农信银资金清算中心有限责任公司
电子认证业务规则

〈版本：V1.5〉

生效日期：2020 年 5 月 25 日

农信银资金清算中心有限责任公司

2020 年 5 月

文档版本控制表			
版本	修订说明	审核/批准人	生效日期
V1.0	正式发布	公司安全策略管理委员会	2018 年 3 月 12 日
V1.1	新增 5.1.3 电力与空调章节弱电系统相关信息	公司安全策略管理委员会	2018 年 9 月 26 日
V1.2	修改 6.5.2 计算机安全要求章节	公司安全策略管理委员会	2019 年 10 月 30 日
V1.3	新增 9.9 赔偿章节	公司安全策略管理委员会	2019 年 11 月 8 日
V1.4	修改 1.4.1 适合的证书应用章节 修改 2.3 信息库访问控制章节	公司安全策略管理委员会	2020 年 5 月 15 日
V1.5	修改 5.4.1 记录事件的类型章节 新增 5.4.2 处理或归档日志的周期章节 修改 5.4.5 审计日志备份程序章节 新增 9.7.2 对最终实体的赔偿担保章节	公司安全策略管理委员会	2020 年 5 月 25 日

目录

1. 概括性描述

1.1. 概述

农信银资金清算中心有限责任公司电子认证业务规则（以下简称《电子认证业务规则》）由农信银资金清算中心有限责任公司按照工业和信息化部《电子认证服务管理办法》的要求，依据《电子认证业务规则规范(试行)》制定，并报工业和信息化部备案。

《电子认证业务规则》详细阐述了农信银资金清算中心有限责任公司在实际工作和运行中所遵循的各项规范。《电子认证业务规则》适用于农信银资金清算中心有限责任公司及其员工、注册机构、证书申请人、订户和依赖方，各参与方必须完整地理解和执行《电子认证业务规则》所规定的条款，并承担相应的责任和义务。

1.2. 文档名称与标识

本文档名称是《农信银资金清算中心有限责任公司电子认证业务规则》。

1.3. 文档名称与标识

1.3.1. 电子认证服务机构

农信银资金清算中心有限责任公司是根据《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：CA 机构）。CA 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。

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、恢复和注销等业务的实体。

CA 机构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。

CA 机构授权外部机构作为注册机构，应与外部机构签署合同，在合同条款

中明确其为授权注册机构，并定义双方的权力与义务，以承担的法律责任。

1.3.3. 订户

订户是指向 CA 机构申请数字证书的实体。

1.3.4. 依赖方

依赖方是指信赖于证书所证明的基础信任关系并开展业务活动的实体。

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

CA 机构签发的数字证书适合应用在企业信息化和电子商务等领域，用于证明订户在电子化环境中所进行的身份认证和电子签名，以及数据加密等服务。

CA 机构的数字证书包含个人证书和机构证书，具体如下：

a. 个人证书

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

b. 机构证书

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

1.4.2. 限制的证书应用

本 CA 机构发放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

本《电子认证业务规则》的管理机构是农信银资金清算中心有限责任公司安全策略管理委员会。由安全策略管理委员会负责本《电子认证业务规则》的制订、发布、更新等事宜。

1.5.2. 联系方式

邮寄地址：北京市丰台区汉威国际广场 2 区 4 号楼 3 层
邮政编码：100071
电话：4008685678
网址：http://www.nongxinyin.com/

1.5.3. 决定 CPS 符合策略的机构

《电子认证业务规则》由农信银资金清算中心有限责任公司安全策略管理委员会组织制定，报农信银资金清算中心有限责任公司安全策略管理委员会批准实行。

1.5.4. CPS 批准程序

《电子认证业务规则》由农信银资金清算中心有限责任公司安全策略管理委员会组织 CPS 编写小组。编写小组完成编写 CPS 草案后，由农信银资金清算中心有限责任公司安全策略管理委员会组织对 CPS 草案进行初步评审。初步评审后，将 CPS 评审稿提交农信银资金清算中心有限责任公司安全策略管理委员会审批。经农信银资金清算中心有限责任公司安全策略管理委员会审批通过后，在农信银资金清算中心有限责任公司的网站上对外公布。

1.6. 定义和缩写

下列定义适用于本《电子认证业务规则》：
a) 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。

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

关于电子认证服务机构在证书签发、证书更新(或密钥更新)、证书吊销或证书管理过程中所采纳的业务实践的声明。

c) 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。

d) 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，在某些环境下主动撤销或挂起证书，处理订户撤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）。

e) 数字证书(证书) Digital Certificate

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

f) 证书撤销列表 (CRL) Certificate Revocation List

一个经电子认证服务机构数字签名的列表，它指定了一系列证书颁发者认为无效的证书，也称黑名单服务。

g) CA 注销列表(ARL) Certificate Authority Revocation List

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

h) 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。

i) 公钥 Public Key

非对称密码算法中可以公开的密钥。

j）身份标识（ID）Identity

应用中的身份标识号码，也称为序列号或帐号，是某个应用中相对唯一的编码，在应用中相当于是一种“身份标识”，身份标识号一般是不变的，至于用什么来标识该“身份标识”，则由应用业务部门自己制定的规则来确定。

2. 信息发布与信息管理

2.1. 认证信息的发布

农信银资金清算中心有限责任公司通过网站公布以下信息：《电子认证业务规则》修订以及其他由农信银资金清算中心有限责任公司不定时发出的信息。农信银资金清算中心有限责任公司网站网址：http://www.nongxinyin.com。

