通 用 数 字 证 书

电子认证服务业务规则

（Version 1.6）

苏博云科数字认证有限公司

二〇二一年八月

目 录

1 概括性描述

1.1 概述

苏博云科数字认证有限公司（简称为“苏博云科 CA”，英文名称为 eCardCA）面向“智慧教育、数字校园、金融、工业互联网、智能交通、新基建、智慧城市”等应用领域，提供以安全芯片、智能 IC 卡、UKEY、可穿戴设备、通话电子学生证等为载体的网络空间新型数字证书管理、密钥管理等基础电子认证服务，提供涵盖“身份认证、授权管理、责任认证、数据安全、隐私保护”等电子认证扩展应用的支撑与服务。

eCardCA 严格按照《中华人民共和国电子签名法》与《电子认证服务管理办法》的要求，遵循国家信息安全保障的总体政策要求，依据国家相关法律法规与标准规范，采用通过国家密码管理局鉴定和认可的商用密码产品，使用创新的电子认证业务与服务模式，提供安全、统一、有序的电子认证服务。

eCardCA 根据《电子认证服务管理办法》，依据《电子认证服务业务规则规范》，依据面向人员、机构、设备等实体提供符合国家密码管理标准规范要求的数字证书（以下统称为“通用数字证书”）服务的要求，制定了《苏博云科 CA 通用数字证书电子认证服务业务规则》（以下简称“eCardCA-CPS”）。

本 eCardCA-CPS 详细阐述了 eCardCA 在实际工作和运营中所遵循的各项规范，适用于 eCardCA 及其员工、注册机构、证书申请方、订户和依赖方，各参与方须完整理解和执行 eCardCA-CPS 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

本文档名称为《通用数字证书电子认证服务业务规则》，版本 Version 1.6。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

苏博云科数字认证有限公司根据《中华人民共和国电子签名法》和《电子认证服务管理办法》的规定，依法开展第三方电子认证服务。

电子认证服务机构是受订户信任，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（以下简称为“RA”）作为电子认证服务机构授权委托的下属机构，包括注册系统（RA 系统）和远程注册机构，负责受理证书申请，负责对证书订户信息的审核、整理汇总、统计分析，负责与 CA 进行数据交换，实现各类证书业务的处理。

RA 必须获得 eCardCA 的授权，根据授权从事相关证书业务服务。各类政府机构、企事业单位等均可申请成为 eCardCA 的注册机构。eCardCA 根据申请单位的性质、证书发展规模、场地和人员情况等，对其进行严格的评估审计，合格后由安全策略委员会最终决定，对其发放授权委托书，授权其成为注册机构。

RA 有责任妥善保存与保管订户的数据，不允许将订户数据透露给与证书申请无关的任何单位或个人，不允许将订户数据用于商业利益方面的用途。RA 对其提供的证书服务负有相关的法律责任，包括但不限于 eCardCA-CPS 和授权协议中所规定的有关内容。

1.3.3 业务受理点

业务受理点(LRA)是经过 eCardCA 或其授权 RA 的审查及授权，负责办理证书的申请、更新、注销、下载及其他授权业务。LRA 对其提供的证书服务的受理过程负有相关的法律责任，包括但不限于 eCardCA-CPS 和授权协议中所规定的有关内容。

1.3.4 订户

订户，即证书持有人，是指从 eCardCA 接收证书的实体。包括已经申请并拥有 eCardCA 签发的数字证书的单位、企业、组织、机构、个人、服务器、网站等各类主体或实体，以及其他任何具有确定的身份标识，并持有 eCardCA 签发的数字证书的对象。

在电子签名应用中，订户即为电子签名人。

1.3.5 依赖方

依赖方是指任何使用 eCardCA 签发的证书进行网络作业的证书持有者和按照 eCardCA-CPS 合理信任证书真实性的任何实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。

在 eCardCA 的证书服务体系中，依赖方是信任 eCardCA 所签发的数字证书（以下简称为通用数字证书），可以对使用通用数字证书生成的数字签名进行验证，使用其他通用数字证书的公钥的实体。依赖方可以在法律规定以及 eCardCA-CPS 规定的范围内信任通用数字证书及其签名，并享有 eCardCA-CPS 规定的各种权利。

依赖方应合理地信任证书以及相关的数字签名。如果信任数字签名时需要额外的保证，依赖方必须得到这些保证后才能合理地信任该数字签名。

非 eCardCA 订户的依赖方，eCardCA 除了担保其所信任的并且由 eCardCA 签发的证书和相关签名信息的真实性以外，不承担其它义务和责任。

1.3.6 其他参与者

其他参与者是指其他为 eCardCA 提供相关服务的实体。

1.4 证书类型

本 eCardCA-CPS 定义了通用数字证书的业务规则。通用数字证书，是指符合国家密码管理标准规范要求的数字证书，以智能密码钥匙（Ukey）为安全存储介质，分为个人证书、机构证书和设备证书三种类型。依赖方通过对通用数字证书进行验证，实现对证书应用实体的身份识别、数字签名、信息保护等安全应用。

在本文档中，在不作特别说明情况下，证书则即指通用数字证书。

1.5 证书应用

1.5.1 适合的证书应用

通用数字证书主要适合以下方面的应用。

1. 身份认证：保证采用 eCardCA 信任服务的证书持有者身份的合法性，主要包括对个人、机构和设备等网络实体的鉴别。
2. 电子签名：使用通用数字证书对信息进行电子签名，实现对信息的完整性保护，防止对信息的篡改。同时，还可实现提交信息的不可抵赖性。通过在电子签名时包含时间信息，还可形成时间戳签名，实现对关键操作的时间进行真实性验证。
3. 信息保护：对于信息化应用中存储与传输的重要信息、敏感信息，可以

使用通用数字证书进行加密保护。

4. 操作审计：使用通用数字证书对操作日志进行电子签名，确保订户对执行的操作的不可抵赖性。
5. 权限管理：以通用数字证书作为订户身份认证的凭证，在此基础上，对订户进行分组划分，进而对其进行权限管理与访问控制。

1.5.2 限制的证书应用

限制 eCardCA 所签发证书应用的场合主要包括（但不限于）：

1. 禁止在任何违反国家法律、法规或破坏国家安全的情形下使用，由此造成的法律后果由订户自己承担；
2. 由于证书的使用可能导致人员死亡、伤残的情形；
3. 由于证书的使用可能导致环境破坏的情形。

违反本限制的证书应用要求所造成的法律后果由订户负责。

1.6 策略管理

1.6.1 策略文档管理机构

eCardCA-CPS 的管理机构是 eCardCA 的安全策略委员会。由安全策略委员会负责 eCardCA-CPS 的制定、发布、更新等事宜。

1.6.2 联系人

本 eCardCA-CPS 通过内部文件发布，对具体个人不另行通知。

联系人：综合管理部门

邮箱：eCardCA-CPS@chinaonenet.com

联系地址：长沙国家高新开发区尖山路 39 号长沙中电软件园 18 栋二层

邮编：410205

联系电话：0731-88239505 传 真：0731-88239505

1.6.3 决定 CPS 符合策略的机构

安全策略委员会负责 eCardCA-CPS 的制订、发布、更新以及对外咨询等事宜，是 eCardCA-CPS 的管理机构。

1.6.4 CPS 批准程序

eCardCA 安全策略委员会负责 eCardCA-CPS 的管理。安全策略委员会指定 CPS 编写小组负责编写 eCardCA-CPS，在征求公司管理职能部门和管理层团队意见的基础上，达成一致意见后提交安全策略委员会审阅；CPS 编写小组依据安全策略委员会评审意见完成 eCardCA-CPS 的修改、确定 eCardCA-CPS 版本号，并形成定稿，报安全策略委员会主任审批；安全策略委员会主任审批同意后，方可对外发布。

安全策略委员会负责自发布之日起 30 天内向国家工业和信息化部备案。

1.7 定义和缩写

下述定义适用于本 eCardCA-CPS。

1．通用数字证书

通用数字证书也称为公钥证书，由数字证书认证机构（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。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

2．eCardCA

受订户信任，负责创建和分配订户密钥和公钥证书的权威电子认证机构。

3．eCardCA 电子认证服务业务规则

关于 eCardCA 在签发、管理、注销或更新证书（或更新证书中的密钥）过程中采纳的业务实践的声明。

4．注册机构

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冻结证书，处理订户撤销或冻结证书的请求，同意或拒绝订户更新其证书或密钥的请求。

5．证书注销列表（CRL）

一个已标识的列表，指定了一套证书发布者认为无效的证书。除普通 CRL 外，还定义了一些特殊的 CRL 类型用于覆盖特殊领域的 CRL。

6．CA 机构撤销列表（ARL）

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。

7．私钥

私钥是指在公钥密码系统中，订户的密钥对中只能由订户持有并保持为秘密的密钥。

8．公钥

公钥是指在公钥密码系统中，订户的密钥对中可以公开的密钥。

9．DN

即证书持有人的唯一标识符（Distinguished Name）。

2 信息发布与信息管理

2.1 认证信息的发布

eCardCA 通过业务门户网站（www.ecardca.com）公布与其相关的信息。该门户网站是 eCardCA 发布所有信息的最权威、最及时、最主要的渠道。

eCardCA-CPS 发布在 eCardCA 的业务门户网站上，供相关方查询、下载。

eCardCA 通过目录服务器发布订户的证书和 CRL。订户或依赖方可以通过访问 eCardCA 的目录服务器获取证书和 CRL。同时，eCardCA 提供在线证书状态查询服务（OCSP 服务）。

