东方新诚信数字认证中心

电子认证服务业务规则

Ver 1.6

东方新诚信数字认证中心有限公司

二〇一八年八月

目 录

1 概括性描述

1.1 概述

东方新诚信数字认证中心有限公司，简称“东方新诚信 CA”（英文缩写为 DFCA）。DFCA 面向社会信息化、社会公共管理、基于物联网、互联网的在线服务等应用领域，提供证书管理、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”等扩展的电子认证应用支撑服务。

DFCA 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，采用通过国家密码主管部门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，面向社会信息化、社会公共管理、基于物联网、互联网的在线服务等应用领域提供安全、统一、有序的电子认证服务，解决应用系统的信息安全问题。

《东方新诚信数字认证中心电子认证服务业务规则》由 DFCA 根据《电子认证服务管理办法》，依据《电子认证业务规则规范》制定，适用于 DFCA 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《电子认证服务业务规则》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《东方新诚信数字认证中心电子认证服务业务规则》，简称“DFCA-CPS”。本文档版本 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

DFCA 是根据《中华人民共和国电子签名法》和《电子认证服务管理办法》规定，依法建设的第三方电子认证服务机构。

电子认证服务机构是受订户信任，负责对证书的签发、发布、更新、撤销等证书全生命周期进行管理的实体。

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，包括本地注册机构（RA 系统）和远程注册机构，负责受理证书申请、审核、更新、注销等各类证书业务的处理。

RA 必须获得 DFCA 的授权，根据 DFCA-CPS 和 DFCA 授权开展相关证书业务服务。DFCA 根据申请单位的性质、证书发展规模、场地和人员情况等，经过严格的评估审计，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 DFCA-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 DFCA 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 DFCA-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 DFCA 接收证书的实体。包括已经申请并拥有 DFCA 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 DFCA 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 DFCA 签发的证书进行网络作业的证书持有者和按照 DFCA-CPS

合理信任证书真实性的实体。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DFCA的证书服务体系中，依赖方是信任DFCA所签发的数字证书(以下简称为“东方新诚信证书”)，可以对使用东方新诚信数字证书机制生成的数字签名进行验证，使用其他东方新诚信证书的公钥的实体。依赖方可以在法律规定以及DFCA-CPS规定的范围内信任证书及其签名，并享有DFCA-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DFCA订户的依赖方，DFCA除了担保其所信任的并且由DFCA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DFCA提供相关服务的实体。

1.4 证书应用

1.4.1 适合的证书应用

1.4.1.1 证书应用概述

东方新诚信证书能够满足社会信息化、社会公共管理、基于互联网的在线服务等应用领域对电子认证服务的需要，例如，电子政务、电子商务、医药价格等应用。证书申请人根据实际需要，决定采用哪种类型的数字证书。

东方新诚信证书主要适合以下四方面的应用。

1. 身份认证

保证采用 DFCA 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

采用东方新诚信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，可以采用东方新诚信证书机制进行加密保护。

4. 权限管理

以东方新诚信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。

1.4.1.2 常规数字证书

DFCA 发放的常规数字证书包括个人证书、机构证书和设备证书三种类型，常规数字证书以智能密码钥匙（Ukey）为安全存储介质，依赖方通过对以 Ukey 为证书载体的数字证书进行验证，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。

1.4.1.3 社保卡应用证书

DFCA 或其 RA 负责签发社保卡应用证书（全称"社会保障卡应用证书"），社保卡应用证书采用安全的文件证书预植机制和严格的管理流程，通过经授权的社保安全终端将社保卡应用证书写入到订户社保卡中，订户的社保卡应用证书与其社保卡具有一一对应关系；社保卡应用证书按照 DFCA-CPS 规定，为订户的社会保障卡应用提供身份识别、数字签名、数据加解密等安全保障服务。

1.4.1.4 社保卡副本证书

DFCA 或其 RA 负责签发社保卡副本证书（全称"社会保障卡网上副本应用证书"），社保卡副本证书以移动智能终端为证书载体，订户的社保卡副本证书与其个人移动智能终端以及终端上的社保卡应用相互对应，若订户具有多个移动智能终端或多个社保卡应用，则可能拥有多张社保卡副本证书。

1.4.1.5 嵌入式设备证书

嵌入式设备证书（全称为“物联网装置嵌入式设备身份鉴权应用证书”）是指在嵌入式安全芯片中生成或植入的数字证书，主要用于集成在各类物联网设备、终端、模块、系统等（统称为“物联网装置”），用于物联网装置的网络身份认证。

1.4.2 限制的证书应用

各类证书的使用应符合证书内容对其用途的限定，如参与方未经 DFCA 认可或不遵守相关约定，其对证书的应用超出限定的应用范围，将不受 DFCA 的保护。

限制东方新诚信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 DFCA-CPS 限制的证书应用要求所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

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

DFCA-CPS 由东方新诚信数字认证中心有限公司拥有完全版权。

1.5.2 联系人

DFCA-CPS 通过内部文件发布，对具体个人不另行通知。

联系人：东方新诚信安全策略委员会

邮箱：dfca-cps@chinaonenet.com

联系地址：长沙高新开发区麓龙路 199 号麓谷商务中心 A 栋 1502 号

邮编：410205

联系电话：0731-88239536

传　　真：0731-88239503

1.5.3 决定 CPS 符合策略的机构

DFCA 安全策略委员会负责 DFCA-CPS 的制订、发布、更新以及此方面的对外咨询服务等事宜。

1.5.4 CPS 批准程序

DFCA 安全策略委员会负责 CPS 的管理。安全策略管理委员会指定 CPS 编写小组负责起草 CPS 形成讨论稿，并征求公司领导和各部门意见，达成一致意见后提交策略管理委员会审阅；CPS 编写小组依据策略管理委员会评审意见完成 CPS 修改、确定 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 天内向工业和信息化部备案。

1.6 定义和缩写

下列定义适用于本《电子认证服务业务规则》：

1. 东方新诚信数字认证中心

受订户信任，负责创建和分配订户密钥和公钥证书的权威机构。

2. 东方新诚信数字认证中心电子认证服务业务规则

关于东方新诚信数字证书电子认证服务机构在签发、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。

3. 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。

4. 数字证书

亦简称为证书，包含公开密钥拥有者的信息，公开密钥，签发者信息、有效期，以及一些扩展信息的数字文件。

5. 社会保障智能 IC 卡

亦简称为社保卡，有社保卡管理部门发放，记录居民社会保障信息，用于为居民提供社会保障相关服务的智能 IC 卡。

6. 社会保障卡应用证书

亦简称为社保卡应用证书，包含公开密钥拥有者的信息，公开密钥，签发者信息、有效期，以及一些扩展信息的数字文件。

7. 社会保障卡网上副本应用证书

亦简称为社保卡副本证书，包含公开密钥拥有者的信息，公开密钥，签发者信息、有效期，以及一些扩展信息的数字文件。

8. 物联网装置

各类集成了嵌入式安全芯片的物联网嵌入式设备、终端、模块、系统等，统称为物联网装置。

9. 嵌入式安全芯片

植入到硬件系统内、为硬件系统提供可信根的集成电路芯片，具有唯一的芯片标识，支持基于国产密码算法的公开密钥体制，提供根密钥生成、电子签名等功能。

10. 物联网装置嵌入式设备身份鉴权应用证书

亦简称为嵌入式设备证书，由电子认证服务机构签发，植入在嵌入式芯片中，用于对嵌入式设备提供电子认证服务的数字证书。

11. 证书撤销列表（CRL）

一个已标识的列表，它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。

12. 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。

13. 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。

14. 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。

2 信息发布与信息管理

2.1 认证信息的发布

DFCA 通过在线业务网站（http://www.dfca.cn/）公布与其相关的信息。该网站是 DFCA 发布所有信息的最权威、最及时、最主要的渠道。

DFCA-CPS 发布在 DFCA 的在线业务网站上，供相关方查询、下载、查阅。

DFCA 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 DFCA 的目录服务器获取证书和 CRL。同时，DFCA 提供在线证书状态查询服务（OCSP 服务），OCSP 服务地址：www.dfca.cn：2415。

2.2 发布的时间与频率

1. CPS 的发布时间与频率

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

2. 证书/CRL 的发布时间与频率

(1) DFCA 的证书一经签发，应在订户收到证书后实时发布；

(2) DFCA 的 CRL 最迟 24 小时发布一次；

(3) 通过 OCSP 对证书状态的查询是及时的。

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，DFCA 将实时在业务门户网站发布与东方新诚信电子认证服务相关的公告与通知；

(2) 这类信息是不定期发布的，DFCA 将保证在第一时间发布信息。

2.3 信息库访问控制

对于公布的 DFCA-CPS、证书、CRL 等信息，DFCA 允许公众自行通过网站和目录服

务器进行查询与访问。

DFCA 设置了访问控制与安全审计措施，保证只有经授权的 DFCA 业务人员才能编写和修改 DFCA 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