《电子认证业务规则》发布在农信银资金清算中心有限责任公司的网站上，供相关方下载、查阅。

2.2. 发布时间或频率

CA 机构的 CPS 按照 1.5.4 所述的批准流程，一经发布到农信银资金清算中心有限责任公司的网站即时生效。

2.3. 信息库访问控制

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

3. 身份标识与鉴别

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

订户的甄别名(DN)必须具有一定的代表意义。

个人证书的甄别名通常可包含个人的真实名称或者证件号码，作为标识订户

的关键信息被认证。

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

3.1.3. 订户的匿名或伪名

在 CA 证书服务体系中，除在特定场景下的标识证书以外，原则上订户不使用匿名或伪名。

3.1.4. 理解不同名称形式的规则

DN 的具体内容依次由 CN、OU、O、C 四部分组成。其中 CN 用来表示用户名，OU、O 用来表示组织单位名称、C 用来表示国家。

3.1.5. 名称的唯一性

在 CA 的证书服务体系中，证书主体名称必须是唯一的。但对于同一订户，可以用其主体名为其签发多张证书，但证书的扩展项不同。

3.1.6. 商标的承认、鉴别和角色

CA 机构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

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

3.2.2. 个人身份的鉴别

个人身份的鉴别可以使用有效的身份证件，包括但不限于：身份证、港澳台居民身份证、户口簿、护照、军官证等。

成员机构需要对个人身份鉴别完成后将有效的信息提供给 CA 机构，CA 机构对电子材料真实性进行审核，审核通过后进行批准申请或拒绝申请的操作。

审核批准后，CA 机构或注册机构按照相关法律法规的要求妥善保存订户申请材料。

本 CPS 简要说明了如何进行个人身份鉴别。农信银资金清算中心有限责任公司保留根据最新国家政策法规的要求更新个人身份鉴别方法与流程的权利。

3.2.3. 组织身份的鉴别

对于组织身份的鉴别， 成员机构需要首先验证组织的合法证件。CA 机构对电子材料真实性进行审核，审核通过后进行批准申请或拒绝申请的操作。

审核批准后，CA 机构或注册机构按照相关法律法规的要求妥善保存订户申请材料。

本 CPS 简要说明了如何进行组织身份鉴别。农信银资金清算中心有限责任公司保留根据最新国家政策法规的要求更新组织身份鉴别方法与流程的权利。

3.2.4. 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，属于没有验证的订户信息。

3.2.5. 授权确认

个人在 CA 机构的数字证书申请表上写明代办人的身份信息并签名确认后，则证明本人对代办人的授权确认。

代表组织获取数字证书，需要出具组织授权其该组织为办理 CA 数字证书事宜的授权文件。组织在 CA 机构的数字证书申请表上加盖单位公章后，则证明本组织对办理人的授权确认。

3.2.6. 互操作准则

CA 机构将根据业务需要，在遵循本《电子认证业务规则》的各项控制要求的基础上，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与证关系。但交叉认证并不表示本 CA 机构批准了或赋予了其他 CA 中心或电子认证服务机构的权力。

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

数字证书的常规密钥更新中，通过订户使用当前有效私钥对包含新公钥的密钥更新请求进行签名，CA 机构使用订户原有公钥验证确认签名来进行订户身份标识和鉴别。

3.3.2. 吊销后密钥更新的标识与鉴别

数字证书吊销后的密钥更新等同于订户重新申请证书，其要求与 3.2 相同。

3.3.3. 证书变更的标识与鉴别

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

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

3.4. 吊销请求的标识与鉴别

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

如果是因为订户没有履行《证书策略》和本《电子认证业务规则》所规定的义务，由 CA 机构或授权的注册机构申请吊销订户的证书时，不需要对订户身份进行标识和鉴别。

4. 证书生命周期操作要求

4.1. 证书申请

4.1.1. 证书申请实体

证书申请实体包括个人和具有独立法人资格的组织机构(包括事业单位、企

业单位、社会团体和人民团体等)。

4.1.2. 申请过程与责任

证书申请人按照本《电子认证服务规则》所规定的要求，通过现场面对面或在线方式提交证书申请，包括相关的身份证明材料。CA 机构或注册机构应明确告知证书用户所需承担的相关责任和义务，证书申请人表达申请证书的意愿后，CA 机构或注册机构依据身份鉴别规范对证书申请人的身份进行鉴别，并决定是否受理申请。

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 CA 机构或授权的注册机构完成对身份信息的采集、记录和审核。

CA 机构：CA 机构参照 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，CA 机构向订户签发证书。如果用户身份信息的鉴别由授权的注册机构完成，CA 机构应对授权的注册机构进行监督管理和审计。

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

对于标识证书，授权的注册机构或应用业务部门应明确申明其所申请标识证书的目的及使用范围，负责订户身份鉴证，将应用关联信息（包括应用 ID 编码、应用随机编码或其杂凑值等）进行数字签名后通过安全通道发送至 CA 机构，CA 机构校验注册机构的数字签名，记录应用关联信息后，CA 机构负责签发标识证书。

根据《中华人民共和国电子签名法》的规定，证书申请人未向 CA 机构提供真实、完整和准确的信息，或者有其他过错，给 CA 机构或电子签名依赖方造成损失的，应承担相应的法律责任和经济赔偿。

4.2. 证书申请处理

4.2.1. 执行识别与鉴别功能

CA 机构或授权的注册机构按照本《电子认证业务规则》所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见 3.2 初始身份确认。

4.2.2. 证书申请批准和拒绝

CA 机构或授权的注册机构根据本《电子认证业务规则》所规定的身份鉴别流程对证书申请人身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

如果证书申请人通过本《电子认证业务规则》所规定的身份鉴别流程且鉴证结果为合格，CA 机构或授权的注册机构将批准证书申请，为证书申请人制作并颁发数字证书。

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

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

在必要时 CA 机构有权复核注册机构提交的订户申请材料，并有权拒绝不符合本 CPS 的高风险申请。

4.2.3. 处理证书申请的时间

CA 机构或授权的注册机构将做出合理努力来尽快确认证书申请信息，一旦注册机构收到了所有必须的相关信息，将在 1 个工作日内处理证书申请。

CA 机构或授权的注册机构能否在上述时间期限内处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了 CA 的管理要求。

4.3. 证书签发

4.3.1. 证书签发过程中电子认证服务机构的行为

CA 机构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

CA 机构通过注册机构对数字证书订户的通告有以下几种方式：

a) 通过面对面的方式，通知订户到注册机构领取数字证书；注册机构把密码信封和证书等直接提交给订户，来通知订户证书信息已经正确生成；

b）邮政信函或电子邮件通知订户；

c）CA 机构认为其他安全可行的方式通知订户。

对于标识证书，授权的注册机构或应用业务部门负责对标识证书订户的通告。

4.4. 证书接受

4.4.1. 构成接受证书的行为

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

对于标识证书，当订户通过授权的注册机构或应用业务部门的身份鉴证后，获得 CA 机构签发的标识证书即视为订户已经接受该标识证书。

4.4.2. 电子认证服务机构对证书的发布

CA 机构在签发完数字证书后，就将证书发布到数据库和目录服务器中。CA 机构采用主、从目录服务器结构来分布所签发证书。签发完成的数据直接写入主目录服务器中，然后通过主从映射，将主目录服务器的数据自动发布到从目录服务器中，供订户和依赖方查询和下载。

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

CA 机构不对其他实体进行通告，其他实体可以在信息库上自行查询。

4.5. 密钥对和证书的使用

4.5.1. 订户私钥和证书的使用

订户在提交了证书申请并接受了 CA 机构所签发的证书后，均视为已经同意遵守与 CA 机构、依赖方有关的权利和义务的条款。

数字证书订户接受到数字证书，应妥善保存其证书对应的私钥。订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了相关证书之后才能使用对应的私钥，并且在证书到期或被吊销之后，订户必须停止使用该证书对应的私钥。

