私钥保护口令的要求。

如果订户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。

沃通还建议订户使用双因素机制（如硬件+密码，生物识别设备+密码等）来控制私钥的激活。

6.4.2 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。

6.4.3 激活数据的其他方面

6.4.3.1 激活数据的传送

存有沃通数字认证中心 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。

沃通数字认证中心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。

通常情况下订户证书私钥的激活数据由订户自己产生、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，订户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，有可能代订户在特定的密码硬件（如 USB Key）中产生私钥并产生相应的激活数据，在这种情况下，沃通数字认证中心或其注册机构，或者通过面对面的方式，或者通过电话、电子邮件等方式，将激活数据传送给订户。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，订户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。

6.4.3.2 激活数据的销毁

存有沃通数字认证中心 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。

当订户证书私钥的激活数据不需要时应该销毁，订户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。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

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。

6.5.2 计算机安全评估

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。

6.6 生命周期技术控制

6.6.1 系统开发控制

沃通通过内部流程来控制证书认证系统的研发工作， 并确保该系统安装的可靠性。

6.6.2 安全管理控制

沃通已制定了各种安全策略、管理制度与流程对 CA 运营系统进行安全管理。

6.6.3 生命期的安全控制

沃通的证书认证系统在系统设计过程中充分进行了安全性考虑，在开发过程中有严格的流程进行代码安全管理，在开发完成后进行了严格的安全测试，在正式使用前通过了国家有关部门的系统安全性审查。

6.7 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。

6.8 时间戳

沃通数字认证中心签发的数字证书、CRL、OCSP 响应以及时间戳服务响应包含有时间及日期信息，且这些时间和日期信息是经过数字签名的。

七. 证书、CRL 和 OCSP

7.1 证书

沃通签发的证书符合(a)ITU-T X.509v3 4-edition（2001）：信息技术-开放系统互连-目录：认证框架（1997 年 6 月）标准；(b) RFC 3280：Internet X.509 公钥基础设施证书和 CRL 结构（1999 年 1 月）。

证书至少包含基本的 X.509v1 域，其规定值或值的限制如表 6 所描述。

表 6 - 证书结构的基本域

域	值或值的限制
版本	V3
序列号	每个证书唯一的值
签名算法	用于签证书的算法的名称（见 CPS 7.1.3）
签发者 DN	签发者的甄别名。
有效期从	基于国际通用时间(UTC)，和北京时间同步，按 RFC 3280 要求编码
有效期到	基于国际通用时间(UTC)，和北京时间同步，按 RFC 3280 要求编码。有效期限的设置符合 CPS 6.3.2 规定的限制
主体 DN	证书持有者或实体的甄别名。
公钥	根据 RFC 3280 编码，使用 CPS 7.1.3 中指定的算法，密钥长度满足 CPS 6.1.5 指定的要求。
签名	生成和编码满足 RFC 3280 的要求。

7.1.1 版本号

X.509v3 证书。

7.1.2 证书扩展项

针对特别的用户，沃通签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。

7.1.2.1 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 FALSE。

7.1.2.2 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。

7.1.2.3 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。

7.1.2.4 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 FALSE。

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。对于最终用户证书签发 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。

7.1.2.5 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	帐户证书	服务器证书	个人证书

		书			
Criticality		非关键	非关键	非关键	非关键
0	Server Auth 服务器认证	未设置	未设置	设置	未设置
1	Client Auth 客户端认证	未设置	设置	设置	设置
2	CodeSigning 代码签名	未设置	未设置	未设置	未设置
3	EmailProtection 邮箱保护	设置	设置	未设置	设置
4	IpsecEndSystem 安全协议末端系统	未设置	未设置	未设置	未设置
5	IpsecTunnel 安全协议隧道	未设置	未设置	未设置	未设置
6	IpsecUser 安全协议用户	未设置	未设置	未设置	未设置
7	TimeStamping 时间戳	未设置	未设置	未设置	未设置
8	OCSP Signing OCSP 签字	未设置	未设置	未设置	未设置
	Microsoft Server Gated Crypto (SGC) OID: 1.3.6.1.4.1.311.10.3.3	未设置	未设置	设置	未设置
-	Netscape SGC - OID: 2.16.840.1.113730.4.1	未设置	未设置	设置	未设置
-	TBD - OID: 2.16.840.1.113733.1.8.1	未设置	未设置	未设置	未设置

