农信银资金清算中心有限责任公司

证书策略

〈版本：V2.0〉

农信银资金清算中心有限责任公司

2024年6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	形成版本	公司安全策略管理委员会	2021年11月
V2.0	根据CPS内容更新修订	公司安全策略管理委员会	2024年6月

目 录

1 概括性描述

1.1 概述

证书策略(Certificate Policy，以下简称 CP)是电子认证服务机构制订的一组策略，表明农信银资金清算中心有限责任公司（以下简称农信银） PKI 体系中各个参与者的划分与义务，并包含农信银证书基本策略。

本 CP 的适用范围为农信银发放的证书。

1.2 文档名称与标识

此文档的名称为《农信银资金清算中心有限责任公司证书策略》，文档编写遵从 IETF RFC3647 及 GB/T 26855-2011。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

农信银是根据《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（CA）。

CA 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（RA）是识别和鉴别证书申请人，受理数字证书申请、更新、恢复和注销等业务的实体。

CA 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。农信银授权的注册机构包括电子认证服务的应用机构。

1.3.3 订户

订户是指向 CA 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

农信银证书支持相应的合法应用，具体应用场景在农信银 CPS 1.4 章节说明。

1.4.2 限制的证书应用

农信银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 CP 的策略文档管理机构为农信银安全策略管理委员会。由安全策略管理委员会负责本CP的制订、发布、更新等事宜。

1.5.2 联系方式

联系地址：北京市丰台区南四环西路186号汉威国际广场 二区 4号楼
邮政编码：100160
电话：4008685678
网址：http://www.nongxinyin.com/

1.5.3 决定 CP 符合策略的机构

本 CP 由农信银安全策略管理委员会组织制定，报农信银安全策略管理委员会批准实行。

1.5.4 CP 批准程序

本 CP 经农信银安全策略管理委员会审批通过后，在农信银网站上对外公布。

本 CP 从对外发布之日起三十日之内向中华人民共和国工业和信息化部备案。

本 CP 的网上发布遵照农信银官网要求执行。自本 CP 发布之日起，所有以各种形式对外提供的 CP 必须与网站公布的 CP 保持一致。

1.6 定义和缩写

下列定义适用于本 CP：

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

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

2、电子认证服务机构（CA）Certificate Authority

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。

3、注册机构（RA）Registration Authority

识别和鉴别证书申请人，受理数字证书申请、更新、恢复和注销等业务的实体。

4、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。

5、证书策略（CP）Certificate Policy

电子认证服务机构（CA）制订的一组策略，表明证书对具有相同安全需求的一个特定团体和（或者）应用类型的适用性。

6、电子认证业务规则（CPS）Certificate Practice Statement

关于电子认证服务机构（CA）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。

7、证书撤销列表（CRL）Certificate Revocation List

一个经电子认证服务机构（CA）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。

8、私钥 Private Key

非对称密码算法中只能由拥有者使用的不公开密钥。

9、公钥 Public Key

非对称密码算法中可以公开的密钥。

10、甄别名（DN）Distinguished Name

数字证书的主体名称域中，用于唯一标识证书主体的X.500名称。

11、在线证书状态协议（OCSP）Online Certificate Status Protocol

在线查询数字证书状态协议，用于实时查询数字证书状态信息。

2 信息发布与信息管理

2.1 信息库

农信银信息库面向订户及证书应用依赖方提供信息服务。

农信银信息库包括但不限于以下内容：证书、CRL、CPS、CP、农信银网站信息以及农信银不定期发布的信息。

2.2 认证信息的发布

农信银的 CPS、CP 以及相关的技术支持信息等在农信银网站上发布。

证书状态可通过 CRL 或 OCSP 获得。

2.3 发布的时间或频率

农信银 CP 按照 1.5.4 所述的批准流程，一经发布到农信银网站即时生效。

农信银采用实时或定期的方式发布 CRL 。

2.4 信息库访问控制

只有经授权的 CA/RA 管理员可以查询 CA 和 RA 数据库中的数据。

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。

DN (Distinguished Name)：唯一甄别名，在数字证书的主体名称域中，用于唯一标识证书主体的 X.500 名称。除农信银预签证书外，此域需要填写反映证书主体真实身份的、具有实际意义的、与法律不冲突的内容。

3.1.3 订户的匿名或伪名

在 CA 证书服务体系中，除在特定的场景下，原则上订户不使用匿名或伪名。

3.1.4 解释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 商标的识别、鉴别和角色

农信银签发的证书不包含任何商标或者可能对其他机构构成侵权的信息。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

