社会保障卡应用证书

证书策略

V1.0

发布日期：2017 年 7 月

生效日期：2017 年 7 月

东方新诚信数字证书认证有限公司

二〇一七年六月

目 录

1 概括性描述 Introduction

1.1 概述 Overview

1.1.1 证书服务机构简介 Company Profile

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 面向全国市场，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。

1.1.2 证书策略 Certificate Policy（CP）

本 CP 描述社会保障卡应用证书（以下简称“社保卡应用证书”）的证书策略（CP），是 DFCA 关于社保卡应用证书的策略声明，适用于所有由 DFCA 签发和管理的社保卡应用及相关参与主体。

社保卡应用是指在订户移动智能终端中载入的数字证书，主要为社保卡持卡人提供身份认证、数字签名、数据加密、权益送达、挂号邮局等人社信息化应用。本 CP 不能作为 DFCA 和各参与方之间的法律性协议。DFCA 和各参与方之间的权利、义务，应由他们之间签署的各类协议确定。

DFCA 作为第三方电子认证服务机构，在本 CP 的约束下生成并签发社保卡应用。DFCA 制订的社保卡应用证书电子认证服务业务规则（CPS）接受本 CP 的约束。所有 DFCA 社保卡应用的订户及依赖方应参照本 CP 及相关 CPS 的规定，决定对证书的使用和信任。

本 CP 遵循以下标准规范：

1. GB/T 31508-2015 信息安全技术 公钥基础设施数字证书策略分类分级

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

1.1.3 证书服务机构架构 Certificate Policy Architecture

本 CP 是 DFCA 关于社保卡应用证书的最高策略。DFCA 按照本 CP 制定 CPS，RA 按照本 CP 及相关 CPS 进行证书服务申请鉴别，订户、依赖方及其他相关实体按照本 CP 及相关 CPS 决定对证书的使用、信任并履行相关的义务。