2.2 发布的时间与频率

2.2.1 CPS 的发布时间与频率

按照 eCardCA-CPS 的相关规定，eCardCA 及时在业务门户网站上发布 eCardCA-CPS 最新版本。

2.2.2 证书 CRL 的发布时间与频率

1. 证书一经签发，就即时在 eCardCA 的证书服务目录服务器公布；
2. CRL 每 24 小时发布一次；在紧急情况下，eCardCA 可自行决定 CRL 的发布时间与频率；
3. 通过 OCSP 对证书状态的查询是及时的。

2.2.3 其他公告、通知等信息的发布时间与频率

1. 根据实际业务开展的需要，eCardCA 将及时在业务门户网站发布与电子认证服务相关的公告与通知；
2. 该类信息不定期发布，eCardCA 将保证发布信息的及时性。

2.3 信息库访问控制

对于公开发布的 eCardCA-CPS、证书、CRL 等信息，eCardCA 允许公众自行通过网站和目录服务器进行查询与访问。

eCardCA 设置了访问控制与安全审计措施，保证只有经授权的 eCardCA 业务人员才能编写和修改 eCardCA 在线公布的信息。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

通用数字证书采用 X.500 定义的唯一甄别名 DN（Distinguished Name）来标识订户身份。

3.1.2 对名称意义化的要求

订户的甄别名必须具有明确的、肯定的意义。主体名称应能正确标识证书与证书实体的之间的对应关系，且应当符合法律法规等相关规定的要求。

3.1.3 订户的匿名或伪名

eCardCA 不允许、也不接受任何匿名或伪名，仅接受具有明确意义的名称作为 DN。

3.1.4 理解不同名称形式的规则

DN 由 CN、OU、O、C 等部分组成，其中 CN 表示订户名，OU、O 表示组织单位名称，C 用来表示国家。

3.1.5 名称的唯一性

在通用数字证书的服务体系中，“证书主体名＋证书序列号”必须是唯一的。

3.1.6 商标的识别、鉴别和角色

通用数字证书的主体甄别名中不包含商标名。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

eCardCA 通过证书请求信息中所包含的数字签名，来证明证书申请人持有与公钥对应的私钥。

在订户申请数字证书时，订户签名私钥由订户密码设备生成。证书请求信息中包含用该私钥进行的数字签名，可以用其对应的公钥来验证这个签名。因此，证书申请人视作其签名私钥的唯一持有者。证书申请人应妥善保管自己的私钥。

3.2.2 组织机构身份的鉴别

组织机构的身份鉴别需要验证组织的合法证件。

证书申请人需提交统一信用代码证、工商营业执照、事业单位法人证书与组织机构代码证书等证件之一，以及组织机构给经办人的授权和经办人的身份证件，向 eCardCA 提出申请。若该组织需申请设备类型证书，还需提交相关使用权证明文件。

eCardCA 或其 RA 可通过第三方验证或其他非现场方式明确组织身份，接受申请者通过传真、邮递、网络及其他认可的方式递交申请材料。

经办人经组织机构授权，通过邮寄或现场提交等方式，向 eCardCA 或其 RA 提交书面数字证书申请表以及下述组织机构的证明文件等申请资料，并缴纳相应的费用。

1．单位合法证件的复印件；

2．组织机构给经办人的授权书（须加盖公章）；

3．经办人有效身份证件的原件和复印件；

4．如该组织需申请设备类型证书，还需提交相关使用权证明文件。

以上各项证明文件需加盖申请单位的公章。

eCardCA 或其 RA 按照组织机构身份鉴别规范，对申请资料的原件和复印

件真实性进行审核，并进行批准申请或拒绝申请的操作。组织机构的身份鉴别规范简要说明了如何进行组织机构的身份鉴别。eCardCA 保留根据最新国家政策、法律、法规的要求更新组织机构身份鉴别规范的权利。

批准申请后，eCardCA 或其 RA 将保留相关盖单位公章的证明材料复印件，与证书申请表一并存档保存。

3.2.3 个人身份的鉴别

个人身份的鉴别可以使用以下有效的身份证件：居民身份证、港澳台居民身份证、户口簿、护照等。

对于证书申请业务，若数字证书申请表中有单位名称等单位信息时，数字证书申请表需要由该单位盖章，并需要提供单位身份的以下证明材料：由单位盖章的统一信用代码证、工商营业执照、事业单位法人证书与组织机构代码证书等证件之一。

个人到 eCardCA（或其 RA）受理点营业现场，向 eCardCA（或其 RA）提交书面数字证书申请表和上述有效身份证件的复印件等申请资料，并缴纳相关费用。

若申请人与证书持有人不是同一人时，还需提交申请人有效身份证件的原件（备查）与复印件。

eCardCA（或其 RA）按照个人身份鉴别规范对申请资料的原件和复印件真实性进行审核，并进行批准申请或拒绝申请的操作。个人身份的鉴别规范简要说明了如何进行个人身份鉴别。eCardCA 保留根据最新国家政策、法律、法规的要求更新个人身份鉴别规范的权利。

批准申请后，eCardCA（或其 RA）将保留复印件，与证书申请表一并存档保存。

3.2.4 设备身份的鉴别

设备身份的鉴别程序如下：

1. 提交以下申请材料：

(1) 填写完整的申请表；

(2) 订户的身份证件（参考前述组织机构、个人的身份证件要求）

(3) 订户授予经办人的授权证明（若经办人即订户本人，不需要）

(4) 经办人的个人身份证件（若经办人即订户本人，不需要）

(5) 产权证明文件（原件与复印件）

(6) 证书申请文件（CSR 或 REQ 文件）

2. eCardCA 对申请人的身份鉴别，可参考章节“3.2.2-3.2.3”相关内容；

3. eCardCA 检查设备的产权证明文件的复印件，并与原件进行比较，以确认对订户拥有设备的管理权。eCardCA 不确认产权证明文件的真实性与合法性；

4. eCardCA 对于证书申请文件的鉴别主要包含，文件中的信息是否与申请表中的申请信息一致，是否符合相关规范；

5. eCardCA 不对订户的设备进行验证。

3.2.5 域名的确认

如果证书名称是域名（或互联网 IP 地址），订户还需要额外提供域名（或互联网 IP 地址）使用权或所有权的证明材料，以确定申请者有权使用相应的域名（或互联网 IP 地址）。

eCardCA 还需采取其他独立的审查措施，以确认该域名（或互联网 IP 地址）的归属权，并要求申请者提供相应的协助。申请者不得拒绝这种要求。

3.2.6 没有验证的订户信息

订户提交证明文件以外的信息为没有验证的订户信息。

3.2.7 授权确认

为确保经办人具有特定的许可，代表组织机构或个人申请数字证书，需要出具组织机构或个人授权其办理数字证书事宜的授权文件。

组织机构或个人在 eCardCA 的数字证书申请表以及授权书上加盖单位公章或签名后，则证明本组织机构或个人对经办人的授权确认。

3.2.8 互操作准则

目前，eCardCA 未与其他电子认证服务机构建立交叉认证关系。

如果国家法律法规对此有规定，eCardCA 将严格予以执行。

3.3 密钥更新请求的身份标识与鉴别

3.3.1 密钥更新的标识与鉴别

订户密钥到期后需更新密钥，应向 RA 申请重新签发证书。在密钥更新过程中，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，eCardCA 使用订户原有公钥验证签名来进行订户身份的标识和鉴别。

3.3.2 注销后密钥更新的标识与鉴别

eCardCA 不提供证书被注销后的密钥更新。订户必须重新进行身份鉴别和注册。对身份标识和鉴别的要求，使用初始身份确认相同的流程（见“3.2.2 组织机构身份的鉴别”、“3.2.3 个人身份的鉴别” 、“3.2.4 设备身份的鉴别”、“3.2.5 域名的确认”）。

3.4 注销请求的标识与鉴别

3.4.1 订户注销申请

订户本人注销时的身份标识和鉴别使用初始身份确认相同的流程（见“3.2.2 组织机构身份的鉴别”、“3.2.3 个人身份的鉴别” 、“3.2.4 设备身份的鉴别”、“3.2.5 域名的确认”的相关规定）。

3.4.2 其他注销申请

如果是司法机关依法提出注销，eCardCA 将直接以司法机关书面的注销请求文件作为鉴别依据，不再进行其他方式的鉴别。

如果是因为订户没有履行 eCardCA-CPS 所规定的义务，由 RA 申请注销订户的证书时，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

本章阐述了 eCardCA 根据公布的 eCardCA-CPS 进行证书的申请、签发、管理、更新、注销等证书生命周期管理的全过程，以及在这些过程中各参与方的责任与义务。

4.1 证书申请

4.1.1 证书申请实体

证书申请实体包括企业单位、事业单位、政府机构、社会团体等各类组织机构与个人订户。

4.1.2 申请过程

证书申请流程简要说明如下：

1. 证书申请人按照 eCardCA-CPS 所规定的要求，通过在线方式或离线方式，填写证书申请表，并提交相关的身份证明材料；

2. eCardCA 或其 RA 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。

4.1.3 责任

申请过程中各方责任说明如下：

1.订户：按照 eCardCA-CPS 的要求准备证书申请材料，并确保申请材料真实准确。

2. eCardCA 或其 RA：负责接收并审核证书申请材料，对证书申请人所提供的证书申请信息与身份证明资料进行鉴别验证。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

eCardCA 或其 RA 按照见“3.2.2 组织机构身份的鉴别”、“3.2.3 个人身份的鉴别” 、“3.2.4 设备身份的鉴别”、“3.2.5 域名的确认”的相关规定进行身份鉴别。

4.2.2 证书申请批准和拒绝

4.2.2.1 证书申请的批准

eCardCA 或其 RA 根据 eCardCA-CPS 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 eCardCA-CPS 所规定的身份鉴别流程且鉴证结果为合格，eCardCA 或其 RA 将批准证书申请，为证书申请人制作并颁发数字证书。