证书请求中所包含的数字签名来证明订户持有与注册公钥对应的私钥。 农信银在签发证书前，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 订户身份鉴别

订户在申请农信银签发的证书前应在农信银授权的注册机构端完成实名认证，并接受证书申请的有关条款，同意承担相应的责任。

具体鉴别内容参见农信银 CPS 3.2 章节。

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，属于没有验证的订户信息。

3.2.4 授权确认

当订户代表个人或组织机构申请证书时，需出示农信银 CPS 3.2 章节要求的个人或组织机构有效身份证明材料以及获得个人或组织机构的授权证明材料。

3.3 密钥更新请求的标识与鉴别

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 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

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本 CP 和农信银 CPS 所规定的义务，由农信银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 注册过程与责任

订户需按照本 CP 及农信银 CPS 所规定的要求提交证书申请，并提供真实、准确的申请材料，配合注册机构完成对身份信息的采集、记录和审核。根据《中华人民共和国电子签名法》规定，订户未向 CA 或注册机构提供真实、完整和准确的信息，或者有其他过错，给农信银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。

注册机构应明确告知订户所需承担的相关责任和义务，按照本 CP 及农信银 CPS 所规定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，注册机构向农信银提交证书申请，由农信银向订户签发证书。注册机构应按照协议约定及本 CP 及农信银 CPS 规定履行相关责任与义务。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

农信银或授权的注册机构按照本 CP 及农信银 CPS 所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程见农信银 CPS 3.2 章节。

4.2.2 证书申请批准和拒绝

农信银或授权的注册机构根据本 CP 及农信银 CPS 所规定的身份鉴别流程对订户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。

如果订户通过本 CP 及农信银 CPS 所规定的身份鉴别流程且鉴证结果为合格，注册机构向农信银提交证书申请，由农信银向订户签发证书。

订户未能通过身份鉴证，农信银或授权的注册将拒绝订户的证书申请，并通知订户鉴证失败，同时向订户提供失败的原因（法律禁止的除外）。被拒绝的订户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

农信银将在合理的时间内完成证书申请处理。

具体时间在农信银 CPS 中规定。

4.3 证书签发

4.3.1 证书签发中电子认证服务机构和注册机构的行为

通过鉴证后，注册机构向农信银提交证书申请，由农信银向订户签发证书。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 电子认证服务机构和注册机构对订户的通告

农信银通过注册机构对数字证书订户的通告有以下几种方式：

1、通过面对面的方式，通知订户到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；

2、通过邮政信函、电子邮件、电话、短信等通知订户；

3、农信银认为其他安全可行的方式通知订户。

4.4 证书接受

4.4.1 构成接受证书的行为

订户从获得数字证书起，就被视为同意接受证书。

具体描述参见农信银 CPS 4.4.1 章节。

4.4.2 电子认证服务机构对证书的发布

农信银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。

4.4.3 电子认证服务机构对其他实体的通告

农信银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农信银所签发的证书后，均视为已经同意遵守与农信银、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 依赖方公钥和证书的使用

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

验证证书的有效性包括：

1、用农信银的证书验证证书中的签名，确认该证书是农信银签发的，并且证书的内容没有被篡改。

2、检验证书的有效期，确认该证书在有效期之内。

3、检验数字证书有效性，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，到农信银或授权的注册机构申请更新证书。

4.6.2 请求证书更新的主体

已经申请过农信银证书的订户可以请求证书更新。

4.6.3 证书更新请求的处理

订户在证书到期前，应按要求向农信银或授权的注册机构提出更新申请，提供相关申请材料。

注册机构按照农信银 CPS 3.2 要求，对订户申请材料进行鉴别，鉴别通过后向农信银提出证书更新申请，由农信银为订户制作新的证书。

4.6.4 颁发新证书时对订户的通告

同 4.3.2。

4.6.5 构成接受更新证书的行为

同 4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

同 4.4.2。

4.6.7 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4. 7 证书密钥更新

4.7.1 证书密钥更新的情形

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书。

证书更新的具体情形如下：

1、当订户证书即将到期或已经到期时；

2、当订户证书密钥遭到损坏时；

3、当订户证实或怀疑其证书密钥不安全时；

4、其它可能导致密钥更新的情形。

4.7.2 请求证书密钥更新的主体

已经申请过农信银证书的订户可以请求证书密钥更新。

4.7.3 证书密钥更新请求的处理

同 3.3 。

4.7.4 颁发新证书时对订户的通告

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 请求证书变更的主体

已经申请过农信银证书的订户可以请求证书变更。

4.8.3 证书变更请求的处理

同3.3.3。

4.8.4 颁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 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