7.1.2.6 CRL 的分发点（cRLDistributionPoints）

沃通签发的证书中包含 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。

7.1.2.7 签发 CA 密钥标识符

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

7.1.2.8 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。

7.1.3 密钥算法对象标识符

沃通签发的证书按照 RFC 3280 标准，用 sha1RSA 算法签名：

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}。

7.1.4 名称形式

沃通签发证书的甄别名符合 X500 关于甄别名的规定。对于证书主体甄别名，O 代表证书持有者所在的组织机构，第一个 OU 代表证书持有者所在的部门。

对于证书签发者甄别名，O 代表证书签发机构，第一个 OU 签发机构中的部门或服务类（如 CN Individual Comsumer Service Center）。甄别名可以包含不止一个的 OU 用于存放其他信息，如可将一个附加的组织部门(OU)域包含在最终用户证书中，该域指出证书对应的依赖方协议所在的 URL。

7.1.5 名称限制

除一类证书外，沃通签发的其他证书中的通用名不能使用假名、伪名。

7.1.6 证书策略对象标识符

未使用。

7.1.7 策略限制扩展项的用法

未使用。

7.1.8 策略限定符的语法和语义

未规定。

7.1.9 关键证书策略扩展项的处理规则

与 ITU X.509 和 RFC3280 规定一致。

7.2 CRL

沃通认证系统签发的 CRL 符合 RFC3280 标准。CRL 至少包含如表 8 所述基本域和内容。

表 8 - CRL 结构的基本域

域	值或值的限制
版本	V2
签名算法	签发 CRL 的算法。使用 sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)算法签名。
颁发者	签发 CRL 的实体。颁发者甄别名。
有效期	CRL 的签发日期。

下次更新	CRL 下次签发的日期。对于 CA，隔 2 年；对于最终用户证书 24 小时。
吊销的证书	列出吊销的证书，包括吊销证书的序列号和吊销日期。

7.2.1 版本号

V2。

7.2.2 CRL 和 CRL 条目扩展项

与 ITU X.509 和 RFC3280 规定一致。

7.3 OCSP

沃通认证系统签发的 OCSP 响应符合 RFC2560 标准。OCSP 响应至少包含如表 9 所述基本域和内容。

表 9 - OCSP 结构的基本域

域	值或值的限制
状态	响应状态，包括成功、请求格式错误、内部错误、稍候重试、请求没有签名和请求签名证书无授权，当状态为成功时必须包括以下各项。
版本	V1
签名算法	签发 OCSP 的算法。使用 sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)算法签名。
颁发者	签发 OCSP 的实体。签发者公钥的 SHA1 数据摘要值和证书甄别名。
产生时间	OCSP 响应的产生时间。
证书状态列表	包括请求中所查询的证书状态列表。每个证书状态包括证书标识、证书状态以及证书吊销信息。
证书标识	包括数据摘要算法(SHA1，OID: 1.3.14.3.2.26)、证书甄别名数据摘要值、证书公钥数据摘要值和证书序列号。
证书状态	证书的最新状态，包括有效、吊销和未知。
证书吊销信息	当返回证书状态为吊销时包含吊销时间和吊销原因。

7.3.1 版本号

V1。

7.3.2 OCSP 扩展项

与 RFC2560 一致。

八. 认证机构审计和其他评估

沃通数字认证中心在物理控制、密钥管理、操作控制、证书生命周期管理等方面的执行等情况将被审查、评估，以确定实际发生情况是否与预定的标准、要求一致，称为一致性审计，并根据审查结果采取行动。