DFCA 依照特定的签发程序，保存与订户相关的身份信息，对订户的身份进行鉴别。

对于常规数字证书和嵌入式设备证书，每个订户按照 X.509 的规定，将对应一个可分辨的名称。该名称由甄别名（Distinguished Name，简称为 DN）和订户唯一标识项组成。DN 包含于证书的主题中。DN 遵从关于 DN 的 X.501 标准，并用 X.501 Printable String 格式。

对于社保卡应用证书和社保卡副本证书，证书订户的甄别名是居民姓名，必须与居民合法身份证件上的法定姓名相符。

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。能够与证书主体所对应的实体建立确定联系。

主体识别名称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

DFCA 不允许和不接受任何匿名或伪名，仅接受有明确意义的名称。

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 DFCA 证书服务体系中，“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

DFCA-CPS 受到完全的版权保护，本文件中涉及的“DFCA”及其图标是 DFCA 独立持有的专有商标。其他参与者的商标为其拥有方所有。

DFCA 所签发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

3.2.1.1常规数字证书

DFCA 通过证书请求信息中所包含的数字签名来证明订户持有与公钥对应的私钥。在订户申请证书中，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。

证书申请人应妥善保管自己的私钥。因此，证书申请人视作其签名私钥的唯一持有者。

3.2.1.2社保卡应用证书

在社保卡应用证书业务中，DFCA 制订了严格的管理流程，从技术与制度上保证了在生成证书时，与此张证书相对应的私钥只留存在社保 IC 卡中，不会留存任何备份。当订户申领证书时，社保卡管理部门须对其身份进行审核，并将证书与订户的身份信息进行绑定，并与应用系统进行关联后，此证书才能被订户有效使用。此时，订户是其签名私钥的唯一持有者。

3.2.1.3社保卡副本证书

DFCA 通过证书请求信息中所包含的数字签名来证明订户持有与公钥对应的私钥。在订户申请证书中，订户签名私钥由订户移动智能终端和经国家密码管理部门批准的终端安全产品共同生成。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。

证书申请人应妥善保管自己的私钥。因此，证书申请人视作其签名私钥的唯一持有者。

3.2.1.4嵌入式设备证书

嵌入式设备证书采用了预植证书的方式。DFCA 建设了安全的嵌入式设备证书自动化批量写证系统，制定了严格的管理流程，从技术与管理上保证了在生成证书时，与该证书对应的私钥只存放在嵌入式芯片（通过国家密码主管部门安全性审查的硬件密码设备）内。不会留存任何备份。

当订户申领证书时，由 DFCA 或授权的 RA 对其身份进行确认与审核，并通过证书的主账号（即嵌入式设备证书唯一甄别名）与订户的身份信息进行绑定，该证书才能被订户有效使用。此时，订户是嵌入式设备证书签名私钥的唯一持有者。DFCA 要求订户妥善保管自己的签名私钥。

3.2.2 组织机构身份的鉴别

3.2.2.1常规数字证书

对于组织机构的身份鉴别，需要验证组织的合法证件。证书申请人需持工商营业执照、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 DFCA 或其 RA 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。

申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。

如果 DFCA 或其 RA 可以通过第三方验证或其他非现场方式明确组织身份时，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，通过邮寄或现场等方式，向 DFCA 的 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。

DFCA 或其 RA 按照组织机构身份鉴别规范对申请资料的真实性进行审核，并进行批准申请或拒绝申请的操作。组织机构身份鉴别规范简要说明了如何进行组织机构的身份鉴别。DFCA 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。

针对非证书申请类业务申请，允许订户不重新提交身份证明材料，使用处于有效期内的 DFCA 常规数字证书对申请材料进行的电子签名得到验证通过，亦可视为完成对用户鉴别验证。

批准申请后，DFCA 或其 RA 应妥善保存申请者的申请资料。

3.2.2.2社保卡应用证书

无规定。

3.2.2.3社保卡副本证书

无规定。

3.2.2.4嵌入式设备证书

组织机构订户在申领证书前应指定并授权证书的申领代表，接受证书申领的有关条款，承担相应的责任。

DFCA 鉴别组织机构的身份时，指定证书申领者须填写证书申请表并加盖机构公章，同时须向发证机构提供有效证明文件以证明该申领的有效性。机构有效证明文件包括但不限于：

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. 相关设备的使用权证明文件。

DFCA 或其授权 RA 将复核并验证申领文件的真实性，并进行批准申领或拒绝申领的操作。

3.2.3 个人身份的鉴别

3.2.3.1常规数字证书

个人身份的鉴别可以使用的有效身份证件包括但不限于：身份证、公安部居民身份证网上副本、公民网络身份标识（eID）、户口簿、护照等。

如果 DFCA 或其 RA 可以通过第三方验证或其他非现场方式明确个人身份时，接受申请者通过传真、邮递、网络以及 DFCA 认可的其他方式递交申请材料。

申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。

个人通过邮寄或现场等方式，向 DFCA 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。DFCA 或其 RA 按照个人身份鉴别规范对申请资料的真实性进行审核，并进行批准申请或拒绝申请的操作个人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。DFCA 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。

针对非证书申请类业务申请，允许订户不重新提交身份证明材料，使用处于有效期内的 DFCA 常规数字证书对申请材料进行的电子签名得到验证通过，亦可视为完成对用户鉴别验证。

批准申请后，DFCA 或其 RA 应妥善保存申请者的申请资料。

3.2.3.2社保卡应用证书

在社保卡制卡数据采集过程中，社保卡管理部门需要当面核实个人身份信息；订户个人身份的鉴别依托社保卡管理部门完成，DFCA 信任社保卡管理部门的身份鉴别结果；社保卡管理部门向 DFCA 提交的证书申请数据必须进行数据签名，DFCA 在完成证书申请数据接收之后，对证书申请数据进行签名验证，确认数据的有效性和完整性。

3.2.3.3社保卡副本证书

社保卡副本证书的订户通过移动智能终端向 DFCA 或其 RA 发送提交个人身份信息（如：姓名、居民身份证号码、公民网络身份标识等），DFCA 或其 RA 使用订户申请信息与社保卡管理部门的社保卡信息进行效验比对；与社保卡管理部门社保卡数据效验通过之后，DFCA 以在线方式向公安部门权威身份认证系统对订户身份进行验证，并信任验证结果。

3.2.3.4嵌入式设备证书

个人订户在申领证书前应接受证书申领的有关条款，承担相应的责任。个人订户填写证书申领文件并提交个人身份证明文件，个人身份证明文件主要包括但不限于：身份证、公安部居民身份证网上副本、公民网络身份标识（eID）、户口簿、护照等。

DFCA 或其授权 RA 将复核并验证申领文件的真实性，确认个人订户的真实身份，并进行批准申领或拒绝申领的操作。

3.2.4 域名的确认

3.2.4.1常规数字证书

如果证书名称是域名（或互联网 IP 地址），除了在对申请者提交的书面材料进行审核外，还需要证书申请者额外提供域名使用权证明材料，以确定申请者有权使用相应的域名

（或互联网 IP 地址）。DFCA 或其 RA 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请求。

3.2.4.2社保卡应用证书

无规定。

3.2.4.3社保卡副本证书

无规定。

3.2.4.4嵌入式设备证书

无规定。

3.2.5 没有验证的订户信息

除该类型证书所必须要求的身份信息需要得到明确、可靠的验证以外，DFCA 不对申请时的其他信息予以验证。

对于没有验证过的订户信息，DFCA 将不承诺此类信息的真实性，并不承担由于此类信息引起的任何责任和解决纠纷的义务。

3.2.6 授权确认

3.2.6.1常规数字证书

为确保办理人具有特定的许可，代表组织机构申请数字证书，需要出具组织机构授权其为该组织机构办理数字证书事宜的授权文件。

组织机构在 DFCA 的数字证书申请表以及授权书上加盖单位公章后，则证明本组织机构对办理人的授权确认。

3.2.6.2社保卡应用证书

无规定。

3.2.6.3社保卡副本证书

无规定。

3.2.6.4嵌入式设备证书

当申请者代表组织机构申请证书时，需要出示足够的证明信息以证明组织机构是否真实存在，申请者是否已获得组织机构的授权。DFCA 有责任确认该授权信息，并将授权信息妥善保存。

3.2.7 互操作准则

互操作可能是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电子认证服务机构之间建立相互信任关系，使双方的订户可以实现互相认证。

DFCA 将根据业务需要，在遵循 DFCA-CPS 的各项控制要求的基础上，与 DFCA 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东方形成性 CA 批准了或赋予了其他 CA 或电子认证服务机构的权力。

如果国家法律法规对此有规定，DFCA 将严格予以执行。

3.3 密钥更新请求的身份标识与鉴别

DFCA 仅支持常规数字证书密钥更新请求。

对于社保卡 IC 证书订户如有更新密钥的请求，需要向社保卡管理部门申请更换社保卡，由 DFCA 为重新签发社保卡应用证书。

对于社保卡副本证书订户如有更新密钥的请求，需要依据 DFCA-CPS 规定，重新申请证书。

对于嵌入式设备证书，当证书生成后将集成在物联网装置中，嵌入式设备证书一经签发，将永久有效，除非订户对该证书申请注销。

3.3.1 密钥更新的标识与鉴别

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，DFCA 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。