1、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本 CP 及农信银 CPS ；

2、发生下列情形之一的，农信银或授权的注册机构可以吊销签发的数字证书：

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 CP 及农信银 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 请求证书吊销的主体

已申请农信银证书的订户可请求证书吊销。

农信银或授权的注册机构也可在 4.9.1 所述的情形下主动吊销订户的证书。

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。

1、订户到农信银或授权的注册机构提交证书吊销申请，并注明吊销原因；

2、农信银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；

3、农信银吊销订户证书后，注册机构将当面通知订户证书被吊销，订户证书将定期发布到 CRL ；

4、强制吊销是指当农信银或授权的注册机构确认订户违反本 CP 或农信银 CPS 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。

农信银定期发布 CRL，供请求者查询下载。

4.9.6 依赖方检查证书吊销的要求

在具体应用中，依赖方必须使用以下两种功能之一进行所依赖证书的状态查询：

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

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

注意：依赖方要验证 CRL 的可靠性和完整性，确保是经农信银发布并且签名的。

4.9.7 CRL 发布频率

农信银采用实时或定期的方式发布 CRL 。

4.9.8 CRL 发布的最大滞后时间

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

证书状态可以通过农信银提供的 OCSP 服务获得。

4.10.2 服务可用性

提供 7*24 小时的证书状态查询服务。

4.11 订购结束

订购结束是指当证书有效期满或证书吊销后，该证书的服务时间结束。

订购结束包含以下两种情况：

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

2、在证书有效期内，证书被吊销后，即订购结束。

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

数字证书的签名密钥对由国家密码管理部门认可的密码设备生成，加密密钥对由密钥管理中心生成。

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。

具体描述参见农信银 CPS 4.12.1 章节。

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

本章节参见农信银 CPS 内容。

6 认证系统技术安全控制

本章节参见农信银 CPS 内容。

7 证书、证书吊销列表和在线证书状态协议

7.1 证书

7.1.1 版本号

X.509 V3。

7.1.2 证书扩展项

农信银证书扩展项使用 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）

用于识别与证书签名私钥相对应的公钥，可辨别同一 CA 使用的不同密钥。

2、主体密钥标识符（Subject Key Identifier）

标识了被认证的公钥，可用于区分同一主体使用的不同密钥。

3、密钥用法（Key Usage）

指明已认证的公开密钥用于何种用途。

4、扩展密钥用途（Extended Key Usage）

可作为对密钥用法扩展项中指明的基本用途的补充或替代。

5、基本限制（Basic Constraints）

标识证书的主体是否是一个 CA，通过该 CA 可能存在的认证路径有多长。

6、证书撤销列表分发点（CRL Distribution Points）

依赖方可根据该扩展项提供的地址下载 CRL 。

7、颁发机构授权信息访问（Authority Info Access）

用于获得证书签发者的证书来验证用户证书。

7.1.3 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。

7.1.4 名称形式

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

7.2 证书吊销列表

7.2.1 版本号

X.509 V2 。

7.2.2 CRL 和 CRL 条目扩展项

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

不使用 CRL 条目扩展项。

7.3 在线证书状态协议

农信银提供在线证书状态查询服务。

在正常的网络状态下，农信银可确保有足够的资源使 CRL 和 OCSP 服务在合理的时间内向用户提供查询结果。

8 电子认证服务机构审计和其它评估

8.1 评估的情形

评估是为了检查、确认 CA 是否按照 CP 、CPS 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。

1、根据《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》规定，接受主管部门的评估和检查。

2、根据工作需要，定期组织开展评估。

8.2 评估者的资质

内部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，农信银将根据报告内容准备一份解决方案，明确对此采取的行动，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，农信银一般不公开评估结果。

对农信银关联方，农信银将依据签订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

农信银数字证书的收费按照与应用机构签订的数字证书技术服务协议中约定的收费标准执行。

9.1.2 证书查询费用

农信银暂不收取此项费用，但保留对此项服务收费的权利。

9.1.3 证书吊销或状态信息的查询费用

农信银暂不收取此项费用，但保留对此项服务收费的权利。

9.1.4 其他服务费用

农信银暂不收取其他服务费用，但保留收取其他服务费用的权利。

9.1.5 退款策略

在实施证书操作和签发证书的过程中，农信银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，农信银将不办理退证、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，农信银将不退还剩余时间的服务费用。