8.1 评估的频率和情形

沃通每年进行一次一致性审计，由电子认证服务的主管部门组织。

8.2 评估者的资质

由电子认证服务的主管部门负责确定。

8.3 评估者与被评估者之间的关系

评估者为电子认证服务的主管部门选择的独立第三方人员，与沃通不存在任何商业利益关系。

8.4 评估的内容

评估的内容包括：CA 环境控制、服务完整性（包括密钥和证书生命周期管理控制）和 CPS 对实际业务情况的披露和执行情况等。

8.5 对问题与不足采取的措施

沃通管理层将对审计报告进行评估，对在一致性审计中发现的重大意外或不作为积极采取扑救措施，直到问题解决。从完成审计到采取行动纠正问题的时间不超过 30 天。

8.6 评估结果的传达与发布

电子认证服务主管部门的年度审查结果将在其相关网站上公开，任何人均可查询。

8.7 其他评估

除了电子认证服务主管部门的年度审计外，沃通将定期进行内部审计评估，审计评估的内容与外部审计一致。

九. 其他业务和法律事务

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 证书查取的费用

沃通目前不对证书查取收取专门的费用。

9.1.3 证书吊销或状态信息的查询费用

证书吊销和吊销列表（CRL）的获取不应收取任何费用。沃通有可能根据需要将 OCSP 服务作为增值服务收取费用。

9.1.4 其他服务费用

无规定。

9.1.5 退款策略

如果由于沃通的原因，造成订户合同无法履行、订户证书无法使用，沃通会将有关费用返还给订户。

9.2 财务责任

9.2.1 保险范围

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

9.2.2 其他资产

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。

9.2.3 对最终实体的保险或担保

沃通客户保障计划提供的服务保障针对的最终实体主要是证书订户和证书依赖方。

9.3 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。

9.3.1 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；

9.3.2 不属于保密的信息

证书、证书状态信息及信息库中的信息，都不是不需保密的信息。

9.3.3 保护保密信息的责任

沃通不但有各种严格的管理制定、流程和技术手段保护自身的商业秘密，并且把保护客户信息作为自己应尽的义务。沃通的每个员工到要接受信息保密方面的培训。

9.4 个人隐私保密

9.4.1 隐私保密方案

沃通有客户隐私计划保护证书订户的个人信息。

9.4.2 作为隐私处理的信息

作为隐私处理的信息包括，订户注册证书中提交的、但不在证书中显示的信息，包括联系电话、地址等；个人与沃通、沃通注册机构签订的协议。

9.4.3 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。

9.4.4 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。

9.4.5 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。

9.4.6 依法律或行政程序的信息披露

由于法律执行、法律授权的行政执行的需要，沃通及其注册机构有可能需要将有关信息在客户知晓或不知晓的情况下提供有关执法机关、行政执行机关，即使出现这种情形，沃通及其注册机构也将尽可能地保护客户隐私信息。

9.4.7 其他信息披露情形

对其他信息的披露受制于法律、订户协议。

9.5 知识产权

9.5.1 证书和吊销信息中的知识产权

沃通对它签发的证书、证书吊销列表及其中信息的拥有知识产权，证书公钥是订户的知识产权。

9.5.2 CPS 中的知识产权

沃通对本 CPS 拥有知识产权。

9.5.3 命名中的知识产权

证书订户对证书注册信息及签发给他的证书中包含的商标、服务标志或商品名和甄别名拥有知识产权。

9.5.4 密钥和密钥材料的知识产权

证书中的密钥对是证书中主体对应实体或实体拥有者的知识产权。

9.6 陈述与担保

9.6.1 CA 的陈述与担保

订户同意沃通订户协议是订户注册申请沃通证书的一个条件，在订户成功完全证书申请注册前，订户必须以下列两种方式之一接受订户协议：

1）对订户协议文件签名并提交给沃通或其注册机构；

2）阅读注册页面上订户协议，并点击同意订户协议。

依赖方决定信赖沃通签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。订户和依赖方必须依订户协议和依赖方协议确保证书用于允许使的目的。