4.5.2. 依赖方对公钥和证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了解对方的身份，并通过公钥验证对方电子签名的真实性。验证证书的有效性包括：

a）用 CA 机构的证书验证证书中的签名，确认该证书是 CA 机构签发的，并且证书的内容没有被篡改。

b）检验证书的有效期，确认该证书在有效期之内。

c）检验数字证书有效性，需要检查该证书没有被注销。

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示签名过的数据。

4.6. 证书更新

4.6.1. 证书更新的情形

证书更新指在不改变证书中订户的公钥或其他任何信息的情况下，为订户签发一张新证书，证书更新由用户自行决定采用证书更新或证书密钥更新。

证书上都有明确的证书有效期，表明该证书的起始日期与截至日期。订户应当在证书有效期到期前，到 CA 机构或授权的注册机构申请更新证书。

4.6.2. 颁发新证书对订户的通告

同 4.3.2

4.6.3. 构成接受密钥更新证书的行为

同 4.4.1

4.6.4. 电子认证服务机构对更新证书的发布

同 4.4.2

4.6.5. 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3

4.7. 证书密钥更新

4.7.1. 证书密钥更新的情形

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书，CA 机构提供证书更新时，密钥必须同时更新。证书更新的具体情形如下：

a) 当订户证书即将到期或已经到期时；
b) 当订户证书密钥遭到损坏时；
c) 当订户证实或怀疑其证书密钥不安全时；
d) 其它可能导致密钥更新的情形。

4.7.2. 请求证书密钥更新的实体

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

4.7.3. 证书密钥更新请求的处理

同 3.3

4.7.4. 颁发新证书对订户的通告

同 4.3.2

4.7.5. 构成接受密钥更新证书的行为

同 4.4.1

4.7.6. 电子认证服务机构对密钥更新证书的发布

同 4.4.2

4.7.7. 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3

4.8. 证书变更

4.8.1. 证书变更的情形

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

4.8.2. 请求证书变更的实体

订户可以请求证书变更。订户包括持有 CA 机构签发的个人、组织及设备等各类证书的证书持有人。

4.8.3. 证书变更请求的处理

同 3.3.3

4.8.4. 颁发新证书对订户的通告

同 4.3.2

4.8.5. 构成接受密钥更新证书的行为

同 4.4.1

4.8.6. 电子认证服务机构对变更证书的发布

同 4.4.2

4.8.7. 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3

4.9. 证书吊销和挂起

4.9.1. 证书吊销的情形

a) 发生下列情形之一的，订户应当申请吊销数字证书：
1) 数字证书私钥泄露；
2) 数字证书中的信息发生重大变更；
3) 认为本人不能实际履行数字证书认证业务规则。
b) 发生下列情形之一的，CA 机构可以吊销其签发的数字证书：
1) 订户申请吊销数字证书；
2) 订户提供的信息不真实；
3) 订户没有履行双方合同规定的义务，或违反本 CPS
4) 数字证书的安全性得不到保证；
5) 法律、行政法规规定的其他情形。

4.9.2. 请求证书吊销的实体

根据不同的情况，订户、CA 机构、注册机构可以请求吊销最终用户证书。

4.9.3. 吊销请求的流程

证书吊销请求的处理采用与初始证书签发相同的过程。

a) 数字证书吊销的申请人到 CA 机构或授权的注册机构书面填写《证书吊销申请表》，并注明吊销原因；

b) CA 机构或授权的注册机构根据 3.2 的要求对订户提交的吊销请求进行

审核；

c) CA 机构吊销订户证书后，注册机构将当面通知订户证书被吊销，订户证书在 24 小时内进入 CRL；

d) 强制吊销是指当 CA 机构或 CA 授权的注册机构确认用户违反本《电子认证业务规则》的情况发生时，对订户证书进行强制吊销，吊销后将立即通知该订户。

4.9.4. 吊销请求宽限期

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

4.9.5. 电子认证服务机构处理吊销请求的时限

注册机构接到吊销请求后立即处理，24 小时生效。CA 机构每日签发一次 CRL,CRL 发布到目录服务器指定的位置，供请求者查询下载。

CRL 的结构如下：

a) 版本号(version)

b) 签名算法标识符(signature)

c) 颁发者名称(insure)

d) 本次更新(this update)

e) 下次更新(next update)

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

g) 签名算法(signature algorithm)

h) 签名(signature value)

4.9.6. 依赖方检查证书吊销的要求

在具体应用中，依赖方必须使用以下两种功能之一进行所依赖证书的状态查询：

a) CRL 查询：利用证书中标识的 CRL 地址，通过目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的检验。

b) 在线证书状态查询(OCSP)：服务系统接受证书状态查询请求，从目录服务器中查询证书的状态，查询结果经过签名后，返回给请求者。

注意：依赖方要验证 CRL 的可靠性和完整性，确保是经 CA 机构发布并且签名的。

4.9.7. CRL 的颁发频率

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

4.9.8. CRL 发布的最长滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.10. 证书状态服务

4.10.1. 操作特点

证书状态可以通过 CA 机构提供的 OCSP 服务获得。CA 机构将该证书信息记录在指定的数据库中，订户终端会对证书状态实时检测。根据与依赖方约定，可向依赖方提供状态查询服务。

4.10.2. 服务可用性

提供 7*24 小时的证书状态查询服务。

4.10.3. 可选特征

根据请求者的要求，在请求者支付相关费用后，CA 机构可以提供以下通知服务：

a) 收到证书主题的电子签名消息的接受者要求，确认该证书是否已被吊销；

b) 提供通知服务，当指定的证书被吊销时，CA 机构将通知请求该项服务的请求者。

4.11. 订购结束

订购结束是指当证书有效期满或证书吊销后，该证书的服务时间结束。

订购结束包含以下两种情况：

a) 证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订户可以终止订购；

b) 在证书有效期内，证书被吊销后，即订购结束。

4.12. 密钥生成、备份与恢复

4.12.1. 密钥生成、备份与恢复的策略和行为

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

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

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

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

具体策略在 6.1 和 6.2 中详细描述。

4.12.2. 会话密钥的封装与恢复的策略和行为

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

5. 电子认证服务机构设施、管理和操作控制

5.1. 物理控制

5.1.1. 场地位置与建筑

农信银资金清算中心有限责任公司北京数据中心机房属于租赁机房，出租方位中国金融电子化公司，承担外包服务的机房为 1、2、3、4 号机房。机房总面

积约为750平米，位于北京市宣武区右内大街新安南里甲一号院内主楼。其中2号机房为CA机房，楼层高度为3.3米，楼板承重800公斤/平方米，机房面积约100平米。2号机房内设两个屏蔽机房，采用焊接式屏蔽壳体，配置电动（手动）锁紧双功能屏蔽门、波导窗、波导管滤波器等屏蔽设备，设计、施工满足国家保密局BMB3-1999屏蔽机房屏蔽效能C级指标要求。

机房整体设计、建设依照《电子信息系统机房设计规范》（GB50174-2008）中“A”级机房标准执行，并遵从可靠性、先进性、可扩充性、安全性、环保性和经济性的原则。

5.1.2. 物理访问

为了保证本系统的安全，采取了一定的隔离、控制、监控手段。机房的所有门都足够结实，能防止非法的进入。机房通过设置门禁和侵入报警系统来重点保护机房物理安全。

物理访问控制包括如下几个方面：

a) 门禁系统：控制各层门的进出。工作人员需使用身份识别卡结合生物特征认证才能进出，进出每一道门应有时间纪录和信息提示。

b) 报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况都应触发报警系统。报警系统明确指出报警位置。

c) 监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对安全区域和操作区域进行 24 小时不间断录像。所有录像资料需要保留不少于6个月，以备查询。

5.1.3. 电力与空调

机房供电按照一级负荷要求，供电采用10KV双路市电接入，单路额定容量5000KVA，并配有两台2400KW低压柴油发电机组用于应急。机房供配电方式采用交流50Hz，380V/220V，接地采用TN-S方式。1、2号机房共用400KVA UPS系统，采用2N双系统冗余结构为机房IT设备提供双路电源保障，各系统UPS后备电池后备时间不少于15分钟。