国家主管部门对密钥的管理、更新等有规定的，DFCA 将严格予以执行。

3.3.2 注销后密钥更新的标识与鉴别

DFCA 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，详见 3.2.2 组织身份的鉴别、3.2.3 个人身份的鉴别与 3.2.4 域名的确认。

3.4 撤销请求的标识与鉴别

3.4.1 订户个人撤销请求

3.4.1.1常规数字证书

订户本人撤销时的身份标识和鉴别使用初始身份确认相同的流程，详见 3.2.2 组织身份的鉴别、3.2.3 个人身份的鉴别与 3.2.4 域名的确认。

3.4.1.2社保卡应用证书

DFCA 或其 RA 仅支持响应社保卡管理部门提出的注销请求，DFCA 对社保卡管理部门提出的注销请求进行签名验证，确保撤销请求的真实性；证书注销完成之后，将注销结果通知社保卡管理部门。

3.4.1.3社保卡副本证书

由订户根据个人应用情况提出社保卡副本证书注销请求，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，详见 3.2.3 个人身份的鉴别；社保卡管理部门请求注销订户社保卡应用证书，订户社保卡副本证书也将被注销。

3.4.1.4嵌入式设备证书

订户本人撤销时的身份标识和鉴别使用初始身份确认相同的流程，详见 3.2.2 组织身份的鉴别、3.2.3 个人身份的鉴别。

3.4.2 其他撤销请求

司法机关依法提出撤销请求，DFCA 将直接以司法机关书面的撤销请求文件作为鉴别依据，不再进行其他方式的鉴别。

因为订户没有履行 DFCA-CPS 所规定的义务，由 RA 申请撤销订户的证书时，不需要对订户身份进行标识和鉴别。

3.5 非验证的用户信息

由订户提供的电子邮件地址、联系电话等非敏感性信息，东方新诚信只做记录，但不予验证。

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

4.1.1.1常规数字证书

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，以及个人、服务器、网站等各类实体订户。

4.1.1.2社保卡应用证书

证书申请实体是指持有社保卡的参保人。

4.1.1.3社保卡副本证书

证书申请实体是指持有社保卡的参保人。

4.1.1.4嵌入式设备证书

证书申请实体包括个人或具有独立法人资格的组织机构(包括企业单位、事业单位、政府机构、社会团体等）。

4.1.2 申请过程

4.1.2.1常规数字证书

证书申请人按照 DFCA-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，并准备相关的身份证明材料。DFCA 或其 RA 依据 DFCA-CPS 要求对证书申请人的身份进行鉴别，并决定是否受理申请。

4.1.2.2社保卡应用证书

社保卡应用证书申请过程如下：

1. 社保卡管理部门负责采集证书申请人的基础身份信息，并根据基础身份信息生成社保卡应用证书申请数据，经审核正确后发送 DFCA 或其 RA；
2. DFCA 或其 RA 收到证书申请数据后，将验证社保卡管理部门的数据签名信息，确认发卡申请数据的真实性、准确性；
3. 根据验证后的发卡申请数据，DFCA 根据申请数据签发社保卡应用证书，并将生成后的证书发送给社保卡管理部门；
4. 社保卡管理部门将社保卡应用证书（包括对应的密钥）安全地写入到社保卡中；
5. 社保卡管理部门将社保卡交付社保卡持卡人；
6. 根据社保卡激活结果，DFCA 激活对应的社保卡应用证书。

4.1.2.3社保卡副本证书

社保卡副本证书申请过程如下：

1. 订户通过移动智能终端以在线方式向 DFCA 或其 RA 提交社保卡副本证书申请信息；
2. DFCA 或 RA 收到证书申请信息后，将申请信息与社保卡管理部门的持卡库进行比对，确认申请人社保信息的真实性、有效性；
3. 证书申请信息数据比对通过后，DFCA 通过公安部门的网络身份认证系统，对订户身份进行在线鉴别；
4. 订户身份鉴别通过后，DFCA 根据证书申请信息为订户签发社保卡副本证书；
5. DFCA 签发证书完成后，通过在线提交方式将证书发送给社保卡副本证书订户。

4.1.2.4嵌入式设备证书

嵌入式设备证书的申请过程如下：

1. 申请者将相关的嵌入式设备证书申请材料提交到 RA；
2. RA 对申请材料及申请者进行真实性鉴别，鉴别通过后，对申请材料进行签名，发

送给 CA；

3. CA 接收到该请求后，验证 RA 的签名；
4. DFCA 将嵌入式设备证书的 DN 信息与订户的身份信息进行绑定,签发嵌入式设备证书。

4.1.3 责任

4.1.3.1常规数字证书

申请过程中各方责任为：订户要按照 DFCA-CPS 的要求准备证书申请材料（或申请信息），并确保申请材料（或申请信息）真实准确。DFCA 或其 RA 负责接收证书申请人的请求材料（或申请信息），对订户所提供的证书申请信息与身份证明资料进行鉴别验证。

4.1.3.2社保卡应用证书

申请过程中各方责任说明如下：

1. 订户：订户在接受社保卡时激活社保卡应用证书，并明确表示其愿意接受订户协议中所规定的相关责任和义务（订户协议在激活社保 IC 卡时由订户确认）；
2. 社保卡管理部门：在交付 DFCA 或其 RA 时，对订户身份进行确认，社保卡管理部门对提交的社保卡应用证书申请数据的真实性、准确性进行审核；
3. DFCA：DFCA 应对证书申请数据进行签名验证，以确认数据的真实性、完整性。

4.1.3.3社保卡副本证书

申请过程中各方责任说明如下：

1. 订户：订户在提交网络数字证书申请时明确表示其愿意接受订户协议中所规定的相关责任和义务；
2. 社保卡管理部门：社保卡管理部门接收 DFCA 发送的订户的社保卡副本证书申请数据，对数据进行效验并向 DFCA 发送申请数据效验结果，确保订户社保信息的真实性、准确性；
3. 公安部门：公安部部门接收 DFCA 发送的居民身份验证申请信息，对居民身份进

行验证并向 DFCA 发送身份验证结果，确保订户身份信息的真实性、有效性；

4. DFCA：DFCA 应将社保卡副本证书申请发送到社保卡管理部门的进行效验，并接收社保卡管理部门效验结果，以确认订户社保卡信息的真实性、完整性；DFCA 将订户身份信息提交公安部门进行身份验证，别接收公安部门验证结果，确保订户身份信息真实性、有效性。

4.1.3.4嵌入式设备证书

申请过程中各方责任说明如下：

1. 订户:订户应事先了解订户协议、CP 及 CPS 等文件的约定事项，特别是其中关于证书适用范围、权利、义务和担保的相关内容，订户负有其证书申请材料真实准确的责任和证书申请人身份真实性的责任。
2. RA:RA 负责接收证书申请信息，承担对订户提供的证书申请信息与身份证明材料的一致性检查工作，同时承担相应的审核责任。
3. DFCA:DFCA 及其注册机构有责任向订户告知嵌入式设备证书的使用条件、适用范围、收费项目与标准、保存和使用订户信息的权限和责任、订户的责任范围以及 DFCA 的责任范围。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

4.2.1.1常规数字证书

DFCA 或授权的 RA 按照 DFCA-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。具体的鉴别流程详见“3.2.2 组织身份的鉴别”、“3.2.3 个人身份的鉴别”与“3.2.4 域名的确认”。

4.2.1.2社保卡应用证书

DFCA 或授权的 RA 按照 DFCA-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。具体的鉴别流程详见“3.2.3 个人身份的鉴别”。

4.2.1.3社保卡副本证书

DFCA 或授权的 RA 按照 DFCA-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。具体的鉴别流程详见“3.2.3 个人身份的鉴别”。

4.2.1.4嵌入式设备证书

DFCA 或授权的 RA 按照 DFCA-CPS 所规定的身份鉴别流程对订户的申请材料进行识别与鉴别。具体的鉴别流程详见“3.2 初始身份的确认”。

4.2.2 证书申请批准和拒绝

DFCA 或其 RA 根据 DFCA-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 DFCA-CPS 所规定的身份鉴别流程且鉴证结果为合格，DFCA 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。

证书申请人未能通过身份鉴别，DFCA 或其 RA 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申请材料后，再次提出申请。

4.2.3 处理证书申请的时间

DFCA 或其 RA 能否在本 DFCA-CPS 规定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 DFCA 的管理要求。DFCA 或其 RA 将做出合理努力来尽快确认证书申请信息。

4.2.3.1常规数字证书

DFCA 的 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。

4.2.3.2社保卡应用证书

根据 DFCA 与社保卡管理部门约定的处理证书申请时间执行。

4.2.3.3社保卡副本证书

DFCA 实时处理社保卡副本证书申请。

4.2.3.4嵌入式设备证书

DFCA 或授权的 RA 收到嵌入式设备证书申请材料，将及时进行证书申请的处理，DFCA 或授权的 RA 应在 5 个工作日内完成证书申请的处理。

4.3 证书签发

4.3.1 证书签发过程中 DFCA 的行为

4.3.1.1常规数字证书

DFCA 根据证书申请数据签发生成数字证书。

DFCA 建设了安全的证书签发系统，制定了严格的管理流程，从技术与管理上保证了在生成证书时，与该证书相对应的私钥只存放在智能密码钥匙(通过国家密码主管部门安全性审查的硬件密码设备）内，不会在留存任何备份（加密密钥除外）。