沃通、注册机构和订户之间的担保、免责和有限责任由他们之间的协议规定约束。

沃通对证书订户做出如下担保：

- 证书中不存在批准证书申请或签发证书时沃通已知的对事实的实质性错误描述；
- 批准证书申请或签发证书时，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 WOSIGN_DCA 证书策略所有实质性的要求；
- 吊销服务和信息库的使用在所有方面符合沃通 WOSIGN_DCA 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、验证的订户信息外，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签发给了个人或组织机构(它们的名字包含在证书中)，订户已经根据 CPS 4.4 接收了该证书。
- 批准证书申请或签发证书的实体签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。

9.6.2 RA 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证工作，并且确认了信息是正确的、准确的。

9.6.3 订户的陈述与担保

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订户协议并且同意订户协议，并且：

- 在证书申请时，订户的所有陈述都是对的；
- 订户提供的，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，订户同意做到：

- 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订户的数字签名，订户知晓要签名的内容，产生数字签名时，订户已经接受了证书，且该证书没有过期或吊销。

- 订户对自己的私钥进行了有效的保护，其他人员无法使用订户的私钥。

9.6.4 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。

9.6.5 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。

9.7 担保免责

沃通不对其签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。

9.8 有限责任

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签发、假冒，或管理上的疏忽导致 CA 私钥泄漏、盗用等，造成了证书订户、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、吊销（错误）证书、经济赔偿。

对于电子邮件证书、帐户证书、以及设备不涉及经济赔偿，只涉及恢复证书使用、吊销

（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 10,000 元
机构证书	最高人民币 24,000 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。

9.9 赔偿

有下列情形之一的，沃通承担有限的赔偿责任：

- 沃通将证书错误的签发给订户以外的第三方，导致订户或者依赖方遭受损失的；
- 订户提交的注册信息或者资料真实、完整、准确，但沃通签发了有错误信息的证书，导致订户或者依赖方遭受损失的；
- 订户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签发的证书中，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，致使订户或者依赖方遭受损失的；

订户有下列情形之一，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；
- 订户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订户私钥的安全损害、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；
- 订户使用的名字（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吊销。

有下列情形之一的，沃通不承担赔付责任：

- 因订户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订户或者依赖方遭受损失的。

赔付的过程将受到电子认证服务管理办公室的监督与管理。

9.10 有效期限与终止

9.10.1 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。

9.10.2 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。

9.10.3 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、订户协议、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。

9.11 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，如在主动吊销订户证书、发现订户将证书用于规定外用途及订户其他违反订户协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知订户、依赖方。

9.12 修订

9.12.1 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，沃通安全策略指导委员会将对本 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，由沃通安全策略指导委员会负责组织有关文档、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。

9.12.2 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：http://www.wosign.cn 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。

9.12.3 必须修改业务规则的情形

由沃通安全策略指导委员会根据公司业务情况决定。

9.13 争议解决

当沃通、订户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。沃通订户协议、依赖方协议和其他订户协议已包括该项内容。

9.14 管辖法律

中华人民共和国法律、规则、规章、法令和政令将管辖沃通的业务活动。沃通的任何业务活受有关法律、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。

9.15 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。

9.16 一般条款

9.16.1 完整协议

CP、CPS、订户协议及依赖方协议及其补充协议将构成沃通 WOSIGN_DCA 信任域参与者之

间的完整协议。

9.16.2 转让

沃通、注册机构、订户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。

9.16.3 分割性

法律允许的范围内，在沃通订户协议、依赖方协议和其他订户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。

9.16.4 强制执行

在沃通、注册机构、订户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。

9.16.5 不可抗力

当由于不可抗力，如地震、洪灾、雷电等自然灾害和战争等，造成沃通、注册机构无法提供正常的服务时，沃通、注册机构不承担由此给客户造成的损失。

9.17 其他条款

未规定。