2 号机房配置风冷式精密行间空调，送风方式为水平前送风后回风方式，空调本身具有加湿和除湿功能；另每个机房区配置 2 台 5P/3P 高性能工业专用柜机空调作为冗余。机房内配置有新风机，用于室内空气流通，维持室内正压；同时机房内设置排烟风机，用于机房区气体灭火系统的废气排放。

机房动力系统采用双路末端互投的供电方式为机房空调、照明等设施提供电源保障。机房照明不小于 500LX/平米，应急照明不小于 300LX/平米，安装适量维修插座。

弱电系统考虑技术先进、易于使用、安全可靠、扩展性强、兼容性强的产品。采用星型结构化布线方式，走线方式采用上走热镀锌网格式桥架方式，机房内铜缆采用非屏蔽线缆，光缆采用万兆多模光纤。

5.1.4. 水患防治

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

CA 机房的系统有充分保障，能够防止水侵蚀。

目前机房内无上下水系统，空调间做了严格防水处理，由漏水检测系统提供（7*24）实时检测。

5.1.5. 火灾预防和保护

火灾预防：

a) CA 机房设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位设置烟、温感探测器。

b) 敏感区及高敏区配置独立的气体灭火装置，使用七氟丙烷（HFC-227ea）等洁净气体灭火系统，备有相应的气体灭火器，非敏感区根据实际情况可配置水喷淋灭火装置。CA 机房内除对纸介质等易燃物质进行灭火外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂。

c) 火灾自动报警、自动灭火系统避开可能招致电磁干扰的区域或设备，同时配套设置消防控制室。还设有不间断的专用消防电源和直流备用电源，并具有自动和手动两种触发装置。

d) 火灾自动灭火设施的区域内，其隔墙和门的耐火极限不低于 1 小时，吊顶的耐火极限不得低于 15 分钟。

e) 在非敏感区及敏感区的办公区域内，须设置紧急出口，紧急出口必须设有消防门，消防门符合安全要求。紧急出口门外部不能有门开启的装置，且紧急出口门须与门禁报警设备联动外，需装配独立的报警设备。

f) 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。 机 CA 房采取适当的管理手段来保障非紧急避险状态下，紧急出口门不能被内部人员任意打开。

灭火系统采用电动，手动，紧急启动三种方式：

a) 电动方式：防护区报警系统第一次火警确认后，发出声光警示信号，切断非消防电源（如：空调电源、照明电源等）。并送排风（烟），防火阀关闭。第二次火警确认后，经延时，同时发出气体释放信号，并发出启动电信号，送给对应的管网启动钢瓶，喷气灭火。

b) 手动方式：人员对钢瓶或药剂瓶直接开启操作。

c) 紧急启动：防护区外设有紧急启动按钮供紧急时使用。

CA 机房通过与专业防火部门协调，实施消防灭火等应急响应措施。

5.1.6. 介质存储

CA 机房的存储介质包括硬盘、软盘、磁带、光盘等，介质存储地点和 CA 机房系统分开并且保证物理安全，注意防磁、防静电干扰、防火、防水，由专人管理。

5.1.7. 废物处理

当 CA 机房存档的敏感数据或密钥已不再需要或存档的期限已满时，应当将这些数据进行销毁。写在纸张之上的，必须切碎或烧毁。如果保存在磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。

5.2. 程序控制

5.2.1. 可信角色

电子认证服务机构、注册机构、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。

可信角色包括：

a) 系统管理员

系统管理员负责对数字证书服务体系在本单位的系统进行日常管理，执行系统的日常监控，并可根据需要签发服务器证书和下级操作员证书。

b) 安全管理员

安全管理员对 CA 中心的物理、网络、系统的安全全面负责。并且拟订安全管理制度和操作流程，监督各岗位安全管理的执行情况。

c) 审计管理员

审计管理员控制、管理、使用安全审计系统，安全审计系统分布于证书管理系统的各个子系统中，负责各个子系统的运行和操作日志记录。

d) 密钥管理员

密钥管理员负责管理 CA 中心的密钥相关设备，进行 CA 中心密钥的生成、备份、恢复、销毁等操作。

5.2.2. 每个角色和识别与鉴别

所有 CA 机构的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和生物特征认证技术；进入系统需要使用数字证书进行身份鉴别。CA 机构将独立完整地记录其所有的操作行为。

5.2.3. 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，即 CA 机构的可信角色由不同的人担任。

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

5.3. 人员控制

5.3.1. 资格、经历和无过失要求

所有的员工与农信银资金清算中心有限责任公司签定保密协议。对于充当可信角色或其他重要角色的人员，必须具备的一定的资格，具体要求在人事管理制度中规定。CA 机构要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响 CA 机构运行的其它兼职工作、无同行业重大错误记录、无违

法记录等。

5.3.2. 背景审查程序

CA 机构与有关的政府部门和调查机构合作，完成对 CA 机构可信任员工的背景调查。

所有目前的可信任员工和申请调入的可信任员工都必须书面同意对其进行背景调查。

背景调查分为：基本调查和全面调查。

基本调查包括对工作经历，职业推荐，教育，社会关系方面的调查。

全面调查除包含基本调查项目外还包括对犯罪记录，社会关系和社会安全方面的调查。

调查程序包括：

a) 人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

b) 人事部门通过电话、信函、网络、走访、等形式对其提供的材料的真实性进行鉴定。

c) 用人部门通过现场考核、日常观察、情景考验等方式对其考察。

d) 经考核，人事部门和用人部门联合填写《干部任免审批表》，报主管领导批准后准予上岗。

5.3.3. 培训与考核要求

CA 机构对运营人员按照其岗位和角色安排不同的培训。培训有：系统硬件安装与维护、系统软件运行与维护、系统安全、应用软件的运行和维护、CA 中心的运行管理、CA 中心的内部管理、政策和规定及系统备份与恢复等。

对于运营人员，其 CA 的相关知识与技能，每年至少要总结一次并由 CA 机构组织培训与考核。技术的进步、系统功能更新或新系统的加入，都需要对相关人员进行培训并考核。

5.3.4. 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受 CA 机构组织的培训一次。

认证策略调整、系统更新时，应对全体人员进行再培训，以适应新的变化。

5.3.5. 工作轮换周期和顺序

对于可替换角色，CA 机构将根据业务的安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。

5.3.6. 对未授权行为的处罚

当 CA 机构员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用 CA 系统或进行越权操作，CA 机构得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

5.3.7. 独立合约人的要求

对不属于 CA 机构内部的工作人员，但从事 CA 有关业务的人员等独立签约者(如注册机构的工作人员)，CA 机构的统一要求如下：

a) 正规劳务公司派遣人员；

b) 具有相关业务的工作经验；

c) 必须接受 CA 组织的岗前培训。

5.4. 审计日志程序

5.4.1. 记录事件的类型

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

审计范围包括人员、物理安全、通信安全、操作安全、系统安全。

5.4.2. 处理或归档日志的周期

CA 机构建有 CA 应用系统的日志收集分析系统，实时收集应用日志并归档保存。

每年对 RA 和 CA 进行全面审计；每月对 RA 和 CA 进行操作审计。

审计工作完成后审计员将审计报告递交至 CA 档案管理员，档案管理员定期将 CA 资料递交至中心档案室归档留存。

5.4.3. 审计日志的保存期限

CA 系统审计日志至少保存到证书失效后五年。

5.4.4. 审计日志的保护

CA 机构授权的人员才能对审查日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作。审计日志的制作和访问进行岗位分离。