当订户申领证书时，由 DFCA 或其 RA 对其身份进行确认与审核，并将证书与订户进行绑定，该证书才能被订户有效使用。

4.3.1.2社保卡应用证书

DFCA 根据社保卡应用证书申请数据签发生成社保卡应用证书。

DFCA 建设了安全的证书签发系统，制定了严格的管理流程，从技术与管理上保证了在生成证书时，与该证书相对应的私钥只存放在社保卡内。不会在留存任何备份(加密密钥除外）。

当订户申领证书时，由社保卡管理部门对其身份进行确认与审核，并将证书与订户的社保信息进行绑定，该证书才能被订户有效使用。

4.3.1.3社保卡副本证书

DFCA 根据社保卡副本证书申请数据签发生成社保卡副本证书。

DFCA 建设了安全的证书签发系统，制定了严格的管理流程，从技术与管理上保证了在生成证书时，与该证书相对应的私钥只存放在移动智能终端和终端安全产品(通过国家密码主管部门安全性审查的终端安全产品）上，不会在留存任何备份（加密密钥除外）。

当订户申领证书时，由 DFCA 对其社保卡信息和身份信息进行确认与审核，并将证书与订户的移动智能终端以及社保卡应用进行绑定，该证书才能被订户有效使用。

4.3.1.4社保卡副本证书

嵌入式设备证书采用了预植证书的方式。DFCA 预先在安全的嵌入式芯片中生成或植入证书。DFCA 建设了安全的证书签发系统，制定了严格的管理流程，从技术与管理上保证了在生成证书时，与该证书相对应的私钥只存放在安全的嵌入式芯片(通过国家密码主管部门安全性审查的硬件密码设备）内，不会留存任何备份（加密密钥除外）。

当订户申领证书时，由 DFCA 或授权的 RA 对其身份进行确认与审核，并通过证书的主账号（即嵌入式设备证书唯一甄别名）与订户的身份信息进行绑定，该证书才能被订户有效使用。

4.3.2 DFCA 对订户的通告

4.3.2.1常规数字证书

DFCA 对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 DFCA 或其 RA 领取数字证书；
2. 通过电子邮件（e-mail）方式通知；
3. 其他 DFCA 认为安全可行的方式通知订户。

DFCA 没有上门为订户安装证书的义务。如果订户需要，DFCA 可以上门安装，但需要收取相应的服务费用。DFCA 或其 RA 提供热线支持服务。热线支持电话和信箱由 DFCA 或其 RA 公布。

4.3.2.2社保卡应用证书

DFCA 把社保卡应用证书生成信息提交给社保卡管理部门，由社保卡管理部门负责通知订户。

4.3.2.3社保卡副本证书

DFCA 在证书签发完成之后，以在线方式把证书直接提交给订户。

4.3.2.4嵌入式设备证书

DFCA 或其授权的 RA，对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 DFCA 或其 RA 领取数字证书；
2. 通过电子邮件（e-mail）方式通知；
3. 其他 DFCA 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

4.4.1.1常规数字证书

数字证书签发完成后，DFCA 或其 RA 将数字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。

4.4.1.2社保卡应用证书

社保卡应用证书签发完成后，证书申请人领取已写入社保卡应用证书的社保卡，或主动从社保卡安全终端下载社保卡应用证书，即被视为同意接受证书。

4.4.1.3社保卡副本证书

嵌入式设备证书生成并签发完成后，DFCA 或其授权的 RA 将嵌入式设备证书以当面交付或邮政信函的方式递送给证书申请人，证书申请人即被视为同意接受证书。

4.4.1.4嵌入式设备证书

社保卡副本证书签发完成后，订户通过移动智能终端确认接收证书，即被视为同意接受证书。

4.4.2 DFCA 对证书的发布

DFCA 在签发完证书后，将证书发布到证书服务系统中。

证书服务系统将证书写入到主目录服务器，并自动同步到从目录服务器中，供订户和依赖方查询和下载。

4.4.3 DFCA 对其他实体的通告

除证书订户外，DFCA 和 RA 不需要将证书签发情况通知其他实体。

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 DFCA 所签发的证书后，均视为已经同意遵守与

DFCA、依赖方有关的权利和义务的条款。订户接收到数字证书，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，并按照证书内容对证书用途的约束（如密钥用途、密钥扩展用途）使用私钥和证书。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三个方面的内容：

1. 使用 DFCA 或其子 CA 的认证机构根证书验证订户证书中的签名，确认该证书是 DFCA 或其子 CA 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. 查询证书状态，确认该证书没有被注销。

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 证书密钥更新

DFCA 或其 RA 仅支持常规数字证书的证书密钥更新。

社保卡应用证书订户、社保卡副本证书和嵌入式设备证书如有证书密钥更新情况，需要重新申请证书。

4.6.1 证书密钥更新的情形

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。

证书密钥更新的具体情形如下：

1. 因私钥泄漏而注销证书；
2. 证书无法继续获得信任；
3. 证书无法正常使用；
4. 证书丢失；
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。

4.6.2 请求证书密钥更新的实体

同“4.1.1 证书申请实体”。

4.6.3 证书密钥更新请求的处理

对于订户的证书密钥更新请求，由 DFCA 或其 RA 为订户进行处理。

DFCA 或其 RA 对申请证书密钥更新订户的身份进行鉴别与验证，鉴别要求见“3.2.2 组织身份的鉴别”、“3.2.3 个人身份的鉴别”与“3.2.4 域名的确认”。

4.6.4 颁发新证书时对订户的通告

对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 RA 领取数字证书；
2. 通过电子邮件（e-mail）方式通知；
3. 其他 DFCA 认为安全可行的方式通知订户。

4.6.5 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”。

4.6.6 DFCA 对密钥更新证书的发布

同“4.4.2 DFCA 对证书的发布”。

4.6.7 DFCA 对其他实体的通告

同“4.4.3 DFCA 对其他实体的通告”。

4.7 证书更新

对于嵌入式设备证书，DFCA 不支持证书更新业务。嵌入式设备证书一经签发，将永久有效，除非订户对该证书申请注销。

4.7.1 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。

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，证书密钥更新。

在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止日期。订户应当在证书有效期到期前，向 DFCA 申请更新证书。

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。

4.7.2 请求证书更新的实体

同“4.1.1 证书申请实体”。

4.7.3 证书更新请求的处理

4.7.3.1常规数字证书

对于订户的证书更新请求，由 DFCA 或其 RA 为订户进行处理。

DFCA 或其 RA 对申请常规数字证书密钥更新订户的身份进行鉴别与验证，鉴别要求见“3.2.2 组织身份的鉴别”、“3.2.3 个人身份的鉴别”与“3.2.4 域名的确认”。

4.7.3.2社保卡应用证书

对于订户的证书更新请求，由 DFCA 或其 RA 为订户进行处理。

DFCA 或其 RA 对申请社保卡证书密钥更新订户的身份进行鉴别与验证，鉴别要求见“3.2.3 个人身份的鉴别”。

4.7.3.3社保卡副本证书

对于订户的证书更新请求，由 DFCA 或其 RA 为订户进行处理。

DFCA 或其 RA 对申请社保卡证书密钥更新订户的身份进行鉴别与验证，鉴别要求见“3.2.3 个人身份的鉴别”。

4.7.4 颁发新证书时对订户的通告

同“4.3.2DFCA 对订户的通告”。

4.7.5 构成接受更新证书的行为

同“4.4.1 构成接受证书的行为”。

4.7.6 DFCA 对更新证书的发布

同“4.4.2 DFCA 对证书的发布”。

4.7.7 DFCA 对其他实体的通告

同“4.4.3 DFCA 对其他实体的通告”。

4.8 证书变更

DFCA 仅支持常规数字证书的证书变更；

对于社保卡应用证书和社保卡副本证书，只有在订户（社保卡持卡人）的社保卡身份信息等发生变动时，证书信息才会发生变更。在这种情况下，将为订户发行新的社保卡，从而将签发新的社保卡应用和社保卡副本证书。因此，DFCA 不支持社保卡应用证书和社保卡副本证书的证书变更业务。

对于嵌入式设备证书，DFCA 不支持证书更新业务。嵌入式设备证书一经签发，将永久有效，除非订户对该证书申请注销。

4.8.1 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。在证书有效期内，如以下信息发生变更，应进行证书变更：

1. 机构订户的单位注册地，单位名称、单位组织机构代码号等关键信息；
2. 个人订户的姓名、住址、电子邮件等关键信息；
3. 设备的域名、IP、所有者等关键信息；
4. DFCA 规定的其他相关信息。