9.2 财务责任

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

9.3 业务信息保密

9.3.1 保密信息范围

保密的业务信息包括但不限于以下方面：

1、在双方披露时标明为保密（或有类似标记）的；

2、在保密情况下由双方披露的或知悉的；

3、双方根据合理的商业判断应理解为保密数据和信息的；

4、以其他书面或有形形式确认为保密信息的；

5、或从上述信息中衍生出的信息。

对于农信银来说，保密信息包括但不限于以下方面：

1、最终用户的私人签名密钥都是保密的；

2、保存在审计记录中的信息；

3、年度审计结果也同样视为保密；

4、除非有法律要求，由农信银掌握的，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。

农信银不保存任何证书应用系统的交易信息。除非法律明文规定，农信银及授权的注册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

不属于保密的信息包括但不限于以下方面：

1、信息主体同意公开的信息不属于保密信息。

2、依据法律、行政法规规定可以公开的信息，农信银可以选择公开。

3、订户数字证书的相关信息可以通过农信银目录服务等方式向外公布，但农信银认为涉及订户保密信息的除外。

4、其他可以通过公共、公开渠道获取的信息。

9.3.3 保护保密信息的责任

1、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。

2、当农信银在任何法律、法规或规章的要求下，或在法院的要求下必须提供本 CP 中具有保密性质的信息时，农信银应按照要求向执法部门公布相关的保密信息，农信银无须承担任何责任。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

根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》，农信银在受理客户申请证书及相关电子签名业务时，需由证书申请人及/或经办人提供相关个人信息。其中个人信息包括：姓名、联系方式、身份证号、地址和身份证（原件及任何形式的复本）等个人隐私信息。

9.4.1 隐私保密方案

在数字证书生命周期中，农信银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。

农信银应保护证书申请人所提供的、证明其身份的资料。农信银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。

农信银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

订户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

订户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，农信银可通过目录服务等方式向外公布。

9.4.4 保护隐私的责任

农信银、注册机构、订户、依赖方及其他参与者都有义务按照本 CP 的规定，承担相应的隐私保护责任。在法律法规或公共权力部门通过合法程序或订户书面申请授权要求下，农信银可以向特定的对象公布隐私信息，农信银无需承担由此造成的任何责任。

9.4.5 使用隐私信息的告知与同意

1、订户同意，农信银在业务范围内并按照本 CP 规定的隐私保护政策使用所获得的任何订户信息，无论是否涉及到隐私，农信银均可以不用告知订户。

2、订户同意，在任何法律法规或公共权力部门要求下，农信银向特定对象披露隐私信息时，农信银均可以不用告知订户。

9.4.6 依法律或行政程序的信息披露

农信银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，农信银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，农信银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 其他信息披露情形

农信银、注册机构、订户、依赖方及其他参与者都有义务按照本 CP 的规定，承担相应的隐私保护责任。在法律法规或公共权力部门通过合法程序或订户书面申请授权要求下，农信银可以向特定的对象公布隐私信息，农信银无需承担由此造成的任何责任。

9.5 知识产权

除非额外声明，农信银享有并保留对证书以及农信银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。农信银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 CP 及农信银 CPS 规定，所有由农信银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。注册机构应征得农信银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

农信银在提供电子认证服务活动过程中的承诺如下：

1、遵守《电子认证服务管理办法》及相关法律的规定，接受中华人民共和国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。

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

3、除非已通过证书库发出了 CA 的私钥被破坏或被盗的通知，农信银保证其私钥是安全的。

4、签发给订户的证书符合农信银的 CP 及 CPS 的所有实质性要求。

5、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。

6、及时吊销证书。

7、拒绝签发证书后，将立即向证书申请人归还所付的全部费用。

8、证书公开发布后，农信银向证书依赖方证明，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

农信银授权的注册机构在参与电子认证服务过程中的承诺如下：

1、提供给订户的注册过程完全符合农信银的 CP 及 CPS 的所有实质性要求。

2、注册机构需按本 CP 及农信银 CPS 的规定，核实订户身份信息。在农信银生成证书时，不会因为注册机构的失误而导致证书中的信息与订户的信息不一致。

3、注册机构需按本 CP 及农信银 CPS 的规定，及时向农信银提交证书申请、吊销、更新等服务请求。

9.6.3 订户的陈述与担保

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

1、订户需熟悉本 CP 及农信银 CPS 的条款和与其证书相关的证书政策，还需遵守证书持有人证书使用方面的有关限制。

2、订户在证书申请表上填写的所有声明和信息必须是完整、真实和正确的，可供 农信银或注册机构检查和核实。

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

4、私钥为订户本身访问和使用，订户对使用私钥的行为负责。

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

6、订户已知其证书被冒用、破解或被他人非法使用时，应及时通知农信银和注册机构吊销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉本 CP 及农信银 CPS 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 CP 及农信银 CPS 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 责任免除