5.4.5. 审计日志备份程序

CA 系统审计日志备份采用数据库自身备份程序，根据记录的性质和要求，按照每日、每月等策略进行备份。

5.4.6. 审计日志收集系统

审计日志收集系统涉及：

a)证书注册系统；

b)证书签发系统；

c)证书受理系统；

d)网站和数据库系统；

e)其他需要审计的系统。

CA 机构使用审计工具满足对上述系统审计的各项要求。

5.4.7. 对导致事件实体的通告

CA 机构发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，CA 机构保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

CA 机构有权决定是否对导致事件的实体进行通告。

5.4.8. 脆弱性评估

CA 机构每年对系统进行漏洞扫描和渗透测试等脆弱性评估，以降低系统运行的风险。

5.5. 记录归档

5.5.1. 归档记录的类型

归档记录包括所有审计数据、证书申请信息、与证书申请相关的信息等。

5.5.2. 归档记录的保存期

所有归档记录的保存期为证书失效后五年。

5.5.3. 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能查询。CA 机构保护相关的档案内容，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏。

5.5.4. 归档文件的备份程序

所有存档的文件和数据保存在 CA 机房的存储库。存档的数据一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。CA 机构在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5. 记录时间戳要求

所有记录都要在存档时加具体准确的时间标识以表明存档时间。系统产生的记录，用标准时间加盖时间戳。

5.5.6. 获得和检验归档信息的程序

由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，需要对这两个拷贝进行比较。CA 机构每年会验证归档信息的完整性。

5.6. 电子认证服务机构密钥更替

电子认证服务机构密钥更替指 CA 根证书到期和电子认证服务机构证书到期时，需要更换密钥而采取的措施。

a) CA 根密钥由加密机产生，有效期为 30 年，更替办法为：

使用旧的私钥对新的公钥及信息签名生成证书；

使用新的私钥对旧的公钥及信息签名生成证书；

使用新的私钥对新的公钥及信息签名生成证书。

通过以上 3 张证书达到密钥更换的目的，使新旧证书之间互相信任。

b) 电子认证服务机构证书到期之前，CA 机构将采取以下方式更替：

CA 机构将在 CA 证书到期前的 60 天内停止签发新的下级证书“停止签发（日期”）；

产生新的密钥对，签发新的 CA 证书；

在“停止签发日期”之后，CA 机构将采用新的 CA 密钥签发下级证书。

密钥更替时直接把当前 CA 证书吊销，签发到 ARL 并发布，然后签发一个新的 CA 证书，通过证书库和 LDAP 方式下发给证书应用系统。

c) CA 机构将继续使用旧的私有密钥签发的 CRL 后证书到期为止。

5.7. 损害和灾难恢复

5.7.1. 事故和损害处理程序

发生故障时，CA 机构将按照灾难恢复计划实施恢复。

5.7.2. 计算资源、软件和/或数据被破坏

CA 机构遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，CA 机构将按照灾难恢复计划实施恢复。

5.7.3. 实体私钥损害处理程序

当 CA 根证书被作废时，CA 机构通知订户。

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

5.7.4. 灾难后的业务连续性能力

针对证书系统的核心业务系统，证书签发系统和证书接口系统采用双机热备方式；对核心数据库，证书管理系统数据库采用磁盘阵列方式来确保证书系统的高可靠性和可用性。

发生自然或其它不可抗力性灾难后，CA 机构可采用远程热备站点对运营进行恢复。具体的安全措施按照 CA 灾难恢复计划实施。

5.8. 电子认证服务机构或注册机构的终止

因各种情况，CA 机构需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

CA 机构在终止服务九十日前，就业务承接及其他有关事项通知有关各方，包括但不限于 CA 授权的注册机构和订户等。

在终止服务六十日前向工业和信息化部报告，按照相关法律规定的步骤进行操作。

CA 机构采用以下措施终止业务：

a) 起草 CA 终止业务声明；

b) 停止认证中心所有业务；

c) 处理加密密钥；

d) 处理和存档敏感文件；

e) 清除主机硬件；

f) 管理 CA 系统管理员和安全官员；

g) 通知与 CA 终止运营相关的实体。

根据 CA 机构与注册机构签订的运营协议终止注册机构的业务。

6. 认证系统技术安全控制

6.1. 密钥对的生成和安装

6.1.1. 密钥对的生成

CA 签名密钥生成的安全性通过管理手段和技术手段两方面保证。管理上，需要制定严格的密钥管理流程对其进行控制，至少包括电磁屏蔽机房、人员监督、密钥分割、视频监控等；技术上，密钥的生成、管理、储存、备份和恢复等应遵循国家的相关技术标准，并在通过国家密码主管部门认可的加密设备中进行。

通常订户的密钥对有两对，一对用于签名和验证签名，另一对用于信息的加密和解密，其中用于加密、解密的密钥对由密钥管理中心生成。用于签名和验证的密钥对由订户使用国家密码主管部门批准的密码设备（如智能 USB KEY）生成。服务器证书可以由订户利用服务器提供的密钥生成功能生成密钥对，无论何种方式产生的密钥对，相关责任方必须通过技术以及管理手段保证密钥的安全性。订户同样有责任保护密钥的安全性，并承担由此带来的法律责任。

6.1.2. 私钥传送给订户

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

6.1.3. 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到 CA；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

依赖方可以从农信银资金清算中心有限责任公司的网站(http://www.nongxinyin.com)下载根证书和 CA 证书，从而得到 CA 的公钥。

6.1.5. 密钥的长度

密钥算法和长度符合国家密码主管部门的规定。

6.1.6. 公钥参数的生成和质量检查

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

6.1.7. 密钥使用目的

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

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

6.2. 私钥保护和密码模块工程控制

6.2.1. 密码模块标准和控制

采用符合国家密码管理部门要求的硬件密码模块来产生、管理、保存密钥，并按照国家密码管理的相关要求执行密码模块生命周期的管理和控制，实现私钥的保护。

订户使用国家密码管理部门批准的密码模块，并有责任妥善保护、保管其密码模块，防止其失窃、丢失、损坏及其授权使用。

6.2.2. 私钥的多人控制

采用多人控制 m of n(m=3，n=2)实现 CA 私钥的生成、更新、吊销、备份和恢复等操作。并保证至少其中多数人同时在场，管理员身份鉴别后才能实现上述操作。

6.2.3. 私钥托管

订户加密证书对应的私钥由密钥管理中心托管，订户的签名证书对应的私钥

由自己保管，密钥管理中心不负责托管。

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

6.2.4. 私钥备份

CA 机构和密钥管理中心不备份订户的签名密钥。

加密私钥由密钥管理中心备份，备份数据以密文形式存在。

6.2.5. 私钥归档

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

6.2.6. 私钥导入或导出密码模块

严格依照私钥保护程序和策略对私钥进行备份，私钥的备份用于密钥恢复和灾难恢复的目的，除此之外的任何导入导出操作将不被允许。CA 私钥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。

