沃通电子认证服务有限公司
事件型证书策略（CP2）

版本：1.0.1

发布日期：2024 年 3 月 1 日

生效日期：2024 年 3 月 1 日

沃通电子认证服务有限公司

版本控制表

版本	状态	修订说明	审核/批准人	生效时间
1.0.1	版本发布	初始版本	沃通安全策略管理委员会	2024 年 3 月 1 日

声明

本 CP 全部或者部分支持下列标准：

RFC3647：互联网 X.509 公钥基础设施-证书策略和证书业务声明框架

RFC2459:互联网 X.509 公钥基础设施-证书和 CRL 属性

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

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

RFC 5280:Internet X.509 公钥基础设施证书和 CRL 结构

GB/T 20518-2006:信息安全技术 公钥基础设施 数字证书格式

GB/T 26855-2011：信息安全技术公钥基础设施证书策略与认证业务声明框架

目 录

1.引言

1.1 概述

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

沃通公司面向签名行为业务场景签发出事件型数字证书。事件型数字证书一般用于一次性事件型电子签名，签名过后私钥销毁。通过对签名行为业务场景的信息数据签名，证明业务数据自签名后未发生篡改，保证业务场景信息数据的完整性和签名行为的不可抵赖性。

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

本文档《沃通电子认证服务有限公司事件型证书策略》（以下简称《沃通事件型证书策略》）满足互联网标准组织制定的 RFC3647《互联网 X.509 公钥基础设施-证书策略和证书业务声明框架》，以及国内标准 GB/T 26855-2011《信息安全技术公钥基础设施证书策略与认证业务声明框架》的框架和内容要求。《沃通事件型证书策略》适用范围为沃通发放的事件型证书。具体设定了证书策略、生命周期、使用、依赖和管理的角色、责任与要求，以及各相关主体的职责。为批准、签发、管理和使用证书和相关的可信服务制定业务，提供技术、策略和法律上的要求和规范。

1.2 文档名称与标识

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

1.3 PKI 参与者

1.3.1 电子认证服务机构

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

沃通是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。

1.3.2 注册机构

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

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

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

1.3.3 订户

订户是指向沃通申请数字证书的实体。

根据业务场景，事件型证书的订户分为两种，一种是电子签名人，一种是申请对签名行为业务场景的相关信息进行固化的实体。

1.3.4 依赖方

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

1.3.5 其他参与者

其他参与者指为 CA 证书服务体系提供相关服务的其他实体。

1.4 证书应用

1.4.1 适合的证书应用

沃通签发的事件型证书适合应用在企业信息化、电子政务和电子商务等领域，用于证明业务场景中所进行的电子签名行为。

1.4.2 限制的证书应用

沃通颁发的数字证书禁止在违反国家法律、法规或破坏国家安全的情况下使用，由此造成的法律后果由订户负责。

1.5 策略管理

1.5.1 策略文档管理机构

《沃通事件型证书策略》的管理机构是沃通安全策略管理委员会。由沃通安全策略管理委员会负责《沃通事件型证书策略》的制订、发布、更新等事宜。

1.5.2 联系人

《沃通事件型证书策略》在沃通官网进行发布，对具体个人不另行通知。

官网地址：https://www.wotrus.com/

服务邮箱：casupport@wotrus.com

总机号码：+86-755-8600 8688

传真号码：+86-755-33975112

联系地址：中国深圳市南山区南海大道 1057 号科技大厦二期 A 栋 502

1.5.3 决定 CP 符合策略的机构

沃通安全策略管理委员会。

1.5.4 CP 批准程序

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

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

1.6 定义和缩写

下列定义适用于《沃通事件型证书策略》：

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

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

2) 证书策略（CP）Certification Policy

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

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

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

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

受用户信任，负责创建和分配公钥证书的权威机构。

5) 注册机构（RA）Registration Authority

具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动吊销或挂起证书，处理订户吊销或挂起其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA 并不签发证书（即 RA 代表 CA 承担某些任务）。

6) 事件型数字证书 Event Certificate

沃通公司面向签名行为业务场景签发出的数字证书。在业务过程中，根据订户提交的业务场景中相关信息（电子文档、签名行为特征信息、手写笔迹或其他签名行为证据信息等）自动固化至数字证书的扩展域，签发出事件型数字证书。事件型数字证书所对应的私钥为一次性使用，对业务场景的信息数据进行电子签名，在使用后即被销毁。