4.8.2 请求证书变更的实体

同“4.1.1 证书申请实体”。

4.8.3 证书变更请求的处理

对于订户的证书变更请求，由 DFCA 或其 RA 为订户进行处理。

DFCA或其RA对申请常规数字证书密钥更新订户的身份进行鉴别与验证，鉴别要求见“3.2.2 组织身份的鉴别”、“3.2.3 个人身份的鉴别”与“3.2.4 域名的确认”。

4.8.4 颁发新证书时对订户的通告

同“4.3.2DFCA 对订户的通告”。

4.8.5 构成接受更新证书的行为

同“4.4.1 构成接受证书的行为”。

4.8.6 DFCA 对更新证书的发布

同“4.4.2 DFCA 对证书的发布”。

4.8.7 DFCA 对其他实体的通告

同“4.4.3 DFCA 对其他实体的通告”。

4.9 证书注销和冻结

4.9.1 证书注销的情形

4.9.1.1常规数字证书

证书撤销是指订户由于合同期满、密码令牌丢失或怀疑私钥泄漏等原因，需要停止使用数字证书。

1. 发生下列情形之一的，订户应当申请注销与冻结数字证书：

   (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 DFCA-CPS；

(4) 政务机构的证书持有者工作性质发生变化。

2. 发生下列情形之一的，DFCA 可以注销和冻结其签发的数字证书：

(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。

4.9.1.2社保卡应用证书

发生下列情况，订户社保卡应用证书将被注销：

1. 订户社保基本信息发生变化；
2. 订户社保卡遗失；
3. 订户社保卡无法正常使用，如社保卡损坏、社保卡口令遗忘、订户申请更换社保卡等；
4. 社保卡被社保卡管理部门注销，或因社保卡信息发生变更由社保卡管理部门发起证书注销请求；
5. 订户没有或无法履行双方合同规定的义务；
6. 社保卡应用证书的安全性得不到保证；
7. 法律、法规规定的其他情形。

订户社保卡应用证书与社保卡具有对应关系，当订户社保卡基本信息发生变化，或社保卡遗失、损坏等情况，可以主动前往社保卡管理部门申请更换社保卡，DFCA 或其 RA 将响应社保卡管理部门的请求，注销订户社保卡应用证书；当社保卡管理部门发现订户社保卡应用证书出现问题，可以向 DFCA 或其 RA 提出注销申请，DFCA 将响应上述请求。

4.9.1.3社保卡副本证书

发生下列情况，订户社保卡副本证书将被注销：

1. 订户社保卡副本证书基本信息发生变化；

2. 订户个人移动智能终端遗失；

3. 订户社保卡副本证书无法正常使用，如证书损坏、证书口令遗忘等；

4. 社保卡副本证书被社保卡管理部门注销；

5. 订户没有或无法履行双方合同规定的义务；

6. 社保卡副本证书的安全性得不到保证；

7. 法律、法规规定的其他情形。

订户社保卡副本证书与其移动智能终端，以及终端社保卡应用具有对应关系，当社保卡副本证书基本信息发生变化，或移动智能终端遗失、社保卡副本证书损坏等情况，可以在线申请注销社保卡副本证书，DFCA 或其 RA 将响应注销请求，为订户注销社保卡副本证书；当社保卡管理部门发现订户社保卡副本证书出现问题，可以向 DFCA 或其 RA 提出注销申请，DFCA 将响应上述请求。

4.9.1.4嵌入式设备证书

1. 发生下列情形之一的，用户应当申请注销嵌入式设备证书：

(1) 嵌入式设备证书私钥安全已经受到损害；

(2) 嵌入式设备证书中的信息发生重大变更；

(3) 订户不能实际履行 DFCA-CPS。

2. 发生下列情形之一的，DFCA 可以注销其签发的嵌入式设备证书：

(1) 订户申请注销嵌入式设备证书；

(2) 订户提交的申请材料不真实；

(3) 订户没有或无法履行双方合同规定的义务；

(4) 嵌入式设备证书的安全性得不到保证；

(5) 证书仅用于依赖方主导的系统并由依赖方提出撤销申请；

(6) 法律、法规规定的其他情形。

4.9.2 请求证书注销的实体

同“4.1.1 证书申请实体”。

4.9.3 注销请求的流程

4.9.3.1订户注销申请

4.9.3.1.1 常规数字证书

证书注销请求的处理采用与原始证书签发相同的过程。

1. 证书注销或冻结的申请人通过在线方式或离线方式发起撤销申请，并注明注销或冻结原因，订户需依据 DFCA 要求填写《证书注销/冻结申请表》，；
2. DFCA 的 RA 根据“3.2 初始身份确认”的要求对订户提交的注销或冻结请求进行身份鉴别与审核，以确认为订户本人或得到了订户的授权；
3. DFCA 注销或冻结订户证书后，RA 将通知订户证书被注销或冻结，订户的数字证书在 24 小时内进入 CRL，向外界发布；

4.9.3.1.2 社保卡应用证书

社保卡应用证书注销请求的流程说明如下。

1. 订户以在线方式或离线方式向社保卡管理部门提出补卡或换卡申请，并注明申请原因；
2. 社保卡管理部门对订户提交的申请进行身份鉴别与审核，以确认为订户本人或得到了订户的授权；

3. 社保卡管理部门根据补卡或换卡申请，向 DFCA 发起证书注销申请，申请注销原社保卡的社保卡应用证书；
4. DFCA 根据证书注销申请，实时完成社保卡应用证书注销处理；同时，DFCA 将注销订户的网络社保卡应用证书。对被注销的人员身份鉴权书在 24 小时内进入 CRL，向外界公布。

4.9.3.1.3 社保卡副本证书

社保卡副本证书注销请求的流程说明如下。

1. 订户以在线方式向 DFCA 提出注销申请，并注明申请原因；
2. DFCA 按照“3.2.3 个人身份的鉴别”的要求，对订户提交的申请进行身份鉴别与审核，以确认为订户本人或得到了订户的授权；
3. DFCA 根据证书注销申请，实时完成订户所有(若订户拥有多台移动智能终端，则可能拥有多个社保卡副本证书)社保卡副本证书的注销处理。被注销的人员身份鉴权书在 24 小时内进入 CRL，向外界公布。

4.9.3.1.4 嵌入式设备证书

证书注销请求的处理采用与原始证书签发相同的过程。

1. 证书注销或冻结的申请人通过在线方式或离线方式发起撤销申请，并注明注销或冻结原因，订户需依据 DFCA 要求填写《证书注销/冻结申请表》，；
2. DFCA 的 RA 根据“3.2 初始身份确认”的要求对订户提交的注销或冻结请求进行身份鉴别与审核，以确认为订户本人或得到了订户的授权；
3. DFCA 注销或冻结订户证书后，RA 将通知订户证书被注销或冻结，订户的数字证书在 24 小时内进入 CRL，向外界发布；

4.9.3.2强制注销申请

强制注销是指当 DFCA 或其 RA 确认订户有违反 DFCA-CPS 的情况发生时，或社保卡

管理部门认为社保卡持卡人有违反社保卡管理规定的情况发生时，对订户证书进行强制注销，注销后将通知该订户。

4.9.4 注销请求宽限期

如果出现私钥泄露等事件，注销和冻结请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他注销和冻结原因的注销请求必须在 48 小时内提出。

4.9.5 DFCA 处理注销请求的时限

DFCA 接到注销/冻结请求后实时处理，24 小时生效。

DFCA 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，供订户和依赖方查询下载。

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 DFCA 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）：DFCA 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

CRL 的发布周期为 24 小时，即每日发布一次 CRL。

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 ARL 发布频率

DFCA 目前未发布 ARL。

4.9.10 在线状态查询的可用性

DFCA 向订户和依赖方提供在线证书状态查询服务（OCSP 服务），OCSP 服务地址为： www.dfca.cn: 2415。

4.9.11 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，依赖方在信赖一个证书前，必须通过证书状态在线查询检查该证书的状态。

4.9.12 注销信息的其他发布形式

除了 CRL、OCSP 外，DFCA 暂不提供注销/冻结信息的其他发布形式。

4.9.13 密钥损害的特别要求

无论是最终订户还是DFCA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。

4.9.14 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。

DFCA 不支持嵌入式设备证书的证书冻结请求。

4.9.15 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、DFCA 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。

4.9.16 冻结请求的流程

4.9.16.1 常规数字证书

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

如是是强制冻结，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、DFCA 或 DFCA 授权的 RA。

DFCA 冻结订户证书后，RA 将当面通知或通过发送 E-mail 邮件或邮寄等方式通知订户证书被冻结。

4.9.16.2 社保卡应用证书

证书冻结请求的流程说明如下。

1. 订户以在线方式或离线方式向社保卡管理部门提出冻结申请，并注明申请原因；
2. 社保卡管理部门对订户提交的申请进行身份鉴别与审核，以确认为订户本人或得到了订户的授权；
3. 社保卡管理部门根据冻结申请，向 DFCA 发起证书冻结申请，申请将原社保卡对应的社保卡应用证书冻结；
4. DFCA 根据证书冻结申请，实时完成证书冻结处理。被挂起的社保 IC 卡在 24 小时内进入 CRL，向外界公布。