订户私钥无法从硬件导出。必须通过密码验证之后，才可以使用存储在密码模块中的私钥进行加解密操作。

6.2.7. 私钥在密码模块中的存储

私钥在硬件密码模块中加密保存。

6.2.8. 激活私钥的方法

订户私钥存储于证书载体中，只有通过口令验证后才能被激活使用。

服务器证书，如私钥由服务产生和保存，用户必须设置私钥激活口令，当服务启动软件加密模块被加载后，输入口令私钥被激活。

CA 私钥存放在硬件密码模块中，其激活数据已按照秘密分割要求进行分割，并采用 m of n 的机制对其访问加以控制，具有激活私钥权限的管理员输入口令后登陆，启动密钥管理程序激活私钥。

6.2.9. 解除私钥激活状态的方法

对个人和机构证书，在私钥退出登录状态、移除密码设备、或关闭计算机时，私钥激活状态解除。

服务器证书在服务程序关闭、操作系统注销或关闭时解除私钥激活状态。

CA 私钥在其密码设备关闭的时候解除激活状态，或者具有激活私钥权限的管理员通过密钥管理程序，终止激活私钥的操作。

6.2.10. 销毁密钥的方法

在 CA 私钥不再被使用且超过归档保存期限后，CA 私钥连同其备份进行销毁。销毁过程需要多个可信人员参与，CA 必须采用合适的方法以确保没有导致密钥重建的密钥残留，例如，采取硬件加密模块的归零、物理销毁加密设备和其他相应的方法确保 CA 私钥被完全销毁。一旦执行，CA 的密钥销毁动作将被记录。

订户加密私钥由 KMC 负责生成、保存、归档及销毁，具体执行方法遵循国家相关法律要求。建议订户在私钥生成周期结束后的一段时间内妥善保存私钥，以便解密信息，订户承担私钥的保护责任。如果订户私钥无需继续保存可以通过私钥删除或密码设备格式化的方法销毁私钥。

6.2.11. 密码模块的评估

CA 机构使用具有国家密码主管部门颁发商用密码型号证书的服务器密码机，符合国家有关标准。密码机采用以分组密码体制为核心的高强度密码算法和非对称密码体制，密钥采取分层结构，逐层提供保护。主要技术指标如下：

a) 通信接口：符合国际 ITU Ethernet RJ45 标准；

b) 带宽控制：10M/100M/1000M 自适应，充分满足突发业务需要；

c) 并发容量：可支持同时并发 100 个的独立安全处理容量；

d) 密钥管理：密钥不以明文形式出现在服务器密码机以外；通信密钥通过身份鉴别后协调得到；

e) 身份鉴别：通过口令对用户进行身份鉴别管理，以控制对加密系统的使用；

f) 处理速度：数据加解密处理能力大于 100Mbps。

6.3. 密钥对管理的其他方面

6.3.1. 公钥归档

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

6.3.2. 证书操作期和密钥对使用期限

通常签名证书的密钥对使用期限与证书有效期一致，签名私钥只能在证书有效期内才可以用于签名。对于加密证书，加密私钥的有效期可以长于证书有效期，以保证在证书有效期内加密的信息可以被解密。

无论是订户证书还是 CA 证书，有效期满后，允许使用原密钥对对证书进行更新。但是密钥对不能无限期使用。

6.4. 激活数据

6.4.1. 激活数据的产生和安装

激活数据是私钥保护密码，数字证书存储介质（如：智能 USB KEY）出厂时设置了缺省的 PIN 值，证书制作时将此 PIN 值更改为密码信封中的密码，从而激活了证书存储介质的 PIN。

6.4.2. 激活数据的保护

CA 私钥的激活数据按照 m of n 机制被分割，并由多名可信人员分别保管，这些拥有私钥激活数据的可信人员必须遵守职责分离及安全操作等要求。

订户私钥激活数据由订户自行妥善保管，不可被他人获得。为了保证私钥使用安全，应定期修改私钥的激活数据。如果发生激活数据丢失而造成私钥被盗用，将视同订户本人使用私钥进行的操作。

6.4.3. 激活数据的其他方面

考虑到安全因素，对于订户激活数据的生命周期，规定如下：

1、订定用于申请、下载证书的口令，下载成功后失效。

2、用于保护私钥或者 USB KEY 的口令，建议订户根据业务应用的需要及时变更。

6.5. 计算机安全控制

6.5.1. 特别的计算机安全技术要求

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

对于设备有一套完整的保管和维护制度：

a) 专人负责设备的领取和保管，做好设备的领用、进出库和报废登记。

b) 对设备定期进行检查、清洁和保养维护。

c) 制定设备维修计划，建立满足正常运转最低要求的易损坏备件库。

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

e) 设备维修时，必须有派专人在场监督。

6.5.2. 计算机安全要求

CA 系统建设符合《GB/T22239-2019 信息系统安全等级保护基本要求》的第三级要求。

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

CA 机构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。CA 机构采取防火墙、病毒防治、入侵检测、漏洞扫描、数据备份、灾难恢复等安全防护措施。

6.8. 时间戳

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

7. 证书、证书吊销列表和在线证书状态协议

7.1. 证书

CA 签发的证书符合 X.509 V3 格式。遵循 RFC3280 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 UTF-8。

7.1.4. 证书扩展项

CA 证书扩展项除使用 IETF RFC 3280 中定义的证书扩展项，还支持私有扩展项。

CA 采用的 IETF RFC 3280 中定义的证书扩展项：

颁发机构密钥标识符 Authority Key Identifier

主体密钥标识符 Subject Key Identifier

密钥用法 Key Usage

扩展密钥用途 Extended Key Usage

私有密钥使用期 Private Key Usage Period

主体可选替换名称 Subject Alternative Name

基本限制 Basic Constraints

证书撤销列表分发点 CRL Distribution Points

私有扩展项可支持以下类型：

个人身份证号码 Identify Card Number

企业营业执照（统一社会信息代码）IC Registration Number

企业组织机构代码 Organization Code

企业税号 Taxation Number

7.2. 证书吊销列表

7.2.1. 版本号

CA 签发的证书吊销列表符合 X.509 V2 格式。遵循 RFC3280 标准。

7.2.2. CRL 和 CRL 条目扩展项

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

7.3. 在线证书状态协议

7.3.1. 版本号

使用 OCSP 版本 1。

7.3.2. OCSP 扩展项

不使用 OCSP 扩展项。

8. 电子认证服务机构审计和其他评估

8.1. 评估和频率或情形

审计是为了检查、确认 CA 机构是否按照《电子认证业务规则》及其业务规范、管理制度和安全策略开展业务，发现存在的可能风险。审计分内部审计和外部审计。

内部审计是由 CA 机构自己组织内部人员进行的审计，审计的结果可供 CA 机构改进、完善业务，内部审计结果不需要公开。

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

8.2. 评估者的资质

内部审计人员的选择一般包括：
CA 的安全负责人及安全管理人员；
CA 业务负责人；

认证系统及信息系统负责人；
人事负责人；
其他需要的人员。
外部审计的审计人员的资质由第三方确定。

8.3. 评估者与被评估者之间的关系

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

8.4. 评估内容

审计所涵盖的主题包括：
人事审查；
物理环境建设及安全运营管理规范审查；
系统结构及其运行审查；
密钥管理审查；
客户服务及证书处理流程审查。

8.5. 对问题与不足采取的措施

对审计中发现的问题，CA 机构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。机构将根据国际惯例和相关法律、CA 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，CA 机构一般不公开评估结果。
对 CA 关联方，CA 机构将依据签署的协议来公布评估结果。