在本 CP 中，如无特殊定义，所述的数字证书，均指事件型数字证书。

7) 私钥 Private Key

非对称密码算法中只能由拥有者使用的不公开密钥。

8) 公钥 Public Key

非对称密码算法中可以公开的密钥。

2. 信息发布与管理

2.1 信息库

沃通的信息库是一个对外公开的信息库，面向订户及依赖方提供信息服务。提供信息服务包括但不限于以下内容： CPS 和 CP 以及其他不定期发布的信息。

沃通的信息库地址为：https://www.wotrus.com/ca/。

2.2 认证信息的发布

《沃通事件型证书策略》发布在沃通公司的网站上（https://www.wotrus.com/ca/），供相关方下载、查阅。

2.3 发布时间或频率

《沃通事件型证书策略》一经网站发布，即时生效。

2.4 信息库访问控制

对于公开发布的 CP 和 CPS 等公开信息，沃通允许公众自行通过网站进行查询和访问。

3. 标识与鉴别

3.1 命名

3.1.1 名称类型

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

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

3.1.2 对名称意义化的要求

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

3.1.3 订户的匿名或伪名

不接受或者允许任何匿名或者伪名，仅接受有明确意义的名称作为唯一标识符。

3.1.4 理解不同名称形式的规则

数字证书符合 X.509 标准，甄别名格式遵守 X.500 标准。

甄别名的命名规则由沃通公司定义。

3.1.5 名称的唯一性

在 CA 认证服务体系中，不同订户的证书主体的名称是唯一的。但对于同一订户，可以用其主体名为其签发多张证书，但证书的扩展项不同。

3.1.6 商标的识别、鉴证和角色

沃通签发的证书不包含任何商标或者可能对其他机构构成侵权的信息。

3.2 初始身份确认

3.2.1 证明持有私钥的方法

事件型证书申请人在签名行为发生时产生证书请求，包括申请人的身份信息，以及证书申请人在进行签名行为时的记录信息(包括证书申请人的签名场景、签名动作、签名内容对象或签名内容特征值，从而可以事后有效还原签名行为)。签名行为的记录信息与证书申请人的身份信息在证书申请时进行绑定。因此，在签名行为发生时证书申请人视作其私钥的唯一持有者。

3.2.2 订户身份的鉴别

事件型证书订户身份的鉴别参照个人或组织身份鉴别方法，订户在申请事件型证书前，需通过身份鉴别，有效确认订户身份，并接受相关条款，自愿承担相应责任。在事件型证书鉴别过程中，沃通或授权的注册机构负责接收订户的证书申请，对订户身份真实性进行审核，同时收集和记录订户的身份信息以及电子签名行为记录信息。若订户拒绝接受沃通的身份鉴别要求，将被视为放弃证书申请。此外，沃通声明保留拒绝任何申请的权利，并无义务解释拒绝申请的原因。

3.2.3 没有验证的订户信息

订户提交鉴证文件不属于鉴别范围内的信息，为没有验证的订户信息。对于没有验证过的订户信息，沃通将对申请信息以书面或电子形式进行归档。沃通将不承诺这类信息的真实性，并且不承担由于这类信息的不真实、不完整等引起的任何责任和解决纠纷的义务。

3.2.4 授权的确认

当申请人代表委托申请人申请证书时，需要出示足够的证明信息或授权委托条款以证明个人或机构是否真实存在，申请人是否已获得委托人的授权。沃通或授权的注册机构有责任确认该授权信息，并将授权信息妥善保存。