4.9.16.3 社保卡副本证书

证书冻结请求的流程说明如下。

1. 订户以在线方式向 DFCA 提出冻结申请，并注明申请原因；
2. 社保卡管理部门对订户提交的申请进行身份鉴别与审核，以确认为订户本人；
3. DFCA 根据证书冻结申请，将订户社保卡副本证书冻结；
4. DFCA 根据证书冻结申请，实时完成证书冻结处理。被挂起的社保 IC 卡在 24 小时内进入 CRL，向外界公布。

4.9.17 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 DFCA 或 DFCA 授权的 RA 有权自行撤销证书。对此造成的任何后果，DFCA 不负责任。

4.10 证书状态服务

4.10.1 操作特征

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

4.10.2 服务可用性

原则上，DFCA 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，订户各参与方能够实时获得证书状态查询服务。

4.11 订购结束

终止服务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 DFCA 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 DFCA 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。

4.12 密钥生成、备份与恢复

具体策略在“6.1 密钥生成与安装”与“6.2 私钥的安全保证”中详细描述。

4.12.1 密钥托管与恢复的策略与行为

4.12.1.1 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。

4.12.1.1.1 常规数字证书

订户的签名密钥对由订户的密码设备生成，或由密码设备与经国家认证的第三方密钥服务机构生成，加密密钥对由密钥管理中心生成。

4.12.1.1.2 社保卡应用证书

订户的签名密钥对和加密密钥对均由密钥管理中心生成，DFCA 制订严格的安全流程，通过安全授权的社保卡终端将签名密钥对写入订户社保卡，签名密钥对只在用户社保卡中保存。

4.12.1.1.3 社保卡副本证书

订户的加密密钥对由密钥管理中心生成，DFCA 通过订户移动智能终端和移动智能终端密码产品来生成分散式签名密钥对。

4.12.1.1.4 嵌入式设备证书

对于嵌入式设备证书的签名密钥对，DFCA 建设了安全的证书签发系统，制定了严格

的管理流程，从技术与管理上保证了在生成签名证书时，与该签名证书相对应的签名私钥只存放在嵌入式芯片（通过国家密码主管部门安全性审查的硬件密码设备）内，不会留存任何备份。

对于嵌入式设备证书的加密密钥对，由密钥管理中心生成，并加密存储在密钥管理中心的数据库服务器中。在生成加密证书时，加密密钥对将下载至嵌入式安全芯片内。

4.12.1.2 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 DFCA 申请进行密钥恢复。经审核后，通过 DFCA 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 DFCA 申请。由 DFCA 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。

4.12.2 会话密钥的封装与恢复的策略与行为

会话密钥的封装采用数字信封的方式。数字信封使用接收者的公钥对会话密钥加密，接收者用自己的私钥解密，恢复会话密钥。

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

DFCA 的建筑物和机房建设按照下列标准实施：

1. GB 50174-2008：《电子计算机机房设计规范》
2. GB 2887-2000：《电子计算机场地通用规范》
3. GB 9361-88：《计算站场地安全要求》
4. SJ/T 10796-2001：《防静电活动地板通用规范》
5. GB 50034-2004：《建筑照明设计标准》
6. GB 50054-95：《低压配电设计规范》
7. GB 50019-2003：《采暖通风与空气调节设计规范》
8. GB 157：《建筑防雷设计规范》
9. GBJ 79-1985：《工业企业通信接地设计规范》

DFCA 机房位于长沙麓谷高新区标志麓谷坐标 A 栋 1502，实行分区访问的安全管理：

DFCA 机房的功能区域划分为 CA 核心区、CA 管理区、CA 服务区、RA 管理区与监控管理区等区域。

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结合指纹鉴定才能进出，系统记录进出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。
3. 监控系统：部署有视频监控系统，对于屏蔽机房区域，进行24小时不间断录像，对于其他机房区域，采用动态录像方式进行监控。系统保留录像资料，以备查询。

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，DFCA 采用使用不间断电源系统（UPS）来保证供电的稳定性和可靠性，当市电停电时，维持系统正常运转。DFCA 的市电由高开区的市电接入供电。高开区的市电具有双市电供电，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，维持系统正常运转。

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。

DFCA 对 CA 系统的电源、空调等物理要求，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。

DFCA 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必须符合 GB 50045-1995《高层民用建筑设计防火规范》中规定的二级耐火等级；
2. DFCA 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、主要空调管道中及易燃物附近部位设置烟、温感探测器；
3. 敏感区及高敏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。DFCA 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；
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；
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。

DFCA 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 DFCA 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。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。

5.1.8 异地备份

东方新诚信定期进行数据备份，备份数据均送到位于异地的银行保险柜，进行异地备份保存。

5.2 程序控制

5.2.1 可信角色

DFCA 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，必须由可信人员担任。

DFCA 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

DFCA 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 DFCA-CPS 的要求，规范证书服务机构和服务系统的管理人员、操作人员的岗位职责和操作行为。

5.2.2 每项任务需要的人数

DFCA 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、互相监督和最小权益的安全管理原则，确保由多名可信人员共同完成敏感操作。

1. 访问和管理 CA 的加密设备及密钥，至少需要 3 个可信人员。

2. 对于证书申请的鉴别和签发，需要 3 个可信人员操作完成。

3. 对于重要的系统操作与维护，DFCA 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 DFCA 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。DFCA 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 DFCA 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。DFCA 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 DFCA 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

DFCA 与有关的政府部门和调查机构合作，完成对 DFCA 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、资格证及身份证等相关有效证明；
2. 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；
3. 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；
4. 考核合格报主管领导批准后准予上岗。

5.3.3 培训要求

DFCA 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. DFCA 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. DFCA 的业务管理相关的流程、标准与规范；
5. DFCA 的运行管理相关的规章、制度与管理办法；
6. 国家电子认证相关的法律法规与政策；
7. 其他必要的培训。

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 DFCA 组织的培训一次。

认证策略调整、系统更新时，应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

对于可替换角色，DFCA 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。

工作岗位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 DFCA 的员工被怀疑，或者已进行了未授权的操作，例如，滥用权利或超出权限使用 DFCA 或进行越权操作，DFCA 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 DFCA 内部的工作人员，但从事 DFCA 有关业务的人员等独立签约者，DFCA 的统一要求如下：

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

5.3.8 提供给员工的文档

为使得系统正常运行，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；

5.4 审计日志程序

5.4.1 记录事件的类型

DFCA 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。DFCA 还可能记录其他与系统不直接相关的事件，例如：物理通道参观记录、人事变动等。

5.4.2 处理日志的周期

DFCA 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

DFCA 在审计日志的保存期限不少于 5 年。

5.4.4 审计日志的保护

DFCA 执行严格的管理，确保只有 DFCA 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。

5.4.5 审计日志备份程序

DFCA 保证所有的审查记录和审查总结都按照 DFCA 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. 密钥管理系统；
3. 证书注册管理系统；
4. 证书服务系统；
5. 证书在线业务门户；
6. 网站、数据库安全管理系统；
7. 其他需要审计的系统。

DFCA 使用系统审计工具对上述审计日志进行收集。

5.4.7 对导致事件实体的通告

DFCA 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，DFCA 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。

DFCA 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

DFCA 每年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

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和证书信息等。

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，DFCA 对与证书相关的归档记录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，DFCA 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。DFCA 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。

DFCA 保存的申请信息、订户基本情况资料和身份鉴别资料，非经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 DFCA 的存储库，还在异地保存其备份。存档的数据库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。DFCA 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

DFCA 暂不采用时间戳技术表明存档时间。

5.5.6 归档收集系统

认证系统的相关运营信息，由 DFCA 内部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

只有 DFCA 授权的可信人员能够访问归档记录。归档记录的一致性在归档时进行验证。归档期间，所有被访问的记录在归还时必须验证其一致性。

5.6 电子认证服务机构密钥更替

DFCA 密钥更替指 DFCA 认证机构证书到期时，需要更换密钥而采取的措施。

DFCA 的认证机构的签名密钥更替办法为：

由国家根 CA 签发的 CA 根证书到期前，DFCA 将向国家根 CA 机构申请新 CA 根证书；新 CA 根证书启用时同时停止旧 CA 根证书的签发证书服务，过渡期内旧 CA 根证书的 CRL 签发服务继续有效，直到依赖旧 CA 根证书签发的证书到期为止；DFCA 采取必要措施保障新旧 CA 根证书之间的信任过渡。

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，DFCA 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

DFCA 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，DFCA 将按照灾难恢复计划实施恢复。

5.7.3 DFCA 私钥损害处理程序

当 DFCA 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，DFCA 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 DFCA-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 DFCA 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 DFCA-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 DFCA 的核心业务系统采用双机备份方式；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，DFCA 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 DFCA 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，DFCA 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 DFCA 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 DFCA 主机硬件。

当 DFCA 授权的证书服务机构因故终止服务时，DFCA 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，DFCA 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