4.2.2.2 证书申请的拒绝

证书申请人未能通过身份鉴别，eCardCA 或其 RA 将拒绝证书申请，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

eCardCA 或其 RA 将做出合理努力来尽快确认证书申请信息。一旦 RA 收到了所有必须的相关信息，将在 3 个工作日内处理证书申请。

eCardCA 或其 RA 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 eCardCA 的管理要求。

4.3 证书签发

4.3.1 证书签发过程中 eCardCA 的行为

eCardCA 在批准证书申请之后，将签发证书。证书的签发意味着 eCardCA 最终完全正式地批准了证书申请。

4.3.2 eCardCA 对订户的通告

eCardCA 通过 RA 通告订户，主要有以下几种方式：

1. 通过面对面的方式，通知订户到 RA 领取数字证书；
2. RA 把证书直接提交给订户，来通知订户证书信息已经正确生成；
3. 其他 eCardCA 认为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

在证书签发后，eCardCA 或其 RA 将证书本身，或者证书获得的方式，或者与证书相关的授权码，递送给证书申请人，证书申请人即被视为同意接受证书。

4.4.2 eCardCA 对证书的发布

eCardCA 签发的证书，通过证书服务系统发布到目录服务器中，供订户和依赖方查询和下载。

4.4.3 eCardCA 对其他实体的通告

其他实体可以通过从目录服务器查询 eCardCA 已经签发的数字证书。

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 eCardCA 所签发的证书后，均视为已经同意遵守与 eCardCA、依赖方有关的权利和义务的条款。订户接收数字证书后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。只有在接受了相关证书之后，订户才能使用对应的私钥。在证书到期或被注销之后，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

依赖方只能在合法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。证书的有效性验证应包括以下内容：

1. 使用 eCardCA 或其子 CA 的认证机构证书验证证书中的签名，确认该证书是 eCardCA 或其子 CA 签发的，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. 查询证书状态，确认该证书没有被注销。

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。在验证电子签名时，依赖方应准确知道什么数据已被签名；依赖方需了解电子签名认证证书的具体内容、证书有效期等证书内容，并核实证书当中的相关内容是否与申请表格所填写内容相符。

4.6 证书密钥更新

4.6.1 证书密钥更新概述

证书密钥更新指订户或其他参与者生成一对新密钥并申请为新公钥签发一个新证书。

4.6.2 证书密钥更新的情形

证书密钥更新的具体情形如下：

1. 因私钥泄漏而申请新的证书；
2. 证书无法继续获得信任；
3. 证书无法正常使用；
4. 证书介质丢失或损坏；
5. 证书密钥的有效期将要到期；
6. 其他需要更新证书密钥的情形。

4.6.3 请求证书密钥更新的实体

证书持有者、证书持有者的授权代表（例如，机构证书等）或者证书对应实体的拥有者（例如，设备证书等）可以请求证书密钥更新。

4.6.4 证书密钥更新请求的处理

对于证书密钥更新请求，由 eCardCA 或其 RA 来进行处理。

RA 对申请证书密钥更新的订户的身份进行鉴别与验证，鉴别要求见“3.2.2 组织机构身份的鉴别”、“3.2.3 个人身份的鉴别”、“3.2.4 设备身份的鉴别”、“3.2.5 域名的确认”。

4.6.5 颁发新证书时对订户的通告

同“4.3.2 eCardCA 对订户的通告”。

4.6.6 构成接受密钥更新证书的行为

同“4.4.1 构成接受证书的行为”。

4.6.7 eCardCA 对密钥更新证书的发布

同“4.4.2 eCardCA 对证书的发布”。

4.6.8 eCardCA 对其他实体的通告

同“4.4.3 eCardCA 对其他实体的通告”。

4.7 证书更新

4.7.1 证书更新概述

证书更新指在不改变证书中订户的公钥或原有证书申请信息的情况下，为订户签发一张新证书。

4.7.2 证书更新的情形

证书更新的具体情形如下：

1. 证书的有效期将要到期；
2. 其他需要更新证书的情形。

在证书更新时，若订户是基于有效期延续发起的证书更新业务，则证书密钥不更新。证书中其他信息项变化的时候，证书密钥需要更新。

4.7.3 请求证书更新的实体

证书持有者、证书持有者的授权代表（例如，机构证书等）或者证书对应实体的拥有者（例如，设备证书等）可以请求证书更新。

4.7.4 证书更新请求的处理

订户的证书更新请求，由 eCardCA 或其 RA 进行处理。RA 对申请证书更新的订户身份进行鉴别与验证，鉴别要求见“3.2.2 组织机构身份的鉴别”、“3.2.3 个人身份的鉴别”、“3.2.4 设备身份的鉴别”、“3.2.5 域名的确认”的相关规定。

4.7.5 颁发新证书时对订户的通告

同“4.3.2 eCardCA 对订户的通告”。

4.7.6 构成接受更新证书的行为

同“4.4.1 构成接受证书的行为”。

4.7.7 eCardCA 对更新证书的发布

同“4.4.2 eCardCA 对证书的发布”。

4.7.8 eCardCA 对其他实体的通告

同“4.4.3 eCardCA 对其他实体的通告”。

4.8 证书变更

4.8.1 证书变更概述

在证书有效期内，当证书信息发生变化，订户或者其它参与者可以选择证书变更，保留原有公钥，申请签发新的证书。

4.8.2 证书变更的情形

证书变更指改变证书中除订户公钥之外的信息而签发新证书的情形。当订户实体身份信息发生改变，而影响证书项内容时，订户可以向 eCardCA 申请证书变更。

4.8.3 请求证书变更的实体

证书持有者、证书持有者的授权代表（例如，机构证书等）或者证书对应实体的拥有者（例如，设备证书等）可以请求证书变更。

4.8.4 证书变更请求的处理

对于订户的证书变更请求，由 eCardCA 或其 RA 来进行处理。

RA 对申请证书变更订户的身份进行鉴别与验证，鉴别要求见“3.2.2 组织机构身份的鉴别”、“3.2.3 个人身份的鉴别”、“3.2.4 设备身份的鉴别”、“3.2.5 域名的确认”的相关规定。

4.8.5 证书变更时对订户的通告

同“4.3.2 eCardCA 对订户的通告”。

4.8.6 构成接受变更证书的行为

同“4.4.1 构成接受证书的行为”。

4.8.7 eCardCA 对变更证书的发布

同“4.4.2 eCardCA 对证书的发布”。

4.8.8 eCardCA 对其他实体的通告

同“4.4.3 eCardCA 对其他实体的通告”。

4.9 证书注销

4.9.1 证书注销的情形

发生下列情形之一的，订户应当申请注销数字证书：

1. 数字证书私钥安全已经受到损害；
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 eCardCA-CPS；
4. 政务机构的证书持有者工作性质发生变化。

发生下列情形之一的，eCardCA 可以注销其签发的数字证书：

1. 订户申请注销数字证书；
2. 订户提供的信息不真实；
3. 订户没有或无法履行双方合同规定的义务；
4. 数字证书的安全性得不到保证；
5. 政务机构的证书持有者受到国家法律法规制裁；
6. 证书仅用于依赖方主导的系统并由依赖方提出撤销申请；
7. 法律、法规规定的其他情形。

4.9.2 请求证书注销的实体

根据不同的情况，订户、eCardCA、RA、订户所属组织机构或证书使用唯一依赖方可以请求注销订户证书。

4.9.3 注销请求的流程

证书注销请求的处理流程如下。

1. 证书注销的申请人通过在线方式或离线方式发起撤销申请，并注明注销原因，订户需依据 eCardCA 要求填写《证书注销申请表》；
2. eCardCA 或其 RA 根据“3.2 初始身份确认”关于通用数字证书的相关规定，对订户提交的注销请求进行身份鉴别与审核，以确认注销请求是订户本人提交或已得到了订户的授权；
3. eCardCA 注销订户证书后，RA 将通知订户证书被注销，订户的数字证书在 24 小时内进入 CRL，向外界发布。

4.9.4 注销请求宽限期

如果出现私钥泄露等事件，订户发现泄露或有泄露嫌疑应及时提出注销请求。其他注销原因的注销请求必须在 48 小时内提出。

4.9.5 eCardCA 处理注销请求的时限

eCardCA 接到注销请求后实时进行处理。eCardCA 每日签发一次 CRL，并将最新的 CRL 发布到证书服务系统的目录服务器，供请求者查询下载。

4.9.6 依赖方检查证书注销的要求

依赖方应验证 CRL 的可靠性和完整性，确保是经 eCardCA 发布并且签名的。依赖方可以使用以下两种方式查询所依赖证书的证书状态：

1. CRL 查询：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）：eCardCA 接受证书状态查询请求，查询证书的实时状态。查询结果经过签名后，返回给请求者。

4.9.7 CRL 发布频率

eCardCA 的 CRL 的发布周期为 24 小时。

4.9.8 CRL 发布的最大滞后时间

发布的最长滞后时间为 24 小时。

4.9.9 在线状态查询的可用性

eCardCA 向订户和依赖方提供在线证书状态查询服务（OCSP 服务）。

4.9.10 在线状态查询要求

依赖方是否进行在线状态查询完全取决于应用的安全要求。

对于安全保障要求高并且完全依赖数字证书进行身份鉴别与授权的应用，依赖方在信赖证书前，必须通过证书状态在线查询检查该证书的状态。

4.9.11 注销信息的其他发布形式

除了 CRL、OCSP 外，eCardCA 暂不提供注销信息的其他发布形式。

4.9.12 密钥损害的特别要求

无论是最终订户还是 eCardCA 或其授权的 RA，发现证书密钥受到安全损害时，应立即注销证书。

4.10 证书冻结

4.10.1 证书冻结的情形

证书冻结是证书注销的一种特殊情形，由于某种原因暂停使用证书。例如：订户由于某种原因如长期出差，短期内无法使用证书，可以申请证书冻结。

4.10.2 请求证书冻结的实体

请求证书冻结的实体包括：证书有效期限未到的订户本人或其授权代表、eCardCA 或其授权机构的授权代表、司法机关等公共权力部门的授权代表。

4.10.3 冻结请求的流程

申请者以在线或离线方式向 eCardCA 或其 RA 提交证书冻结申请，并注明冻结的原因。eCardCA 授权的 RA 按照“3. 身份标识与鉴别”相关规定对订户提交的证书冻结申请进行鉴别与验证。