9. 法律责任和其他业务条款

9.1. 费用

9.1.1. 证书签发和更新费用

数字证书的收费标准按照国家和北京市物价主管部门批准的收费标准执行。根据证书实际应用的需要，CA 机构在不高于收费标准的前提下可以对证书价格进行适当调整。

9.1.2. 证书查询费用

在证书有效期内，对该证书信息进行查询，CA 机构不收取查询费用。

9.1.3. 证书吊销或状态信息的查询费用

查询证书是否吊销，CA 机构不收取信息访问费用。

对于在线证书状态查询(OCSP)，由 CA 机构与依赖方或订户在协议中约定。

9.1.4. 其他服务的费用

CA 机构可根据请求者的要求，订制各类通知服务，具体服务费用，在与订制者签订的协议中约定。

9.1.5. 退款策略

在实施证书操作和签发证书的过程中，CA 机构遵守并保持严格的操作程序和策略。一旦订户接受数字证书，CA 机构将不办理退证、退款手续。

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

9.2. 财务责任

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

9.3. 业务信息保密

9.3.1. 保密信息范围

保密的业务信息包括但不限于以下方面：

a) 在双方披露时标明为保密(或有类似标记)的；

b) 在保密情况下由双方披露的或知悉的；

c) 双方根据合理的商业判断应理解为保密数据和信息的；

d) 以其他书面或有形形式确认为保密信息的；

e) 或从上述信息中衍生出的信息。

对于 CA 机构来说，保密信息包括但不限于以下方面：

a) 最终用户的私人签名密钥都是保密的；

b) 保存在审计记录中的信息；

c) 年度审计结果也同样视为保密；

d) 除非有法律要求，由 CA 机构掌握的，除作为证书、CRL、认证策略被清楚发布之外的个人和公司的信息需要保密。

CA 机构不保存任何证书应用系统的交易信息。除非法律明文规定， 机构没有义务公布或透露订户数字证书以外的信息。

9.3.2. 不属于保密的信息

与证书有关的申请流程、申请需要的手续、申请操作指南等信息是公开的。CA 机构在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。订户数字证书的相关信息可以通过 CA 机构目录服务等方式向外公布。

9.3.3. 保护保密信息的责任

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

b) 当 CA 机构在任何法律、法规或规章的要求下，或在法院的要求下必须提供本《电子认证业务规则》中具有保密性质的信息时，CA 机构应按照要求，

向执法部门公布相关的保密信息，CA 机构无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4. 用户隐私保护

9.4.1. 隐私保密方案

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

CA 机构应保护证书申请人所提供的、证明其身份的资料。CA 机构应采取必要的安全措施防止证书申请人资料被遗失、盗用与篡改。

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

9.4.2. 作为隐私处理的信息

证书申请人提供的不构成数字证书内容的资料被视为隐私信息。

9.4.3. 不被视为隐私的信息

证书申请人提供的用来构成数字证书内容的资料不认为是隐私信息。

数字证书是公开的，CA 机构可通过目录服务等方式向外公布。

9.4.4. 用户个人信息的收集

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

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

面同意。

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

9.4.5. 个人信息的存储

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

9.4.6. 用户个人信息的使用

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

1、基于国家法律、行政法规、规章的规定而提供的；

2、经过用户本人书面授权或同意提供的。

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

9.4.7. 用户个人信息的共享

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

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

9.4.8. CA 对于用户个人信息的管理

CA 机构通过以下措施规范用户个人信息的内部管理：

a)CA 机构遵循法律法规的要求及行业规范要求采取对个人信息安全保护

b)CA 机构内部建立严格的用户个人信息收集、查阅、使用、处理等管理制度。

c) 机构通过加强内部员工关于个人信息保护的培训，CA 要求员工参加学习培训后签署用户个人信息保护的承诺书；

d) 机构要求注册机构建立不能低于 CA 机构对用户个人信息的保护级别 CA 的用户个人信息保护制度，并提交 CA 机构备案。

9.4.9. 个人信息的查阅

用户如需查阅及浏览自身的个人信息，请用户按农信银资金清算中心有限责任公司官方网站公布的联系方式联系 CA 机构查询。

9.4.10. 个人信息的删除和更改

1、个人信息的删除

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

2、个人信息的更改

用户在使用 CA 证书服务过程中，个人信息发生变更的，应当自个人信息变更之日起 2 日内通过农信银资金清算中心有限责任公司官方网站公布的联系方式提出；由于用户自身原因未及时将变更信息通知 CA 机构的，由此发生的风险由用户自身承担。

9.5. 知识产权

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

按本《电子认证业务规则》的规定，所有由 CA 机构签发的证书和提供的软件中使用、体现和相关的一切版权、商标和其他知识产权均属于农信银资金清算中心有限责任公司所有，这些知识产权包括所有相关的文件和使用手册。注册机构应征得 CA 机构的同意使用相关的文件和手册，并有责任和义务提出修改意见。

9.6. 陈述与担保

9.6.1. 电子认证服务机构的陈述与担保

CA 机构在提供电子认证服务活动过程中的承诺如下：

a) CA 机构遵守《中华人民共和国电子签名法》及相关法律的规定，接受工业和信息化部的领导，对签发的数字证书承担相应的法律责任。

b) CA 机构保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定。

c) 除非已通过 CA 机构证书库发出了 CA 的私钥被破坏或被盗的通知，CA 机构保证其私钥是安全的。

d) CA 机构签发给订户的证书符合 CA 机构的 CPS 的所有实质性要求。

e) CA 机构将向证书订户通报任何已知的、将在本质上影响订户的证书的有效性和可靠性事件。

f) CA 机构将及时吊销证书。

g) CA 机构拒绝签发证书后，将立即向证书申请人归还所付的全部费用。

h) 证书公开发布后，CA 机构向证书依赖方证明，CA 数字证书中载明的订户信息都是准确的。

9.6.2. 注册机构的陈述与担保

CA 机构的注册机构在参与电子认证服务过程中的承诺如下：

a) 提供给证书订户的注册过程完全符合 CA 机构的 CPS 的所有实质性要求。

b) 在 CA 机构生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请人的信息不一致。

c) 注册机构将按 CPS 的规定，及时向 CA 机构提交证书申请、吊销、更新等服务请求。

9.6.3. 订户的陈述与担保

订户一旦接受 CA 机构签发的证书，就被视为向 CA 机构、注册机构及信赖证书的有关当事人作出以下承诺：

a) 订户需熟悉本《电子认证业务规则》的条款和与其证书相关的证书政策，

还需遵守证书持有人证书使用方面的有关限制。

b) 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，可供 CA 机构或注册机构检查和核实。

c) 订户应当妥善保管私钥，采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件的发生。

d) 私钥为订户本身访问和使用，订户对使用私钥的行为负责。

e) 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知 CA 机构和注册机构，申请采取吊销等处理措施。