有下列情况之一的，应当免除农信银之责任。

1、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，得到了农信银签发的数字证书，由此引

起的经济纠纷应由证书申请人全部承担，农信银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。

2、农信银不承担任何其他未经授权的人或组织以农信银名义编撰、发表或散布的不可信赖的信息所引起的法律责任。

3、农信银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。

4、除因数字证书本身问题外，农信银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。

5、农信银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。农信银和证书持有人间的关系以及农信银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农信银承担信托责任。

6、农信银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农信银授权的外部注册机构承担。

7、若数字证书被超出范围或者以非预期的方式使用(如应用领域不被农信银认可等)，农信银不向任何方承担赔偿和/或补偿责任。

8、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 9.16.5。

9、因农信银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。

10、由于监管机构要求导致的非计划性停机以及系统例行维护需要、软件及硬件升级而进行的计划性停机，且已经提前书面通知相关方，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。

11、农信银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及本 CP 、农信银 CPS 开展数字证书认证服务，而仍有损失产生的。

9.8 有限责任

农信银根据协议承担相应的有限责任，对于因注册机构、订户、依赖方或其他参与者原因造成的损害不具有赔偿义务。

9.9 赔偿

（一）农信银的赔偿责任范围：

1、证书信息与订户提交的信息资料不一致，导致订户损失。

2、因农信银原因，致使订户无法正常验证证书状态，导致订户利益受损。

3、农信银在证书有效期限内承担损失或损害赔偿。

农信银对所有当事实体(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，农信银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农信银根据情况重新制定，农信银会将重新制定后的情况立刻通知相关当事人。

农信银所颁发数字证书的赔偿责任上限如下：

个人订户： 800 元人民币。

机构订户： 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。农信银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。

如果农信银根据本 CP 及农信银 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，农信银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。

（二）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农信银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：

1、未向农信银提供真实、完整和准确的信息，而导致农信银或有关各方损失。

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

3、在知悉证书密钥已经失密或者可能失密时，未及时告知农信银和注册机构，并终止使用该证书，而导致农信银或有关各方损失。

4、订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个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。

5、证书的非法使用，即违反农信银对证书使用的规定，造成了农信银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 CP 自发布之日起正式生效。

本 CP 中将详细注明版本号及发布日期。

9.10.2 终止

当新版本的 CP 正式发布生效时，旧版本的 CP 自动终止。

9.10.3 效力的终止与保留

本 CP 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等。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 CP 不适用时，由农信银安全策略管理委员会组织 CP 编写小组进行修订。

修订完成后，农信银安全策略管理委员会进行审批，审批通过后将在农信银网站（http://www.nongxinyin.com）上发布新的 CP 。

CP 将进行严格的版本控制。

9.12.2 通告机制和期限

本 CP 在农信银网站(http://www.nongxinyin.com)上发布。

版本更新时，最新版本的 CP 在农信银网站发布，对具体个人不做另行通知。

9.12.3 必须修改证书策略的情形

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 CP 。

9.13 争议处理

农信银、证书订户、依赖方等实体在电子认证活动中产生争端可按照以下步骤解决：

1、当事人首先通知农信银，根据本 CP 中的规定，明确责任方；

2、由农信银相关部门负责与当事人协调；

3、若协调失败，可以通过仲裁或司法途径解决；

4、任何因与农信银或授权注册机构就本 CP 所产生的任何争议而提起诉讼的，受农信银工商注册所在地的人民法院管辖（与应用机构协议有约定的除外）。

9.14 管辖法律

本 CP 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 CP 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 CP 将替代先前的、与主题相关的书面或口头解释。

9.16.2 转让

CA、RA、订户及依赖方之间的权利义务不能通过违法或者无授权形式转让给任何人。

9.16.3 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。

9.16.4 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。

9.16.5 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，农信银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（如订户等）不得提出异议或者申请任何补偿。

9.17 其他条款

农信银对本 CP 拥有最终解释权。