如需要强制冻结，RA 的管理员可以依法对数字证书进行强制冻结。冻结后必须立即通知该证书订户。强制冻结的命令来源于：司法机关、eCardCA 或 eCardCA 授权的 RA。

eCardCA 冻结订户证书后，RA 将通过发送 E-mail 邮件等方式通知订户证书被冻结。

4.10.4 冻结的期限限制

订户证书被冻结后，订户必须在证书有效期到期前恢复证书，否则 eCardCA 或 eCardCA 授权的 RA 有权自行撤销证书。对此造成的任何后果，eCardCA 不负责任。

4.10.5 eCardCA 处理冻结请求的时限

eCardCA 接到冻结请求后实时进行处理。eCardCA 每日签发一次 CRL，并将最新的 CRL 发布到证书服务系统的目录服务器，供请求者查询下载。

4.10.6 依赖方检查证书冻结的要求

同“4.9.6 依赖方检查证书注销的要求”。

4.10.7 CRL 发布频率

同“4.9.7 CRL 发布频率”。

4.10.8 CRL 发布的最大滞后时间

同“4.9.8 CRL 发布的最大滞后时间”。

4.10.9 在线状态查询的可用性

同“4.9.9 在线状态查询的可用性”。

4.10.10 在线状态查询要求

同“4.9.10 在线状态查询要求”。

4.10.11 冻结信息的其他发布形式

除了 CRL、OCSP 外，eCardCA 暂不提供冻结信息的其他发布形式。

4.11 证书解冻

4.11.1 证书解冻的情形

证书解冻是指订户在证书冻结的情况下，可以申请证书解冻，恢复并使用原有证书。

4.11.2 请求证书解冻的实体

请求证书解冻的实体包括：证书有效期限未到，但已经冻结证书的订户本人或其授权代表、eCardCA 或其授权机构的授权代表、司法机关等公共权力部门的授权代表。

4.11.3 解冻请求的流程

申请者以在线或离线方式向 eCardCA 或其 RA 提交证书解冻申请，并注明解冻的原因。eCardCA 授权的 RA 按照“3. 身份标识与鉴别”相关规定对订户提交的证书解冻申请进行鉴别与验证。

如需要强制解冻，RA 的管理员可以依法对数字证书进行强制解冻。解冻后必须立即通知该证书订户。强制解冻的命令来源于：司法机关、eCardCA 或

eCardCA 授权的 RA。

eCardCA 解冻订户证书后，RA 将通过发送 E-mail 邮件等方式通知订户证书被解冻。

4.11.4 解冻的期限限制

订户必须在证书有效期内申请证书解冻业务，否则 eCardCA 或 eCardCA 授权的 RA 有权自行撤销证书。对此造成的任何后果，eCardCA 不负责任。

4.11.5 eCardCA 处理解冻请求的时限

eCardCA 接到解冻请求后实时进行处理。eCardCA 每日签发一次 CRL，并将最新的 CRL 发布到证书服务系统的目录服务器，供请求者查询下载。

4.11.6 依赖方检查证书解冻的要求

同“4.9.6 依赖方检查证书注销的要求”。

4.11.7 CRL 发布频率

同“4.9.7 CRL 发布频率”。

4.11.8 CRL 发布的最大滞后时间

同“4.9.8 CRL 发布的最大滞后时间”。

4.11.9 在线状态查询的可用性

同“4.9.9 在线状态查询的可用性”。

4.11.10 在线状态查询要求

同“4.9.10 在线状态查询要求”。

4.11.11 解冻信息的其他发布形式

除了 CRL、OCSP 外，eCardCA 暂不提供解冻信息的其他发布形式。

4.12 证书状态服务

4.12.1 操作特征

eCardCA 通过目录服务器和证书在线状态查询服务系为订户提供证书状态服务。

4.12.2 服务可用性

原则上，eCardCA 提供 7×24 小时的证书状态查询服务，即在网络以及电力供应允许的情况下，每天订户能够实时获得证书状态查询服务。

4.12.3 可选特征

无。

4.13 终止使用

终止使用是指当证书有效期满或证书注销后，该证书的服务时间结束。

下列情况视为证书持有者终止使用 eCardCA 提供的证书服务：

1. 证书到期后，订户不再延长证书使用期或者不再重新申请证书，则可以自动终止与 eCardCA 的服务；
2. 在证书有效期内，证书持有者提出终止服务，即服务终止。

4.14 密钥生成、备份与恢复

4.14.1 密钥生成、备份与恢复的策略与行为

4.14.1.1 密钥生成策略与行为

订户的签名密钥对由订户的密码设备生成，加密密钥对由密钥管理中心生成。

4.14.1.2 密钥托管策略与行为

签名密钥对由订户的密码设备保管。加密密钥对由订户的密码设备保管，同时，密钥管理中心保存有加密密钥对的备份数据，以便于密钥恢复。

4.14.1.3 密钥恢复策略与行为

密钥恢复是指加密密钥对的恢复，密钥管理中心不负责签名密钥对的恢复。密钥恢复分为两类：订户密钥恢复和司法取证密钥恢复。

1. 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。订户向 eCardCA 申请进行密钥恢复。经审核后，通过 eCardCA 向密钥管理中心请求密钥恢复；密钥管理中心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。

2. 司法取证密钥恢复

司法取证人员向 eCardCA 申请。由 eCardCA 的业务人员根据司法机关的书面材料，生成司法取证密钥恢复申请。经审核后，由密钥管理中心恢复所需的密钥并记录于特定载体中。

5 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

eCardCA 的机房建设按照下列标准实施：

1. GM/T 0034-2014《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》；
2. GM/T 0037-2014《证书认证系统检测规范》；
3. GM/T 0038-2014《证书认证密钥管理系统检测规范》；
4. GB 50174-2008《电子信息系统机房设计规范》；
5. GB/T 2887-2011《计算机场地通用规范》；
6. GB/T 9361-2011《计算机场地安全要求》；
7. GB/T 12190-2006《电磁屏蔽室屏蔽效能的测量方法》；
8. BMB3-1999《处理涉密信息的电磁屏蔽室的技术要求和测试方法》；
9. GB 50016-2014《建筑设计防火规范(附条文说明)》；
10. GB50019-2003《采暖通风与空气调节设计规范(附条文说明)》；
11. GB 50034-2013《建筑照明设计标准(附条文说明)》；
12. GB 50052-2009《供配电系统设计规范(附条文说明)》；
13. GB 50054-2011《低压配电系统设计规范(附条文说明)》；
14. GB 50198-2011《民用闭路监视电视系统工程技术规范(附条文说明)》；
15. GB 50222-1995《建筑内部装修设计防火规范(2001 年版)(附条文说明)》；
16. GB 50243-2002《通风与空调工程施工及验收规范(附条文说明)》；

17. GB 50303-2002《建筑电气工程质量验收规范(附条文说明)》;

18. GB50311-2007《综合布线系统工程设计规范(附条文说明)》;

19. GB 50312-2007《综合布线系统工程验收规范(附条文说明)》;

20. GB50314-2015《智能建筑设计标准》;

21. GB 50339-2013《智能建筑工程质量验收规范(附条文说明)》;

22. GB 50343-2012《建筑物电子信息系统防雷技术规范(附条文说明)》;

23. GA/T75-1994《安全防范工程程序与要求》;

24. GA308-2001《安全防范系统验收规则》。

eCardCA 机房位于长沙国家高新开发区中电软件园 18 号楼，实行分区访问的安全管理：

eCardCA 机房的功能区域划分为 CA 核心区（屏蔽机房）、CA 管理终端区、CA 服务器区、制证区、配电区等区域。

CA 核心区位于屏蔽机房内，具有最高的安全级别。屏蔽机房设置了非接触 IC 卡指纹门禁系统，并设置了“双人同进、双人同出”策略，即需要两个持有相应 IC 卡的管理人员同时刷卡，方可进入该区域。

其它区域的进入权限授权给不同的管理人员，不能有一个管理人员可单独进入多个区域的情况。

5.1.2 物理访问

为了保证 CA 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：

1. 门禁系统：控制各层门的进出。工作人员需使用身份识别卡与指纹鉴定才能进出，进出每一道门均有时间记录和信息提示。
2. 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，均会触发报警系统。报警系统明确指出报警位置。
3. 监控系统：监控系统对安全区域和操作区域进行 24 小时不间断录像，系统保留录像资料，以备查询。

门禁和物理侵入报警系统备有 UPS，并提供至少 8 小时的不间断供电。

5.1.3 电力与空调

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统。按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。

目前，eCardCA 采用“双路市电+双路 UPS 不间断电源”来保证供电的稳定性和可靠性，维持系统正常运转。eCardCA 的市电由中电软件园的市电接入供电，中电软件园的市电提供了双市电供电，在第一路市电停电的情况下，将自动切换到第二路市电供电。UPS 断电续航时间为 8 小时。