f) 订户已知其证书被冒用、破解或被他人非法使用时，应及时通知 CA 机构吊销其证书。

9.6.4. 依赖方的陈述与担保

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

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

所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本《电子认证业务规则》的有关条款。

9.6.5. 其他参与者的陈述与担保

其他参与者的陈述与担保同 9.6.4。

9.7. 赔偿责任限制

9.7.1. 赔偿责任范围

CA 机构的赔偿责任范围：

a) 证书信息与订户提交的信息资料不一致，导致订户损失。

b) 因 CA 机构原因，致使订户无法正常验证证书状态，导致订户利益受损。

c) CA 机构在证书有效期限内承担损失或损害赔偿。

9.7.2. 对最终实体的赔偿担保

CA 机构对所有当事实体（包括但不限于订户、申请人或信赖方）的合计责任不超过证书的适用的责任封顶。对于一份证书产生的所有数字签名和交易处理，CA 机构对于任何人有关该特定证书的合计责任应该限制在一个不超出赔偿责任上限的范围内，这种赔偿上限可以由 CA 机构根据情况重新制定，CA 机构会将重新制定后的情况立刻通知相关当事人。

CA 机构所颁发数字证书的赔偿责任上限如下。

个人证书：800 元人民币。

机构证书：4000 元人民币。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的责任均有封顶而不考虑数字签名和交易处理等有关的其他索赔的数量。当超过责任封顶时，可用的责任封顶将首先分配给最早得到索赔解决的一方。CA 机构没有责任为每个证书支付高出责任封顶的赔偿，而不管责任封顶的总量在索赔提出者之间如何分配的。

如果 CA 机构根据本 CPS 或任何法律规定，以及司法判定须承担赔偿和/或补偿责任的，CA 机构将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

9.7.3. 责任免除

有下列情况之一的，应当免除 CA 机构之责任。

a) 如果证书申请人故意或无意地提供了不完整、不可靠或已过期的信息，又根据正常的流程提供了必须的审核文件，得到了 CA 机构签发的数字证书，由此引起的经济纠纷应由证书申请人全部承担，CA 机构不承担与证书内容相关的法律和经济责任，但可以根据受害者的请求提供协查帮助。

b) CA 机构不承担任何其他未经授权的人或组织以本 CA 机构名义编撰、发表或散布的不可信赖的信息所引起的法律责任。

c) CA 机构不承担在法律许可的范围内，根据受害者或法律的要求如实提供网上业务中“不可抵赖”的数字签名依据所引起的法律责任。

d) CA 机构不对任何一方在信赖证书或使用证书过程中引起的直接或间接的损失承担责任。

e) CA 机构和注册机构不是证书持有人或依赖方的代理人、受托人、管理人或其他代表。CA 机构和证书持有人间的关系以及 CA 机构和依赖方间的关系并不是代理人和委托者的关系。证书持有人和依赖方都没有权利以合同形式或其他

方法让 CA 机构承担信托责任。

f) CA 机构与授权的外部注册机构签署合同，合同条款中明确注册机构负责并承担订户身份核实责任。对于明显由授权的外部注册机构的过错行为所产生的法律与赔偿责任由 CA 机构授权的外部注册机构承担。

g) 若数字证书被超出范围或者以非预期的方式使用（如应用领域不被 CA 机构认可等），CA 机构不向任何方承担赔偿和/或补偿责任。

h) 由于客观意外或其他不可抗力事件原因而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。关于不可抗力的描述参见 9.16.4。

i) 因 CA 机构的设备或网络故障等技术故障而导致数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“技术故障”引起原因包括但不限于：（1）不可抗力；（2）关联单位如电力、电信、通讯部门而致；（3）黑客攻击；（4）设备或网络故障。

j) CA 机构已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

9.8. 有限责任

CA 机构根据与订户的合同承担相应的有限责任。

CA 机构在与订户和依赖方签定的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

9.9. 赔偿

CA 机构按照本《电子认证业务规则》9.7 条款承担赔偿责任。

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

订户接受证书就表示同意在以下情况下承担赔偿责任:

a) 未向 CA 机构提供真实、完整和准确的信息，而导致 CA 机构或有关各方损失。

b) 未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时。

c) 在知悉证书密钥已经失密或者可能失密时，未及时告知 CA 机构，并终止使用该证书，而导致 CA 机构或有关各方损失。

d) 订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个数字签名后理所当然地相信这些表述，订户必须对这种行为的后果负责。

e) 证书的非法使用，即违反 CA 机构对证书使用的规定，造成了 CA 机构或有关各方的利益受到损失。

9.10. 有效期与终止

9.10.1. 有效期

本《电子认证业务规则》自发布之日起正式生效。
本《电子认证业务规则》中将详细注明版本号及发布日期。

9.10.2. 终止

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

9.10.3. 效力的终止与保留

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

9.11. 对参与者的个别通告与沟通

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

9.12. 修订

9.12.1. 修订程序

当本《电子认证业务规则》不适用时，由农信银资金清算中心有限责任公司安全策略管理委员会组织 CPS 编写小组进行修订。

修订完成后，农信银资金清算中心有限责任公司安全策略管理委员会进行审批，审批通过后将在农信银资金清算中心有限责任公司的网站（http://www.nongxinyin.com）《电子认证业务规则》将进行严格的版本控制。

9.12.2. 通告机制和期限

《电子认证业务规则》在农信银资金清算中心有限责任公司的网站(http://www.nongxinyin.com)版本更新时，最新版本的《电子认证业务规则》在农信银资金清算中心有限责任公司的网站发布，对具体个人不做另行通知。

9.12.3. 必须修改业务规则的情形

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

9.13. 争议处理

CA 机构、证书订户、依赖方等实体在电子认证活动中产生争端可按照以下步骤解决：

a) 当事人首先通知 CA 机构，根据本《电子认证业务规则》中的规定，明确责任方；

b) 由 CA 机构相关部门负责与当事人协调；

c) 若协调失败，可以通过仲裁或司法途径解决；

d) 任何因与 CA 机构或授权机构就本《电子认证业务规则》所产生的任何争议而提起诉讼的，受农信银资金清算中心有限责任公司工商注册所在地的人民法院管辖。

9.14. 管辖法律

《电子认证业务规则》在各方面服从中国法律和法规的管制和解释，包括但不限于《中华人民共和国电子签名法》及《电子认证服务管理办法》等。

9.15. 与适用法律的符合性

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

9.16. 一般条款

9.16.1. 完整规定

本《电子认证业务规则》将替代先前的、与主题相关的书面或口头解释。

9.16.2. 分割性

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

9.16.3. 强制执行

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

9.16.4. 不可抗力

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

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

9.17. 其他条款

农信银资金清算中心有限责任公司对本《电子认证业务规则》拥有最终解释权。