1.1.4 证书层次架构 Hierarchical Architecture of Certificates

社保卡应用证书的证书层次结构如图 1-1 所示。（下图中应体现出两种不同社保卡应用证书）

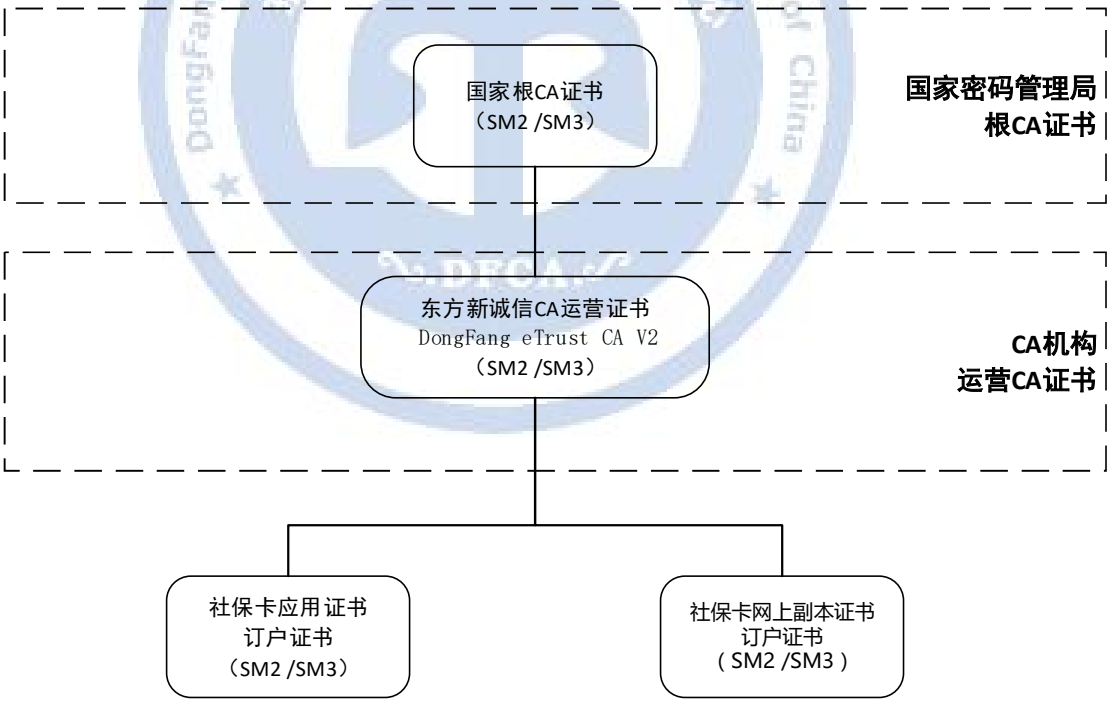

图 1-1 DFCA 社保卡应用证书层次架构示意图

DFCA 根证书，证书通用名：DongFang eTrust CA V2，密钥长度 256-bit，将于 2036 年 10 月 09 日到期。

社保卡应用证书子 CA 根证书，该子 CA 正在规划中。

社保卡应用证书主要面向个人订户签发。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本 CP 规定，为订户的社会保障卡应用提供身份认证、数字签名、数据加解密等安全服务。

1.2 文档名称与标识 Document Name and Identification

本文档名称是《社会保障卡应用证书-证书策略》。

版本号为 V1.0

1.3 电子认证活动参与者 Certification Participants

1.3.1 电子认证服务机构 Certification Authorities

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，负责创建和分配公钥证书的权威机构，是颁发社保卡应用证书的实体。

1.3.2 注册机构 Registration Authorities

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）和证书本地受理点，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 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 必须获得 DFCA 的授权，根据授权从事相关证书业务的办理。

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。

1.3.3 订户 Subscribes

本 CP 所指订户，特指从 DFCA 接收社保卡应用证书的实体，即已经申请并拥有 DFCA 签发的社保卡应用证书的个人。

在电子签名应用中，订户即为电子签名人。

1.3.4 依赖方 Relying Parties

本 CP 所指依赖方，是指任何使用 DFCA 签发的社保卡应用证书进行网络作业和按照本 CP 合理信任社保卡应用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 DFCA 的证书服务体系中，依赖方是信任 DFCA 所签发的社保卡应用证书，可以对使用东方新诚信社保卡应用证书机制生成的数字签名进行验证，使用其他 DFCA 的订户证书的公钥的实体。依赖方可以在法律规定以及本 CP 规定的范围内信任证书及其签名，并享有本 CP 规定的各种权利。

对于依赖方，DFCA 承诺，除了未经验证的订户信息外，证书中的或证书中合并参考到的所有信息都是准确的。

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。

1.3.5 其他参与者 Other Participants

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 Certificate Usage

1.4.1 适合的证书应用 Appropriate Certificate Uses

社保卡应用证书包括签名证书、加密证书。社保卡应用证书主要适合以下四方面的应用：

1. **身份认证：**使用社保卡应用证书，可对社保卡持卡人身份进行认证；

2. 电子签名：使用社保卡应用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：使用社保卡应用证书，实现对信息的机密性保护，防止对信息的非法访问；

4. 操作审计：使用社保卡应用证书，对持卡人的行为日志进行电子签名，确保持卡人的操作行为的不可抵赖性。

1.4.2 限制的证书应用 Prohibited Certificate Uses

社保卡应用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，超出限定的应用范围使用社保卡应用证书，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。

因违反本 CP 规定的限制证书应用要求所造成的法律后果，由使用者自己负责。

1.5 策略管理 Policy Administration

1.5.1 策略管理机构 Organization Administering the Policy

本 CP 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本 CP 的制定、发布、更新等事宜。

1.5.2 联系人 Contact Person

本 CP 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 CP 符合策略的机构 Committees Determining CP Suitability for the Policy