根据机房环境及设计规范要求，机房内设置了空气调节系统。空气调节系统包括空调、通风管路、新风系统。

eCardCA 对 CA 系统的电源、空调等设施，严格参照相关设施管理的规定进行维护和保养，而且每年对其是否符合要求进行检查。

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。

eCardCA 的系统有充分保障，能够防止水侵蚀。

5.1.5 火灾防护

火灾预防与保护措施主要包括以下六个方面：

1. 敏感区、高度敏感区域，其建筑物的耐火等级符合 GB 50016-2014 的规定；
2. eCardCA 的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、以及易燃物附近部位设置烟、温感探测器；
3. CA 核心区、CA 服务器区、配电区配置独立的气体灭火装置，使用专业的灭火系统，备有相应的气体灭火器。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；
4. 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设施。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；

5. 在非敏感区及敏感区的办公区域内，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。紧急出口门需与门禁报警设备联动。

灭火系统采用电动，手动，紧急启动三种方式：

1. 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；
2. 手动方式：人员对钢瓶或药剂瓶直接开启操作；
3. 紧急启动：防护区外设有紧急启动按钮供紧急时使用。

eCardCA 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

数据的存储介质包括硬盘、软盘、磁带、光盘等，介质存储地点和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 eCardCA 存档的敏感数据或密钥已不再需要或存档期限已满时，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；保存在磁盘的，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复方式进行相应的销毁处理。

5.1.8 异地备份

eCardCA 定期进行数据备份，备份数据保存于指定的银行保险箱。

5.2 程序控制

5.2.1 可信角色

eCardCA 或其授权的 RA、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，由可信人员担任。

eCardCA 明确规定 CA 关键职能的职位，主要包括但不限于以下部分：

1. 安全策略委员会主任
2. 可信人员管理员

3. 安全管理员
4. 物理环境安全管理员
5. 密钥管理员
6. 运行维护管理员
7. CA 系统管理员
8. 系统维护管理员
9. 数据库管理员
10. 网络管理员
11. 运行审计管理员
12. 鉴别与验证员
13. 信息录入员
14. 信息审核员
15. 档案管理员
16. 其他。

eCardCA 根据《电子认证服务机构从业人员岗位技能规范》等标准规范与 eCardCA-CPS 的要求，制订其授权的 RA（RA 等）的管理规范，规范 RA 和服务系统的管理人员、操作人员的操作。在与此相关的软件设计中，充分考虑安全的限制与约束。eCardCA 对授权的 RA 的责任进行合理划分，并通过系统和技术实现以及管理的责任义务上进行保证。

5.2.2 每项任务需要的人数

eCardCA 对与运行和操作相关的职能有明确的分工，贯彻职责分割、多人控制、互相牵制和最小权益的安全管理原则。

访问和管理 CA 的加密设备及密钥，至少需要 3 个可信人员。

对于证书的申请鉴别和签发，需要 3 个可信人员操作完成。

对于重要的系统操作与维护，eCardCA 通常会安排一人进行操作，一人进行监督记录。

5.2.3 每个角色的识别与鉴别

所有 eCardCA 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指纹识别；进入系统需要使用数字证书进行身份鉴别。

eCardCA 将独立完整地记录其所有的操作行为。

5.2.4 需要职责分割的角色

需要进行职责分割的角色，包括但不限于下列人员：

1．从事证书申请信息验证的人员；

2．负责证书申请、撤销、更新和信息注册等服务请求的批准、拒绝或其他操作的人员；

3．负责证书签发、撤销等工作或者能够访问受限、敏感信息的人员；

4．负责处理订户信息的人员；

5．负责生成、签发和销毁 CA 系统证书的人员；

6．负责密钥及密码设备管理、操作人员。

对于证书服务的受理，应通过录入员、审核员、制证员 3 个角色才能完成。

对于 CA 密钥的操作，必须有 3 名以上的 CA 密钥管理员同时到场，才能进行有关操作。

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 eCardCA 签订保密协议。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。eCardCA 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 eCardCA 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

eCardCA 与有关的政府部门和调查机构合作，完成对 eCardCA 的可信任人员的背景调查。

所有目前的可信任人员和申请调入的可信任人员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：

1. 人事部门负责对应聘人员的个人资料予以审查与确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等有效证明；
2. 人事部门通过电话、信函、网络、走访等形式对应聘人员提供的材料的真实性进行鉴定；
3. 用人部门通过现场考核、日常观察、情景考验等方式对应聘人员进行考察；
4. 经考核，人事部门和用人部门联合填写《可信人员调查表》，报主管领导批准后准予上岗。

5.3.3 培训要求

eCardCA 对所有人员按照其岗位和角色安排不同的培训。培训内容主要包括但不限于：

1. eCardCA 的安全原则和机制、岗位职责；
2. 电子认证系统相关软、硬件的安装与维护；
3. 电子认证系统的操作与使用；
4. eCardCA 的业务管理相关的流程、标准与规范；
5. eCardCA 的运行管理相关的规章、制度与管理办法；
6. 国家关于电子认证的法律法规与政策；
7. 其他必要的培训。

对于运营人员，有关 CA 的相关知识与技能，每年至少要总结一次并由 eCardCA 组织培训。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。

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 eCardCA 一次以上的培训。认证策略调整、系统更新时，须对相关人员进行再培训，以适应新的变化。

5.3.5 工作轮换周期和顺序

eCardCA 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。

工作轮换遵循国家电子认证服务管理相关规范要求的职责分割的要求。

5.3.6 未授权行为的处罚

当 eCardCA 的员工被怀疑，或者已进行了未授权的操作，例如，滥用权利或进行越权操作，eCardCA 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。对于情节严重的，依法追究相应责任。

5.3.7 独立合约人的要求

对不属于 eCardCA 内部工作人员，但将从事 eCardCA 有关业务的独立签约者，eCardCA 的统一要求如下：

1. 对人员档案进行备案管理；
2. 必须签署保密协议；
3. 必须接受 eCardCA 组织的相关知识与安全规范的培训；
4. 由 eCardCA 派专人监督和陪同从事相关的工作。

5.3.8 提供给员工的文档

为使系统正常运行，必须提供给具有权限的相关人员各种文档，主要包括（但不限于）：

1. 认证系统相关软、硬件的操作手册，例如，认证系统操作手册、密码设备订户手册、目录服务器安装配置说明文件等；
2. 电子认证业务规则与相关的协议和规范；
3. 系统运行与维护相关的流程、管理办法，例如，机房设备管理办法；
4. 电子认证服务相关的宣传资料；
5. 内部操作文件，例如，灾难备份和恢复方案；
6. 其他文档。

5.4 审计日志程序

5.4.1 记录事件的类型

eCardCA 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。主要包括但不限于：

1. 订户服务申请和注销的申请表、协议、身份证明材料和其他相关信息等；
2. 电子认证系统密钥的生成、变化等记录；
3. 电子认证系统自身密钥的生成、配置、更新等成功和失败的记录；
4. 电子认证系统日常运行产生的各类日志记录；
5. CRL 操作记录；
6. 进出 eCardCA 控制区域的表格、门禁卡进出敏感区域的记录、机房工作日志、系统日常维护记录、监控录像等；
7. 系统软硬件设备上线、更换、下线等记录；
8. 其他与系统不直接相关的事件，例如，人事变动等。

5.4.2 处理日志的周期

eCardCA 定期对日志进行审查，并对审查日志的行为进行备案。每年进行的审查不少于 2 次。

5.4.3 审计日志的保存期限

eCardCA 的审计日志保存期限不少于 5 年。

5.4.4 审计日志的保护

eCardCA 执行严格的管理，确保只有 eCardCA 授权的人员才能对审计日志进行相应操作。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。

5.4.5 审计日志备份程序

eCardCA 保证所有的审计日志和审查总结都按照 eCardCA 备份标准和程序进行备份。根据记录的性质和要求按月进行备份，可采用在线和离线两种方式备份。

5.4.6 审计日志收集系统

审计日志收集系统涉及：

1. 证书管理系统；
2. 证书注册管理系统；
3. 证书服务系统；
4. 证书在线业务门户；

5. 网站、数据库安全管理系统；

6. 其他需要审计的系统。

eCardCA 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

eCardCA 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，eCardCA 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、提交司法部门处理等措施。

eCardCA 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

eCardCA 不定期对系统进行脆弱性评估，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

eCardCA 对以下记录（包括但不限于）进行归档保存：

1. 电子认证系统的建设和升级文档；
2. 证书业务申请信息、证书业务申请的批准与拒绝的信息、与订户的协议、证书和 CRL 等；
3. 系统运行所产生的日志；
4. 电子认证服务规划、各类服务规范和协议、规章制度、管理办法等；
5. 认证系统的数据库数据；
6. 人员进出记录和第三方人员服务记录；
7. 监控录像；
8. 员工资料，包括背景调查、录用、培训等资料；
9. 各类外部、内部审核评估文档。

5.5.2 归档记录的保存期限

除了法律法规和管理部门提出的保存期限外，eCardCA 对与证书相关的归档记录（监控录像除外，监控录像的保存期限为 3 个月）至少保存到证书有效期结束后 5 年。与法律政策的规定不一致时，选择两者中较长的期限予以保存。

此外，在不违反法律法规和管理部门的规定的前提下，eCardCA 可以自主

决定信息的存档期限，并不对此做出说明和解释。

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。eCardCA 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。

eCardCA 保存的证书业务申请信息、订户基本情况和身份鉴别资料，非政府主管机构或司法机构经过合法途径予以申请，任何无关的第三方均无法获知。

5.5.4 归档文件的备份程序

所有存档的文件和数据库除了保存在 eCardCA 的存储库，还在从银行租赁的保险柜中保存其备份。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。

5.5.5 记录时间戳要求

对于电子归档记录，eCardCA 暂不采用时间戳技术；归档记录包含归档的具体年限和日期；

对于纸质归档记录，归档材料包含归档的具体年限和日期。

5.5.6 归档收集系统

认证系统的相关运营信息，由 eCardCA 的工作人员或者具备完全控制措施的内部系统，依照人工和自动操作两部分进行产生的收集，并且由具备相关权限的人进行管理和分类。