3.2.5 互操作准则

互操作可能是交叉认证、单身交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各

自认证策略的 CA 中心之间建立相互信任关系，从而使双方的订户可以实现互相认证。

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

3.3 密钥更新请求的身份标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

事件型证书的密钥只适用于一次性签名事件，没有证书密钥更新服务。

3.3.2 吊销后密钥更新的标识与鉴别

事件型证书的密钥只适用于一次性签名事件，不涉及吊销后密钥更新服务。

3.3.3 证书变更的标识与鉴别

事件型证书的密钥只适用于一次性签名事件，没有证书变更服务。

3.4 吊销请求的标识与鉴别

事件型证书只针对即时性签名事件，证书使用后即时失效，没有证书吊销服务。

4. 证书生命周期操作要求

4.1. 证书申请

事件型证书仅接受在线申请方式，订户应遵守证书申请操作所规定的步骤。

4.1.1 证书申请实体

证书申请实体包括个人和具有独立法人资格的组织机构(包括行政机关、事业单位、企业单位、社会团

体和人民团体等)和有明确身份归属的其他网络主体均可申请事件型证书。

4.1.2 申请过程与责任

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

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

申请过程中各方责任为：

1） 订户

订户需要提供 3.2 所述的有效身份证明材料，并确保材料真实准确，配合 沃通或授权的注册机构完成对身份信息的采集、记录和审核。

2） 沃通

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

3） 依赖方

在信任沃通签发的证书时，依赖方需承担如下责任：

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

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

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

4） 密钥生成器提供者

一旦证书申请者选择了某种密钥生成器，则表明该申请者信赖由其产生的密钥对的安全性和可靠性，

沃通并不为此提供任何形式的担保，也没有责任和权力对由此产生的纠纷进行处理。

5） **主管部门**

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

4.2. 证书申请处理

4.2.1. 执行识别与鉴别功能

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

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

1） 确认证书申请者接受订户协议中的各项条款；

2） 按照事件型证书的要求对证书申请者的身份进行验证；

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

4） 确认证书中包含的信息，除了未经验证的订户信息外，都是准确的；

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

6） 确认任何委托办理的各方之间的授权合法性和委托方、受托方的身份。

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

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

4.2.2 证书申请批准和拒绝

沃通或授权的注册机构根据《沃通事件型证书策略》所规定的身份鉴别流程，对证书申请人身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

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

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

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.3 处理证书申请的时间

事件型证书申请为即时处理。

4.3 证书签发

4.3.1 证书签发过程中电子认证服务机构的行为

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

沃通在批准证书申请之后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

4.3.2 电子认证服务机构对订户的通知

事件型证书用于标识和证明订户的电子签名行为。沃通为订户签发证书后，将直接应用于对应的业务场景相关信息的电子签名。订户成功完成电子签名，即视为沃通证书签发成功，沃通不再就证书签发向订户进行其他方式的通告。

4.4 证书接受

4.4.1 构成接受证书的行为

事件型证书签发完成后，并将证书应用于对应的电子签名时起，就被视为同意接受证书。

4.4.2 电子认证服务机构对证书的发布

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

查询方式包括但不限于用户在线自助或人工受理等。对于订户查询，沃通核实身份后提供查询服务。

对于其他实体查询，为保护证书订户的数据安全和隐私保护，沃通只承诺对其他实体提交的证书进行核实。

4.4.3 电子认证服务机构在颁发证书时对其他实体的通告

对于沃通签发事件型证书，沃通不对其他实体进行通告。

4.5 密钥对和证书使用

4.5.1 订户私钥和证书使用

订户在提交了证书申请并接受了沃通所签发的证书后，均视为已经同意遵守与沃通、依赖方有关的权利和义务的条款。只有在此前提下，订户才能使用相应的证书及与之对应的私钥。证书的使用须遵循本文档及相关 CP/CPS 的规定。订户只能在合法的应用范围内使用私钥和证书，且使用行为需符合订户协议的要求。

事件型证书仅适用于订户对应的电子签名行为，订户只能在此次电子签名中使用私钥和证书。在接受相关证书后，订户方可使用对应的私钥执行电子签名运算。私钥在完成本次电子签名运算后将予以销毁，此后订户必须停止使用该证书对应的私钥。