6.1.1.1CA 密钥对生成

CA 系统的根密钥由加密机独立生成，加密机保存在屏蔽机房当中，操作人员只能在屏蔽机房中对根密钥进行操作。

6.1.1.2订户密钥对生成

6.1.1.2.1 常规数字证书

订户的签名密钥对由订户的密码设备生成生成，加密密钥对由密钥管理中心生成。

6.1.1.2.2 社保卡应用证书

社保卡应用证书的加密密钥对由密钥管理中心生成，签名密钥对由密钥管理中心预制生成。

6.1.1.2.3 社保卡副本证书

社保卡副本证书的加密密钥对由密钥管理中心生成，社保卡副本证书通过订户移动终端和移动终端密码产品来生成分散式签名密钥对。

6.1.1.2.4 嵌入式设备证书

嵌入式设备证书的签名密钥对由 DFCA 使用国家密码主管部门批准和许可的硬件密码设备生成。DFCA 建设了安全的证书签发系统，制定了严格的管理流程，从技术与管理上

保证了所生成的签名私钥只存放在安全的嵌入式芯片（通过国家密码主管部门安全性审查的硬件密码设备）内，不会留存任何备份。

嵌入式设备证书的加密密钥对由 DFCA 的密钥管理中心使用国家密码主管部门批准和许可的硬件密码设备生成。

6.1.2 私钥传送给订户

6.1.2.1常规数字证书

订户的签名密钥对由订户自己生成并保管。

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。

6.1.2.2社保卡应用证书

社保卡应用证书的签名密钥和加密密钥均通过安全授权的社保卡终端写入订户社保卡。

6.1.2.3社保卡副本证书

社保卡副本证书签名密钥由订户终端产生，加密密钥通过订户的签名公钥对加密密钥进行加密后，发送到订户移动终端。

6.1.2.4嵌入式设备证书

订户的私钥由订户自己生成时将不会进行传送，由 DFCA 生成时将离线或在线安全方式传递。订户委托DFCA或者其他人产生私钥时，DFCA或者受托方需确保私钥在交给客户前未被使用，且不能保留签名私钥的备份。

6.1.3 公钥传送给证书签发机构

在公钥传递过程中，DFCA 采用国家密码管理局许可的通讯协议及密钥算法，保证传输中数据的安全。

6.1.3.1常规数字证书

订户的签名公钥通过安全通道，经 RA 传递到 DFCA。

订户的加密公钥，由密钥管理中心通过安全通道传递到 DFCA。

6.1.3.2社保卡应用证书

订户的签名公钥和加密公钥，由密钥管理中心通过安全通道传递到 CA。

6.1.3.3社保卡副本证书

订户的签名公钥通过终端安全产品的安全通道传递到CA，加密公钥由密钥管理中心通过安全通道传递到 CA。

6.1.3.4嵌入式设备证书

订户可通过 CA 提供的下载服务建立的安全通道将公钥发送给 CA，或者通过电子邮件的形式发送给 CA。

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 DFCA 的网站下载认证机构证书，从而得到 DFCA 的公钥。

6.1.5 密钥的长度

DFCA 支持 RSA 算法与 SM2 算法。RSA 非对称密钥对的模长是 1024 比特，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，DFCA 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

CA 密钥：用于签发证书和 CRL。

订户密钥：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

DFCA 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。DFCA 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

认证系统的私钥的生成、更新、注销、备份和恢复等操作采用多人控制机制，即采取 3 选 2 方式，将私钥的管理权限分散到 3 张密钥卡中，只有其中 2 至 3 人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

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

订户的签名密钥 DFCA 不予备份。加密密钥由 DFCA 的密钥管理中心备份，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、导出密码模块

DFCA 不提供订户私钥导出的方法。

CA 私钥的导出和导入，应由 3 个密钥管理员分别登录加密机，通过加密机进行加密导出和导入。

6.2.7 私钥在密码模块中的存储

6.2.7.1CA 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。

6.2.7.2订户私钥在密码模块中的存储

私钥均以密文形式存储，硬件密码设备均通过国家密码主管部门批准和许可的。

6.2.7.2.1 常规数字证书

订户私钥在硬件密码模块中加密保存。

6.2.7.2.2 社保卡应用证书

订户签名私钥存储在订户安全存储介质中，加密私钥存储于密钥管理中心的密码设备。

6.2.7.2.3 社保卡副本证书

订户签名私钥分散式存储在移动智能终端和终端安全产品中，订户加密私钥以签名公钥加密保存在订户的移动智能终端中。

6.2.7.2.4 嵌入式设备证书

订户私钥存储在国家密码主管部门批准和许可的安全的嵌入式芯片内。

6.2.8 激活私钥的方法

DFCA 的私钥存放于密码设备中，其激活数据保存于 IC 卡介质中，必须采用 3 选 2 的方式分别输入激活数据才能激活。激活私钥至少需要 2 名密钥管理员同时在场，使用智能 IC 卡登录加密机，启动密钥管理程序，进行激活私钥的操作。

6.2.9 解除私钥激活状态的方法

具有解除私钥激活状态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，进行解除私钥的操作，需要 3 名管理员同时在场。

6.2.10 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，需要三名管理员同时在场；同时，所有用于激活私钥的 PIN 码、IC 卡、动态令牌等密码设备也必须被销毁或者收回。

6.2.11 密码模块的评估

DFCA 使用国家密码主管部门批准和许可的密码设备。根据 DFCA 对密码设备的性能、工作效率、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

订户证书中的公钥包括签名公钥和加密公钥。公钥的归档，其操作过程、安全措施、保存期限以及保存策略和证书保持一致，归档要求参照 DFCA-CPS 中“5.5 记录归档”的相关规定

6.3.2 证书操作期和密钥对使用期限

所有订户证书的有效期和其对应的密钥对的有效期都是一致的。

6.4 激活数据

对于嵌入式设备证书，证书签发后默认为激活状态，因此没有激活数据。

6.4.1 激活数据的产生和安装

6.4.1.1常规数字证书

激活数据是私钥保护密码，智能密码钥匙（证书存储介质）出厂时设置了缺省的 PIN 值，证书制作时，将该 PIN 值修改为私钥保护密码，从而激活了智能密码钥匙的 PIN。

6.4.1.2社保卡应用证书

激活数据是私钥保护密码，IC 卡出厂时设置了缺省的 PIN 值，证书制作时，将该 PIN 值修改为私钥保护密码，从而激活了 IC 卡的 PIN。

6.4.1.3社保卡副本证书

激活数据是私钥保护密码，采用经过国家密码管理批准与认可的终端安全产品，订户申请证书时需要设置 PIN 值，证书制作时，该 PIN 值默认为私钥保护密码。

6.4.2 激活数据的保护

订户应该经常对 PIN 值进行修改。

6.4.3 激活数据的其他方面

只有在拥有证书存储介质并知道 PIN 值时才能将其激活，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

DFCA 根据法律法规和主管部门的规定，按照国家计算机安全等级的要求，实现安全等级制度。同时，DFCA 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

DFCA 的信息安全管理，严格遵循国家密码管理局等主管部门的有关运行规范和 DFCA 的安全管理策略进行操作。

DFCA 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。DFCA 还对认证系统进行定期和不定期的检查与测试。

DFCA 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。DFCA 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

DFCA 暂不采用时间戳技术。

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

DFCA 签发的证书符合国家相关标准的要求，符合 X.509 V3 格式。

7.1.1 版本号

X.509 V3。

7.1.2 证书扩展项

7.1.2.1常规数字证书

DFCA 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。DFCA 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。东方新诚信认证系统定义的 CRL 发布点。

7.1.2.2社保卡 IC 证书与社保卡副本证书

DFCA 签发的社保卡证书支持使用证书标准项和标准扩展项。

1. 基本约束。用于鉴别证书持有者身份；
2. 使用者密钥标识符。是用来标识包含某个公钥的证书的简写方式。
3. 授权密钥标识符。对应根证书的密钥标识符，可用来标识根证书。
4. CRL 发布点。东方新诚信认证系统定义的 CRL 发布点。

5. 密钥用法。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；
6. 证书策略。CA 机构签发的证书策略，符合 X.509 证书格式，这一策略信息存放在证书策略属性栏。
7. 授权信息访问（颁发机构信息访问）。该扩展标识证书的签发者如何访问 CA 的信息以及服务。包括在线验证服务和 CA 策略数据。
8. 机构编码。用来标识证书 RA。
9. SSN 号。通过实名认证后的订户唯一身份编码。
10. 社会保障号码。国家建立全国统一的个人社会保障号码。
11. 社保卡号。社保系统当中的业务唯一编号。

7.1.2.3嵌入式设备证书

嵌入式设备证书使用 X.509 V3 版证书标准扩展项。

7.1.3 算法对象标识符

1. RSA 证书使用 SHA1WithRSAEncryption 算法，算法 OID 1.2.840.113549.1.1.5；

2. SM2 证书使用 SM3withSM2 算法，算法标识 OID 为 1.2.156.10197.1.501。

7.1.4 名称形式

DFCA 签发的数字证书中的主体 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。

7.1.5 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。

7.1.6 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对证书所相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。