5.5.7 获得和检验归档信息的程序

eCardCA 每年会组织专人检验归档信息的完整性，也可根据业务需求不定期进行检查验证。

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时，eCardCA 将生成新的 CA 签名密钥对，并对教育卡人员身份鉴权 CA 证书、教育电子证件人员身份鉴权 CA 证书进行更新。

在生成新的 CA 签名密钥对时，须严格遵守 eCardCA 关于密钥管理的规范。新的密钥对产生后，使用国家密码主管部门签发给 eCardCA 的 CA 证书进行签

发，生成新的教育卡人员身份鉴权 CA 证书、教育电子证件人员身份鉴权 CA 证书。eCardCA 及时进行发布。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

发生故障时，eCardCA 将按照灾难恢复计划实施恢复。

5.7.2 计算机资源、软件和/或数据被破坏

eCardCA 遭到攻击，发生通信网络资源毁坏、计算机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，eCardCA 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 eCardCA 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，eCardCA 采用如下措施处理：

1. 立即向电子认证服务主管部门和其他政府主管部门汇报，通过网站和其他公共媒体对订户进行通告，采取措施保证订户利益不受损失；
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，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 eCardCA-CPS 关于证书签发的规定，重新签发下级证书和订户证书；
4. 新的根证书签发以后，将立即通过 eCardCA 的信息库、目录服务器、门户网站等方式进行发布。

订户的私钥出现损毁、遗失、泄露、破解、被篡改、或者有被第三者窃用的疑虑时，订户应按照 eCardCA-CPS 的规定，首先申请吊销证书，然后按照规定重新申请新的证书。

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备份方式；对核心数据库，证书管理系统数据库采用离线备份方式来确保业务连续性。

发生自然或其它不可抗力性灾难后，eCardCA 可采用备份恢复方式对运营进行恢复。具体的安全措施按照 eCardCA 灾难恢复计划实施。

5.8 电子认证服务机构或其 RA 的终止

因各种情况，eCardCA 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。

在 eCardCA 终止前必须：

1. 在暂停或者终止服务九十日前，就业务承接及其他有关事项向主管机构、证书持有者以及其他所有相关实体进行通告；
2. 安排业务承接；
3. 保存所有的认证服务相关运营资料，包括（但不限于）证书、订户信息、系统文件、CPS、规范与协议等；
4. 停止有关运营服务；
5. 清除系统根密钥；
6. 清除 eCardCA 主机硬件。

当 eCardCA 授权的 RA 因故终止服务时，eCardCA 将按照与其签订的相关协议处理有关业务承接事宜与其他事项。因 RA 故终止服务时，eCardCA 将按照与 RA 签订的相关协议处理有关业务承接事宜与其他事项。

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

6.1.1.1 CA 密钥对的生成

CA 密钥对由加密机独立生成，加密机部署在屏蔽机房当中，密钥管理人员只能在屏蔽机房中对 CA 密钥对进行操作。

6.1.1.2 订户密钥对的生成

订户的签名密钥对由订户的密码设备生成，加密密钥对由密钥管理中心生成。

6.1.2 私钥传送给订户

订户的签名密钥对由订户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的密码设备。

6.1.3 公钥传送给证书签发机构

订户的签名公钥通过安全通道，经证书注册管理系统传递到证书管理系统。订户的加密公钥，由密钥管理中心通过安全通道传递到证书管理系统。

从证书注册管理系统到证书管理系统以及从密钥管理系统到证书管理系统的传递过程中，采用国家密码管理局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 eCardCA 的网站上下载认证机构证书，从而得到 eCardCA 的公钥。

6.1.5 密钥的长度

eCardCA 签发的所有证书，均支持 SM2 算法。SM2 非对称密钥对的长度是 256 比特。

如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，eCardCA 将会完全遵从。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理局许可的密码设备产生。

公钥参数质量的检查同样通过国家密码管理局许可的密码设备进行。

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

eCardCA 所用的密码设备都是经国家相关部门认可的产品，其安全性达到以下要求。eCardCA 所采用密码模块符合国家密码行业相关技术标准。

6.2.2 私钥的多人控制

CA 密钥对的生成、更新、注销、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 张密钥卡中，只有其中 3 至 5 人在场并许可的情况下，才能对私钥进行上述操作。

订户私钥由订户自己通过密码设备控制。

6.2.3 私钥托管

订户加密私钥由密钥管理中心托管，订户的签名私钥由自己保管，密钥管理中心不负责托管。

密钥管理中心严格保证订户加密密钥对的安全，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

eCardCA 的密钥管理中心仅负责订户的加密密钥备份，备份数据以密文形式保存。

6.2.5 私钥归档

订户密钥对的归档是将已过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。

eCardCA 提供过期的托管加密密钥归档服务。

6.2.6 私钥导入、导出密码模块

1. 对于 CA 私钥，应严格按照 CA 密钥管理规范进行备份。除此之外的任何导入导出操作均不被允许。当 CA 私钥备份到另外的硬件密码模块时，以加密形式在模块间传送，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、泄漏、非授权的使用等风险；

2. 对于订户私钥，eCardCA 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 私钥在密码模块中的存储

1. CA 私钥安全存储在国家密码主管部门批准和许可的硬件密码设备中

2．订户私钥在硬件密码模块（智能密码钥匙、教育卡芯片或教育电子证件芯片）中加密保存。

6.2.8 激活私钥的方法

1．对于 CA 私钥，其激活数据按第 6.2.2 节进行分割，并且保存在 IC 卡等硬件介质中，必须采用 M 选 N 的方式分别输入激活数据才能激活私钥；

2．对于订户私钥，存放在硬件密码模块中，订户可以通过 PIN 进一步保护。当订户输入正确的 PIN，则私钥被激活。

6.2.9 解冻私钥的方法

1．对于 CA 私钥，必须采用 M 选 N 的方式，由具有相关权限的密钥管理员登录密码设备，共同启动密钥管理程序，进行解冻私钥的操作；

2．对于订户私钥，由订户自行决定。当订户从系统中退出（或将硬件密码模块从设备上断开），私钥就被解冻。

6.2.10 解除私钥激活状态的方法

私钥不再使用，不需要保存时，应将私钥销毁，以避免丢失、偷窃、泄露或非授权使用。

对于订户的加密私钥，在其生命周期结束后，由密钥管理中心妥善保存一定期限，以便解密加密信息。对于订户的签名私钥，在其生命周期结束后，若无需保存，由订户自行决定其销毁方法。

对于 CA 私钥，在其生命周期结束后，将 CA 私钥进行归档保存，并将其他的备份数据销毁。

6.2.11 销毁密钥的方法

具有销毁密钥权限的管理员使用含有自己身份的密码设备登录，启动密钥管理程序，进行销毁密钥的操作，需要 3 名管理员同时在场。

6.2.12 密码模块的评估

eCardCA 使用国家密码主管部门批准和许可的密码设备。根据 eCardCA 对密码设备的性能、供应厂商的资质等方面的评估，选择需要的密码模块。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

eCardCA 将 CA 证书和订户证书归档。归档的证书存放在数据库中。

6.3.2 证书操作期和密钥对使用期限

1. 对于签名证书，其私钥只能在证书有效期内使用。在数字签名验证的应用场合，为验证在证书有效期内生成的签名信息，公钥的使用期限可以在证书有效期以外；在身份鉴别的应用场合，公钥的使用期限必须在证书有效期以内；

2. 对于加密证书，其公钥只能在证书有效期内使用。为保证在证书有效期内加密的信息可以解密，私钥的使用期限可以在证书有效期以外。

6.4 激活数据

6.4.1 激活数据的产生和安装

1. CA 私钥的激活数据，必须按照关于密钥激活数据分割和密钥管理办法的要求，严格进行生成、分发和使用。

2. 订户私钥的激活数据，设置了缺省的 PIN。订户在接受证书后，应及时修改 PIN。

6.4.2 激活数据的保护

1. 对于 CA 私钥的激活数据，必须通过密钥分割将分割后的激活数据由不同的密钥管理员掌管。密钥管理员必须符合可信人员管理和职责分割的要求，签署协议确认他们知悉密钥管理员的责任；

2. 对于订户私钥的激活数据，订户应妥善保管好，防止泄露或窃取，并应经常对激活数据进行修改。

6.4.3 激活数据的其他方面

只有在拥有订户密码设备并知道 PIN 值时才能激活证书存储介质，进而使用私钥。

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：

1. 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；
2. 对设备定期进行检查、清洁和保养维护；
3. 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；
4. 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。

6.5.2 计算机安全评估

eCardCA 已通过国家密码管理局组织的安全性审查。

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

eCardCA 的信息安全管理，严格遵循国家相关主管部门的有关运行规范和 eCardCA 的安全管理策略进行操作。

eCardCA 的使用具有严格的控制措施，所有和系统都经过严格的测试验证后才进行使用。任何修改和升级均记录在案并进行版本控制、功能测试和记录。eCardCA 还对认证系统进行定期和不定期的检查与测试。

eCardCA 采取严格的管理体系来控制和监视系统的配置，以防止未授权的修改。

6.6.3 生命期的安全控制

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国家密码管理局的鉴定与安全性审查，使用基于标准的强化安全通信协议以确保通信数据的安全；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运行的安全。eCardCA 采用多级防火墙、病毒防治、入侵检测、漏洞扫描等网络安全防护措施，并及时更新各网络安全设备的版本，以尽可能降低来自网络的风险。