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

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

4.5.2 依赖方对公钥和证书的使用

依赖方在信任证书与签名之前，需独立作出应有的努力和合理判断：

1) 确认证书是否由可信的 CA 认证机构签发；

2) 确认证书是否适用于特定目的；并判断证书未用于本文档或法律法规所禁止或限制的使用范围。用户在接受证书后，需负责确保证书的恰当使用。

3） 核实证书在使用过程中与其包含的内容是否一致（若证书中某些字段明确了使用范围和目的，则证书仅在此范围内有效，如密钥用途）。

除非本文档另有规定，否则证书不应被视为发证机构对任何权力或特权的承诺。依赖方仅能在本文档规定的范围内信任证书及其中包含的公钥，并据此作出决策。

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

4.6 证书更新

事件型证书仅用于业务场景的一次性的电子签名，不提供证书更新服务。

4.7 证书密钥更新

事件型证书私钥在使用过一次后即销毁，不提供证书密钥更新服务。

4.8 证书变更

事件型证书仅用于业务场景的一次性的电子签名，不提供证书变更服务。

4.9 证书吊销和挂起

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

4.10 证书状态服务

事件型证书仅用于订户特定一次的电子签名行为，证书使用一次后即失效， 根据依赖方约定，可向依赖方提供状态查询服务。

4.11 订购结束

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

4.12 密钥生成、备份与恢复

订户的签名密钥对由签名设备生成密钥并执行签名后，即时销毁，签名密钥不进行保管。

5. 电子认证服务机构设施、管理和操作控制

本章规定参见沃通已发布的 CPS。

6. 认证系统技术安全控制

6.1 密钥对的生成和安装

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

6.1.1 密钥对的产生

CA 系统和 RA 系统的密钥对是在密码机内部产生，密码机应具有商用密码产品认证证书。在生成 CA 密钥对时，沃通按照密码机密钥管理制度，执行详细的操作流程控制计划，选定并授权 5 个密钥管理员，密钥管理员凭借智能 IC 卡对密钥进行控制。

事件型证书的签名密钥对由签名设备生成，加密密钥对由密钥管理中心生成。

6.1.2 私钥传送给订户

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

6.1.3 公钥传送给证书签发机构

事件型证书的签名公钥通过安全通道，经注册机构传递到沃通。

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

6.1.4 电子认证服务机构公钥传送给依赖方

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

6.1.5 密钥的长度

密钥算法和长度符合国家密码主管部门的规定。

6.1.6 公钥参数的生成和质量检查

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

6.1.7 密钥使用目的

订户的签名密钥可以用于提供安全服务，实现身份认证、不可抵赖性和信息的完整性等，用于签署具备法律效力的电子文档和电子交易数据。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

沃通所用的密码设备都是经国家相关部门认可的产品，其接口、协议、密钥和物理安全要符合国家相关规范要求。

6.2.2 私钥的多人控制

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

6.2.3 私钥托管

加密私钥的保护、管理、存档、备份、托管等，由沃通密钥管理中心进行规范和决定。由于事件型证书的订户证书私钥在使用后即销毁，订户证书私钥存放在硬件安全模块中。

6.2.4 私钥备份

对于订户签名证书，如果其私钥存放在软件密码模块中，建议订户对私钥进行备份，备份的私钥需要采用口令保护等授 权访问控制，防止非授权的修改或泄露。

对于订户加密证书，由于事件型证书私钥在使用后即销毁，不进行备份。

6.2.5 私钥归档

沃通的私钥经过加密后按照严格的安全措施保存，订户私钥不进行归档。

6.2.6 私钥导入或导出密码模块

沃通的私钥安全导入到密码模块中，并严格的按照沃通规定的程序和策略进行备份，除此之外的任何导入、导出操作均不被允许。当 CA 密钥对备份到另外的硬件密码模块上时，以加密的形式在模块之间传送，并且在传递前要进行身份鉴别，以防止 CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

沃通不提供订户私钥从硬件密码模块中导出的方法，也不允许如此操作。

6.2.7 私钥在密码模块的存储

沃通的私钥在国家密码主管部门批准和认可的密码设备及密码模块中存储。

订户证书的私钥在进行签名后即失效。

6.2.8 激活私钥的方法

沃通的私钥在国家密码主管部门批准和认可的密码设备及密码模块中，须由具备激活私钥权限的管理员使用含有自身身份的加密 IC 卡登录，启动密钥管理程序，进行激活私钥的操作。为确保安全，需有超过半数以上的管理员同时在场方可进行私钥激活。

针对存放在诸如订户 USB-Key、智能卡、加密卡、加密机或其他形式的硬件密码模块中的私钥，订户可通过口令、指纹、IC 卡等方式进一步加强保护。在订户计算机安装相应驱动后，将 USB-Key、智能卡等设备插入相应设备，输入保护口令或指纹，即可激活私钥。