7.1.7 策略限制扩展项的用法

系统策略中设定的扩展项结果的分页返回条数，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。

7.1.8 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。

7.1.9 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。

7.2 证书撤销列表

DFCA 签发的证书撤销列表符合 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

1. CRL 扩展项：颁发机构密钥标识符 Authority Key Identifier。
2. 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

DFCA 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 DFCA 是否按照 DFCA-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 DFCA 自己组织内部人员进行的审计，审计的结果可供 DFCA 改进、完善业务，内部审计结果不需要公开。

外部审计由委托第三方审计机构来承担，审计的依据包括 DFCA 所有与业务有关的安全策略、DFCA-CPS、业务规范、管理制度，以及国家或行业的相关标准。

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》、《电子政务电子认证服务管理办法》的规定，接受管理部门的评估和检查。

8.2 评估者的资质

DFCA 无条件接受管理部门的审计评估，评估者所具有的资质由管理部门决定。

在进行内部审计评估时，要求评估人员至少具备认证机构、信息安全审计评估的相关知识，有三年以上的相关经验，并且熟悉 DFCA-CPS 的规范，以及应具备计算机、网络、信息安全等方面的知识和实际工作经验。内部审计评估由企业内控部门组织实施。DFCA 在进行外部审计评估时，选择专业、公正、客观的专业审计评估机构，要求评估者具备以下的资质：

1. 必须是经许可的、有营业执照的评估机构，在业界享有良好的声誉；
2. 了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作；
3. 具备检查系统运行性能的专业技术和工具。

外部审计的审计人员的资质由第三方审计机构确定。

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

评估内容包括但不限于以下方面：

1. CPS：是否制订和发布 CPS，是否按照 CPS 来制订相关的操作规范和运作协议；是否按照 CPS 及相关操作规范和运作协议开展业务；
2. 服务完整性：密钥和证书生命周期的安全管理，业务系统的安全操作，业务操作规范性审查；
3. 物理和环境安全控制：信息安全管理，人员的安全控制，物理环境设施的安全控制，软硬件设备和存储介质的安全控制，系统和网络的安全控制，系统开发和维护的安全控制，灾难恢复和备份系统的管理，审计和归档的安全管理等。

8.5 对问题与不足采取的措施

对审计评估中发现的问题，DFCA 将根据法律法规、行业政策、技术标准规范和自身策略制订有效的改进计划及预防措施，对落实情况进行再次评估以达到解决问题的目标。

8.6 评估结果的传达与发布

管理部门在完成评估后，按照法律法规的要求对评估结果进行处理。

除非法律明确要求，审计评估结果一般不公开。

9 法律责任和其他业务条款

9.1 费用

数字证书收费标准按照与客户所签订的协议执行。

证书订户有义务根据 DFCA 公布的证书价格或者双方签署的协议中指明的价格向 DFCA 支付费用。

9.1.1 证书签发和更新费用

DFCA 收取合理的证书签发和更新费用，并在订户订购时提前告知。

9.1.2 证书查询费用

在证书有效期内，对证书信息进行查询，DFCA 不收取查询费用。

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，目前，DFCA 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，DFCA 会及时予以公布。

对于在线证书状态查询，由 DFCA 与订制者在协议中约定。

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 DFCA 与用户签订的协议中约定。

9.1.5 退款策略

在实施证书操作和签发证书的过程中，DFCA 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，DFCA 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，DFCA 将不退还剩余时间的服务费用。

9.2 财务责任

DFCA 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。

此要求对订户同样适用。

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. DFCA 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. DFCA 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 DFCA 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. DFCA 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

DFCA 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

DFCA 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 DFCA 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 DFCA 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 DFCA 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。

DFCA 不保存任何证书应用系统的交易信息。

除非法律明文规定，DFCA 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。DFCA 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。

订户数字证书及注销信息可以通过 DFCA 目录服务等方式向外公布。

9.3.3 保护保密信息的责任

DFCA 或其 RA、订户、依赖方等各参与方，都有按照 DFCA-CPS 规定，承担保护保

密信息的责任。不将保密信息（也不会促使或允许他人将保密信息）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，如果已明确表示保密信息不得复印、复制或储存于任何数据存储或检索系统，接受方不得复印、复制或储保密信息。

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

当保密信息的所有者出于某种原因，要求 DFCA 公开或披露他所拥有的保密信息时，应书面授权以表示其自身的公开或者披露意愿，DFCA 应满足其要求。如该披露行为涉及任何其他方的赔偿义务和所造成的损失，应由保密信息的所有者承担，DFCA 不予承担。

9.4 个人隐私保密

9.4.1 隐私保密方案

DFCA 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 DFCA 的服务，就表示已经同意接受 DFCA 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 DFCA 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 DFCA 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，DFCA 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，DFCA 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，DFCA 享有并保留对证书以及 DFCA 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。DFCA 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 DFCA-CPS 的规定，所有由 DFCA 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 DFCA 所有，这些知识产权包括所有相关纸质和电子文档。RA 等相关实体应征得 DFCA 的授权后才能使用相关文档，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

DFCA 在提供电子认证服务活动过程中的承诺如下：

1. DFCA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受信息产业部的

领导，对签发的数字证书承担相应的法律责任；

2. DFCA 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 DFCA 证书库发出了 DFCA 的私钥被破坏或被盗的通知，DFCA 保证其私钥是安全的；
4. DFCA 签发给订户的证书符合 DFCA 的 CPS 的所有实质性要求；
5. DFCA 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. DFCA 将及时注销证书；
7. 证书公开发布后，DFCA 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

DFCA 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 DFCA 的 CPS 的所有实质性要求；
2. 在 DFCA 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 CPS 的规定，及时向 DFCA 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 DFCA 签发的证书，就被视为向 DFCA、RA 及依赖方作出以下承诺：

1. 订户需熟悉 DFCA-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 DFCA 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，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知 DFCA 或其 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 DFCA 注销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉 DFCA-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 DFCA-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

DFCA 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、水灾或其他大灾难等；

2. 如果由于非东方新诚 CA 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，DFCA 不负任何赔偿责任；

3. DFCA-CPS 的内容，没有任何信息可以暗示或解释成，DFCA 必须承担其他的义

务或 DFCA 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 DFCA 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，DFCA 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. DFCA 不承担任何其他未经授权的人或组织以 DFCA 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 DFCA-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，DFCA 将不会对此负责，即使 DFCA 曾经警告过这种损害的可能性；

7. DFCA 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，DFCA 不承担任何责任，无论这种使用是滞造成损失；

8. DFCA 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，DFCA 在承担任何责任和义务时，只承担法律范围内的有限责任。

DFCA 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 DFCA-CPS 的规定为处理依据，法律法规另有要求的除外。

1. DFCA 的赔偿责任

(1) 在签发证书时，如果未按照 DFCA-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，DFCA 应承担赔偿责任；

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

(3) 因 DFCA 的根密钥出现问题，造成订户证书出现问题，DFCA 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 DFCA 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 DFCA 按照 DFCA-CPS 的规范进行了有关操作，DFCA 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 DFCA-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 DFCA-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 DFCA，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 DFCA 及其授权的证书服务机构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 DFCA 及其授权的证书服务机构，以及不当交付他人使用造成 DFCA 及其授权的证书服务机构、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 DFCA-CPS 及相关操作规范，或者将证书用于非 DFCA-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 DFCA-CPS 等规范进行合理审核，导致 DFCA 及其授权的证书服务机构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 DFCA 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 DFCA 按照 DFCA-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) DFCA 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

DFCA 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，不可能超过发下所述对这些证书的封顶赔偿金额：

对于有关一张特定证书的所有签名和交易处理的总计，DFCA 及其授权的证书服务机构对于任何人（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 50,000 元

3. 设备类证书，不超过 80,000 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 DFCA 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。DFCA 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。

9.10 有效期限与终止

9.10.1 有效期限

DFCA-CPS 自发布之日起正式生效。

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

9.10.3 效力的终止与保留

DFCA-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

除非法律法规或者协议有特别的规定，DFCA 将以合理的方式与相关各方进行沟通。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 DFCA-CPS 不适用时，由 DFCA 的 CPS 策略委员会组织 CPS 编写小组进行修订。

安全策略管理委员会指定 CPS 编写小组负责起草 CPS 形成讨论稿，并征求公司领导和各部门意见，达成一致意见后提交策略管理委员会审阅；CPS 编写小组依据策略管理委员会评审意见完成 CPS 修改、确定 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。。

公司行政部门负责自发布之日起 30 天内向工业和信息化部备案。

9.12.2 通知机制和期限

DFCA-CPS 在在 DFCA 的网站上发布。

版本更新时，最新版本的 DFCA-CPS 在在 DFCA 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 DFCA-CPS。

9.13 争议处理

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，根据 DFCA-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 DFCA 或授权机构就 DFCA-CPS 所产生的任何争议而提起诉讼的，受

DFCA 所在地的人民法院管辖。

9.14 管辖法律

DFCA-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，DFCA-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

DFCA-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

DFCA、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。

在数字证书认证活动中，DFCA 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

DFCA 对 DFCA-CPS 拥有最终解释权。