6.8 时间戳

eCardCA 暂不采用时间戳技术。

7 证书、证书注销列表和在线证书状态协议

7.1 证书

7.1.1 证书格式

eCardCA 签发的通用数字证书符合 X.509 证书格式。

7.1.2 版本号

其版本号为：X.509 V3。

7.1.3 证书扩展项

eCardCA 支持使用证书标准项和标准扩展项。

1. 密钥用途。主要包括：电子签名，不可抵赖，密钥加密、数据加密、密钥协议、验证证书签名、验证 CRL 签名、只加密、只解密、只签名等；
2. 证书策略。eCardCA 签发的证书策略，符合 X.509 证书格式，这一策略信息存放在证书策略属性栏；
3. 基本限制。用于鉴别证书持有者身份；

4. CRL 发布点。系统定义的 CRL 发布点。

7.1.4 算法对象标识符

证书使用 SM3withSM2 算法，算法标识为 1.2.156.10197.1.501。

7.1.5 名称形式

eCardCA 签发的通用 X.509 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。

主体 Subject 的 X.500 DN 支持多级 OU，其格式如下：

C=CN;
OU=XX；
OU=××；
OU=××;
OU=××;
CN=××;

C（Country）应为 CN，表示中国。

OU（Organization Unit）应为证书主体或者证书主体所属单位的名称全称；

CN（Common Name）中的内容分为 4 种：

1. 个人证书中应为证书主体的姓名；
2. 法人证书中应为证书主体单位的名称或企业税务登记号；
3. 设备证书应为证书主体设备的域名或者 IP 地址；
4. 专网证书中应为证书主体单位的内部名称。

7.1.6 名称限制

证书名称的使用采用实名制，要求证书名称与证书持有者所提交的各种证件原件、复印件、证明材料、印鉴等必须相符。

7.1.7 证书策略对象标识符

证书基本对象标识符可包含证书序列号、证书主题、证书状态、证书有效期等内容；证书附加对象标识符可包含证书所对应的订户信息，如订户名、电子邮件地址等内容；每个证书模版均可根据证书对象按文件字节限定的范围内，按照管理策略的要求自定义的扩展项进行标识符的内容加载。

7.1.8 策略限制扩展项的用法

系统策略中设定的扩展项结果分页返回条数，查询结果可进行分页显示，以支持海量数据的查询，减轻系统的负担。

教育卡人员身份鉴权证书、教育电子证件人员身份鉴权证书不支持策略限制扩展项。

7.1.9 策略限定符的语法和语义

遵照国家规范的语法和语义进行编写录入。

7.1.10 关键证书策略扩展项的处理规则

根据应用场合的要求，需要对关键证书扩展项的添加、删除、修改操作进行评估和审查，以判断这些操作的必要性、正确性、规范性和合法性。

7.1.11 证书策略

证书策略命名的一组规则，指出证书对具有公共安全要求的特定团体和/或应用的适用范围，eCardCA 所签发证书的策略扩展项中，包含证书策略 OID，说明当前证书只能在该证书策略所指定的范围内使用，其中 certificatePolicies:policyIdentifier 设置为 anyPolicy。

7.2 证书注销列表

eCardCA 签发的证书注销列表符合 X.509 V2 格式。

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。

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

eCardCA 为订户提供在线证书状态查询服务（OCSP 服务）。

7.3.1 版本号

使用 OCSP 版本 1（OCSP v1）。

7.3.2 OCSP 扩展项

目前未使用 OCSP 扩展项。

8 认证机构审计和其他评估

8.1 评估的频率或情形

审计是为了检查、确认 eCardCA 是否按照 eCardCA-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。审计分内部审计和外部审计。

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

外部审计由 eCardCA 委托第三方审计机构来承担，审计的依据包括 eCardCA 所有与业务有关的安全策略、CPS、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

CardCA 的内部审计人员，由安全策略委员会负责组织跨部门的审计评估小组。审计评估小组的成员一般包括：

eCardCA 的安全负责人及安全管理人员；

1. eCardCA 业务负责人；
2. 认证系统及信息系统负责人；
3. 人事部门负责人；
4. 需要的其他人员。

聘请的外部审计机构，应具备以下资质：

1. 必须是经主管部门许可的，有行业执业资格的评估机构，在业界有良好的声誉；

2. 熟悉信息安全、电子认证服务、密码管理等相关的要求、技术与规范；

3. 具备进行认证系统审计的专业技术和工具；

4. 具备独立审计的精神。

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

内部审计所涵盖的主题包括：

1. CPS 符合性审查；
2. 运营工作流程和制度是否得到严格遵守；
3. 是否严格按 CP、CPS 和安全要求开展认证业务；
4. 各种日志、记录是否完整，是否存在问题；
5. 是否存在其他可能存在的安全风险。

外部审计应按国家有关法律法规、标准规范以及行业主管部门的管理要求进行独立审计。

8.5 对问题与不足采取的措施

在内部评估完成后，评估人员需列出所有问题项目的清单，由评估人员与被评估者共同讨论有关问题，并将结果书面通知 eCardCA 安全策略委员会与被评估者，进行后续处理。被评估者必须根据评估结果检查缺失与不足，提交修改与预防措施以及整改计划书，并接受评估者对整改情况的检查，以及对整改情况的再次评估。

在外部评估完成后，eCardCA 根据评估的结果检查缺失与不足，根据其提出的整改要求，提交修改与预防措施以及整改计划书，并接受外部评估机构的对整改情况的检查，以及对整改情况的再次评估。

8.6 评估结果的传达与发布

除非法律明确要求，一般不公开评估结果。

对关联方，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

证书收费标准按照与客户所签订的协议或合同执行。

证书订户有义务根据 eCardCA 公布的价格（或者双方签署的协议/合同）中指明的价格向 eCardCA 机构支付费用。

9.1.2 证书查询费用

在证书有效期内，订户对证书进行查询，eCardCA 不另行收取查询费用。

9.1.3 证书注销或状态信息的查询费用

对于查询证书是否注销，eCardCA 不收取信息访问费用。如果该项查询服务的收费政策有任何变化，eCardCA 会及时予以公布。

对于在线证书状态查询，由 eCardCA 与订购者在协议中约定。

9.1.4 其他服务的费用

可根据请求者的要求，定制各类通知服务。具体服务费用，在 eCardCA 与订购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，eCardCA 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，eCardCA 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，eCardCA 将不退还剩余时间的服务费用。

9.2 财务责任

eCardCA 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 eCardCA-CPS 规定，进行赔偿担保。

9.2.1 保险范围

出现下列情形并经公司确认后，证书订户、依赖方等实体可以申请赔偿（法定或约定免责除外）。

1. eCardCA 在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发，并导致订户或依赖方遭受损失的；
2. eCardCA 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；
3. 由于 eCardCA 的原因导致证书私钥被破译、窃取，导致订户或者依赖方遭受损失的；
4. eCardCA 未能及时撤销证书，导致订户或者依赖方遭受损失的。

9.2.2 其他资产

eCardCA 目前有能力维护运营和应对可能出现的赔付。

9.2.3 对最终实体的保险或担保

eCardCA 承担订户或依赖方在使用证书过程中造成损失时的举证责任，如无证据证明订户或依赖方使用过程中存在错误操作，则 eCardCA 将按照发布的赔偿办法予以赔偿。

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 eCardCA 来说，保密信息包括但不限于以下方面：

1. 最终订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 eCardCA 掌握的，除作为证书、CRL、认证策略被清楚发布之外的个人和单位的信息需要保密。

eCardCA 不保存任何证书应用系统的交易信息。

除非法律上有明文规定，eCardCA 没有义务公布或透露订户数字证书以外的其他信息。

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。eCardCA 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 eCardCA 目录服务等方式向外公布。

9.3.3 保护保密信息的责任

各方有保护自己和其他人员或单位的机密信息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。

当 eCardCA 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 eCardCA-CPS 中具有保密性质的信息时，eCardCA 应按照要求，向执法部门公布相关的保密信息，eCardCA 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 个人隐私保密

9.4.1 隐私保密方案

eCardCA 尊重所有用户及其隐私，个人隐私信息保密方案遵守现行法律和政策规定。

用户选择使用 eCardCA 的服务，就表示已经同意接受 eCardCA 有关隐私保护的声明。

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，通过 eCardCA 目录服务等方式向外公布。

9.4.4 保护隐私的责任

接收到隐私信息的参与者，有责任保护隐私信息不被泄漏、使用或发布给第三方。

9.4.5 使用隐私信息的告知与同意

使用隐私信息，须获得本人同意。

9.4.6 依法律或行政程序的信息披露

当 eCardCA 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证书申请人的特定资料或隐私信息时，eCardCA 按照法律、法规或规章的要求或法院的要求，向执法部门公布相关信息，eCardCA 无须承担任何责任。这种提供不能被视为违反了隐私保护的责任和义务。

9.4.7 其他信息披露情形

其他信息的披露遵循国家的相关规定处理。

9.5 知识产权

除非额外声明，eCardCA 享有并保留对证书以及 eCardCA 提供的全部软件的一切知识产权，包括所有权、名称权和利益分享权等。eCardCA 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 eCardCA-CPS 的规定，所有由 eCardCA 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 eCardCA 所有，这些知识产权包括所有相关的文件和使用手册。RA 应征得 eCardCA 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

eCardCA 在提供电子认证服务活动过程中的承诺如下：

1. eCardCA 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；

2. eCardCA 保证使用的系统及密码符合国家政策与标准，保证自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 eCardCA 证书库发出了 eCardCA 的私钥被破坏或被盗的通知，eCardCA 保证其私钥是安全的；
4. eCardCA 签发给订户的证书符合 eCardCA-CPS 的所有实质性要求；
5. eCardCA 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；
6. eCardCA 将及时注销证书；
7. 证书公开发布后，eCardCA 向证书依赖方证明，除未经验证的订户信息外，证书中的其他订户信息都是准确的。