6.2.9 解除私钥激活状态的方法

一旦私钥被激活，除非该状态被吊销，否则私钥将持续保持激活状态。在部分私钥应用场景中，私钥每次激活后仅允许执行一次操作，若需进行二次操作，须再次激活。

6.2.10 销毁密钥的方法

当沃通私钥已不再应用，或与之相对应的公钥已到期或被吊销时，加密设备须进行清空处理。同时，所有用于激活私钥的 PIN 码、IC 卡、动态令牌等载体亦须予以销毁或回收。私钥存档操作需遵循本文档规定进行。事件型证书订户私钥在执行一次签名后即行销毁。具有销毁密钥权限的管理员需利用含有自身身份的加密 IC 卡登录，启动密钥管理程序，执行销毁密钥操作，并要求半数以上管理员同时在场。

6.2.11 密码模块的评估

沃通使用国家密码主管部门批准和许可的密码产品，接受其颁布的各类标准、规范、评估结果、评价证书等各类要求。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

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

6.3.2 证书操作期和密钥对使用期限

事件型证书密钥对的有效期与证书有效期不同，私钥有效期为从签发证书到第一次使用该证书进行数字签名，公钥有效期一般与证书有效期一致。

6.4 激活数据

不适用。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

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

6.5.2 计算机安全评估

CA 系统建设应符合国家相关部门的管理规范与网络安全技术要求。

6.6 生命周期技术控制

6.6.1 系统开发控制

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

6.6.2 安全管理控制

沃通对系统的维护保证操作系统、网络设置和系统配置安全。通过日志检查来检查系统和数据完整性和硬件的正常操作。

6.6.3 生命周期的安全控制

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均通过了主管部门鉴定，使用了基于标准的强化安全通信协议确保了通信数据的安全，

在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。

6.7 网络的安全控制

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

6.8 时间戳

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

7. 证书、证书吊销列表和在线证书状态协议

7.1 证书

沃通签发的证书符合国家相关标准的要求，遵循 RFC5280 等技术标准。

7.1.1 版本号

X.509 V3。

7.1.2 算法对象标识符

符合国家密码主管部门批准的算法对象标识符。

7.1.3 名称形式

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

1) C (Country) 应为 CN ，表示中国；

2) O(Organization)应为证书主体或者签名行为业务场景所关联组织的上一级单位名称，或所在省、

自治区、直辖市名称全称。可选部分；

3) OU(Organization Unit)应为证书主体或者签名行为业务场景所关联组织的名称全称。可选部分；

4) CN(Common Name) 中的内容代表签名行为业务场景的相关信息，分两种：

a. 当订户是电子签名人时，CN 中的内容是订户的名称；

b. 当订户是申请对签名行为业务场景相关信息进行固化的实体时，CN 中的内容可以是实体名称，也可以是需要固化的签名行为相关信息。

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

7.1.4 证书扩展项

CA 证书扩展项除使用 IETF RFC 5280 中定义的证书扩展项，还支持私有扩展项。

CA 采用的 IETF RFC 5280 中定义的证书扩展项：

1) 颁发机构密钥标识符 Authority Key Identifier

2) 主体密钥标识符 Subject Key Identifier

3) 密钥用法 Key Usage（0 digitalSignature）

4) 序列号

5) CRL 发布点

事件型证书应配置以下扩展密钥用途：

1) 文件签署 (1.3.6.1.4.1.311.10.3.12)

2) Adobe PDF 签署 (1.2.840.113583.1.1.5)

事件型证书支持下列私有扩展项：

1) 签名扩展项，Signature Extension，应包含签名相关证据内容，如声音、图像等。

7.2 证书吊销列表

事件型证书不签发 CRL，所有订户证书私钥在签名后即销毁。

8. 电子认证服务机构审计和其他评估

8.1 评估的频率和情形

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

8.2 评估者的资质

内部审计人员由沃通内部人员组成，外部审计的审计人员的资质由第三方确定。

8.3 评估者与被评估者之间的关系

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

8.4 评估的内容

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

8.5 对问题与不足采取的措施

对审计中发现的问题，沃通将根据审计报告的内容准备一份解决方案，明确对此采取的行动。沃通将根据国际惯例和相关法律、法规迅速解决问题。

8.6 评估结果的传达与发布

除非法律明确要求，沃通一般不公开评估结果。

对 CA 关联方，沃通将依据签署的协议来公布评估结果。

9. 法律责任和其他业务条款

本章规定参见沃通发布的正式 CPS 文件。