9.6.2 RA 的陈述与担保

eCardCA 的 RA 在参与电子认证服务过程中的承诺如下：

1. 提供给证书订户的注册过程完全符合 eCardCA-CPS 所有实质性要求；
2. 在 eCardCA 生成证书时，不会因为 RA 的失误而导致证书中的信息与证书申请人的信息不一致；
3. RA 将按 eCardCA-CPS 的规定，及时向 eCardCA 提交证书申请、注销、更新等服务请求。

9.6.3 订户的陈述与担保

订户一旦接受 eCardCA 签发的证书，就被视为向 eCardCA、RA 及信赖证书的有关当事人作出以下承诺：

1. 订户需熟悉 eCardCA-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列的所有声明和信息必须是完整、真实和正确的，可供 eCardCA 或其 RA 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（例如，遗失私钥、遗忘、泄

密以及其他情况），订户应立刻通知 eCardCA 和 RA，申请采取注销等处理措施；

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 eCardCA 注销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉 eCardCA-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 eCardCA-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 依赖方的陈述与担保”。

9.7 担保免责

eCardCA 在下列情况下免于承担责任：

1. 不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担任何赔偿责任。这些事件包括但不限于劳动纠纷、交易一方故意（或无意）的行为、罢工、暴动、骚动、战争、火灾、爆炸、地震、水灾或其他自然灾难等；
2. 如果由于非 eCardCA 的原因而造成的设备故障、线路中断，导致签发数字证书错误、延误、中断或无法签发，eCardCA 不负任何赔偿责任；
3. eCardCA-CPS 的内容，没有任何信息可以暗示或解释成，eCardCA 必须承担其他的义务或 eCardCA 必须对其行为作出其他承诺。包括不承担其他任何形式的任何保证和义务，任何对特殊目的适用性的保证；
4. 如果申请者故意或无意地提供不完整、不可靠或已过期的，包括但不限于伪造、篡改、虚假的信息，而其又根据正常的流程提供了必须的审核文件，由此得到了 eCardCA 签发的数字证书。由此引起的法律问题、经济纠纷应由申请人全部承担，eCardCA 不承担与该证书内容相关的法

律和经济责任，但可以根据受害者的请求提供协查和举证帮助；

5. eCardCA 不承担任何其他未经授权的人或组织以 eCardCA 名义编撰发表或散布不可信赖的信息所引起的法律责任；
6. 对于由于证书、签名或根据 eCardCA-CPS 而提供或设计的任何其他交易或服务的使用、签发、授权、执行或拒绝执行而导致的或与之有关的任何间接性的、特别性的、附带性的、或结果性的损失，或任何利益损失、数据丢失，或其他间接性的、结果性的或惩罚性损失，无论是否可以合理预见，eCardCA 将不会对此负责，即使 eCardCA 曾经警告过这种损害的可能性；
7. eCardCA 对签发的各类证书的适用范围有明确的规定，若证书订户将其证书用于其他不被允许的用途，eCardCA 不承担任何责任，无论这种使用是滞造成损失；
8. eCardCA 在法律许可的法律内，根据法律、政策等以及受害者的要求，如实提供不可抵赖的电子签名依据，但并不对此承担法律或政策规定之外的责任。

9.8 有限责任

根据《中华人民共和国公司法》、《中华人民共和国电子签名法》和其他法律法规的规定，作为依法设立的有限责任公司，eCardCA 在承担任何责任和义务时，只承担法律范围内的有限责任。

eCardCA 在与订户和依赖方签订的协议中，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

9.9.1 赔偿范围

在认证活动中产生的赔偿，都以 eCardCA-CPS 的规定为处理依据，法律法规另有要求的除外。

1. eCardCA 的赔偿责任

(1) 在签发证书时，如果未按照 eCardCA-CPS 的规定进行处理，或者违反法律法规的要求而造成的证书订户损失的，eCardCA 应承担赔偿责任；

(2) 因为操作人员恶意、故意或疏忽，未按照 eCardCA-CPS 的规定办理证书的签发、注销等请求，并造成证书订户损失的，eCardCA 应赔偿订户的损失；

(3) 因 eCardCA 的根密钥出现问题，造成订户证书出现问题，eCardCA 应赔偿相关损失；

(4) 证书订户或其他有权提出注销证书的人提出注销请求后，到 eCardCA 将该证书注销信息予以发布的期间，如果该证书被用以进行非法交易，或进行交易时产生纠纷的，如果 eCardCA 按照 eCardCA-CPS 的规范进行了有关操作，eCardCA 不承担任何损害赔偿责任；

(5) 证书订户赔偿的追溯有效期限，按照法律法规的要求进行操作。

2. RA 的赔偿责任

(1) RA 及其操作人员没有妥善保管订户的注册和身份验证的相关隐私信息，而造成订户信息泄漏、被冒用、自发或者任意使用导致产生损失的，RA 应承担损害赔偿责任；

(2) 如果因为操作人员故意、恶意或者疏忽，没有按照 eCardCA-CPS 的规定办理证书服务注册，或者违反法律法规而造成订户损失的，RA 应赔偿订户的直接损失，以及其他随之产生的附带损失和相关补偿；

(3) 因为 RA 的原因造成系统或软件错误，未能在 eCardCA-CPS 规定的时间内，将订户的证书申请、注销、更新等请求信息发给 eCardCA，而导致订户或依赖方损失的，RA 应承担所有的损害赔偿责任；

(4) 该类赔偿的追溯有效期限，按照有关法律法规的要求进行操作。

3. 订户的赔偿责任

(1) 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致造成 eCardCA 及其授权的 RA 或者第三方遭受损害的，订户应赔偿一切损害责任；

(2) 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知 eCardCA 及其授权的 RA，以及不当交付他人使用造成 eCardCA 及其授权的 RA、第三方遭受损害的，订户应承担一切损害赔偿责任；

(3) 订户使用证书或者依赖方信任证书的行为，有违反 eCardCA-CPS 及相关操作规范，或者将证书用于非 eCardCA-CPS 规定的业务范围的，订户或者依赖方应自行承担一切损害赔偿责任；

(4) 订户使用或信赖证书时，未能按照 eCardCA-CPS 等规范进行合理审核，导致 eCardCA 及其授权的 RA 或者第三方遭受损害的，应由该订户承担一切损害赔偿责任；

(5) 证书订户或者其他有权提出注销证书的实体提出注销请求后，到 eCardCA 将该证书注销信息予以发布期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果 eCardCA 按照 eCardCA-CPS 的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任；

(6) eCardCA 与之签署的协议另有赔偿规定的，参照其规定。

9.9.2 赔偿限额

eCardCA 及其授权的 RA，对所有当事人（包括但不限于订户、申请者、接受者或信赖方）的合计赔偿责任，不可能超过以下所述（对这些证书的封顶）的赔偿金额：

对于有关一张特定证书的所有签名和交易处理的总计，eCardCA 及其授权的 RA 对于任何人（或者其他实体）有关该特定证书的合计赔偿责任应该限制在一个不超出下述数额的范围内（单位：人民币/元）

1. 个人类证书，不超过 2,000 元
2. 单位类证书，不超过 5,000 元
3. 设备类证书，不超过 6,000 元

本条款限制用于一定形式的损害，包括但不限于任何人或实体（包括但不限于订户、证书申请者、接收方或者信赖方）由于信任或者使用 eCardCA 签发、管理、使用或注销的证书或已过期证书而导致的直接的、补偿性的、间接的、特别的、结果的、惩戒性的或意外的损害。

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。每份证书的赔偿均有限额而不考虑签名、交易处理或其他有关的索赔数量。当超过赔偿限额时，除非得到依法判决或仲裁，可用的赔偿限额将首先分配给最早得到索赔解决的一方。eCardCA 没有责任为每张证书支付高出赔偿限额总和的赔

偿，而不管高出赔偿限额总和在索赔提出之间是如何分配的。

9.9.3 赔偿监督管理

eCardCA 所辖的安全管理策略委员会负责监督订户赔偿的执行情况。

9.10 有效期限与终止

9.10.1 有效期限

eCardCA-CPS 自发布之日起正式生效。

eCardCA-CPS 中将详细注明版本号及发布日期。

9.10.2 终止

当新版本的 eCardCA-CPS 正式发布生效时，旧版本的 eCardCA-CPS 自动终止。

9.10.3 效力的终止与保留

eCardCA-CPS 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 eCardCA-CPS 不适用时，由 eCardCA 的安全策略委员会组织 CPS 编写小组进行修订。

修订完成后，eCardCA 的安全策略委员会进行审批，审批通过后将在 eCardCA 的网站上发布新的 eCardCA-CPS。

eCardCA-CPS 将进行严格的版本控制。

9.12.2 通知机制和期限

eCardCA-CPS 在 eCardCA 的网站上发布。

版本更新时，最新版本的 eCardCA-CPS 在 eCardCA 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eCardCA-CPS。

9.13 争议处理

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，根据 eCardCA-CPS 中的规定，明确责任方；
2. 由相关部门负责与当事人协调；
3. 若协调失败，可以通过司法途径解决；
4. 任何因与 eCardCA 或授权机构就 eCardCA-CPS 所产生的任何争议而提起诉讼的，受 eCardCA 所在地的人民法院管辖。

9.14 管辖法律

eCardCA-CPS 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，eCardCA-CPS 的执行、解释、翻译和有效性均适用中华人民共和国的法律。

9.16 一般条款

9.16.1 完整协议

eCardCA-CPS 将替代先前的、与主题相关的书面或口头解释。

9.16.2 转让

eCardCA、RA、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

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。

在电子认证服务的各项活动中，eCardCA 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

eCardCA 对 eCardCA-CPS 拥有最终解释权。