本 CP 由 DFCA 安全策略委员会批准，包括本 CP 的修订和版本变更。

DFCA 安全策略委员会负责评估DFCA 的CPS 是否符合本 CP，是批准和决定 DFCA 的 CPS 是否与本 CP 相适应的机构。

1.5.4 CP 批准程序 CP Approval Procedures

本 CP 由 DFCA 安全策略委员会负责管理。安全策略委员会指定 CP 编写小组负责起草形成本 CP 的讨论稿，并征求公司领导和各部门意见，达成一致意见后提交安全策略委员会审查。经安全策略委员会审查通过后，方可对外发布。

自发布之日起 30 天内，DFCA 将本 CP 上报国家电子认证服务主管部门备案。

1.5.5 CP 修订 CP Revision

本 CP 的修订由 DFCA 根据国家的政策法规、技术要求、业务发展情况及时完成。CP 编写小组根据相关的情况进行修订，提交 DFCA 安全策略委员会审核。经该委员会批准后，正式在 DFCA 官方网站上发布。

本 CP 至少每年修订一次。如果无内容改动，则递增版本号、更新发布时间、生效时间及修订记录。

1.6 定义和缩写 Definitions and Acronyms

1.6.1 术语 Definitions

下列定义适用于本 CP。

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，在某些环境下主动注销或冻结证书，处理订户注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. 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。

5. 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。

6. 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。

7. 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。

1.6.2 缩略语 Acronyms

下列缩略语适用于本 CP。

CA (Certificate Authority) 电子认证服务机构

CP (Certification Policy) 证书策略

CPS (Certification Practice Statement) 证书策略

CRL (Certificate Revoke List) 证书撤消列表

LDAP (Lightweight Directory Access Protocol) 轻型目录访问协议

LRA (Local Registration Authority) 本地注册受理点

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

PIN (Personal Identification Number) 个人身份识别码

PKI (Public Key Infrastructure) 公共密钥基础设施

RA (Registration Authority) 注册审核服务机构

2 发布与信息库责任 Publication and Repository Responsibilities

2.1 信息库 Repositories

社保卡应用证书的电子认证信息库应包括以下内容：证书策略（CP）、电子认证业务规则（CPS）、证书、证书注销列表（CRL）、证书在线状态查询（OCSP）等。

2.2 认证信息的发布 Publication of Certification Information

社保卡应用证书的信息库由 DFCA 通过在线业务网站公布。该网站是社保卡应用证书所有信息的最权威、最及时、最主要的渠道。

社保卡应用证书及其 CRL 由 DFCA 通过 LDAP 服务器发布。订户或依赖方可以通过访问 DFCA 的 LDAP 服务器获取社保卡应用证书 CRL。

DFCA 应提供在线证书状态查询服务（OCSP 服务），订户或依赖方可通过 OCSP 服务在线查询社保卡应用证书状态，DFCA 在其 CPS 中声明 OCSP 服务详细内容。

2.3 发布的时间与频率 Time or Frequency of Publication

本 CP 的最新版本由 DFCA 在业务门户网站上及时发布，这种发布应该是即时的、高效的，并且是符合国家法律的要求的。

社保卡应用证书一经签发，应在订户收到证书后实时发布； CRL 最迟 24 小时发布一次，在紧急的情况下，DFCA 可以自行决定证书和 CRL 的发布时间；

通过 OCSP 对社保卡应用证书状态的查询是及时的。

2.4 信息库访问控制 Access Control on Repositories

对于公开发布的 CP、CPS、证书、CRL 等社保卡应用证书信息，DFCA 允许公众自行

通过网站和 LDAP 服务器进行查询与访问。

应设置访问控制与安全审计措施，保证只有经授权的 CA 业务人员才具有信息库的增加、删除、修改、发布等操作的权限。

3 身份标识与鉴别 Identification and Authentication

3.1 命名 Naming

3.1.1 命名类型 Types of Names

由 DFCA 签发的社保卡应用证书符合 X.509 v3 标准，分配给证书持有者的主体甄别名，采用 X.500 命名方式。

社保卡应用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 对命名有意义的要求 Needs for Names to be meaningful

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 Anonymity or Pseudonymity of Subscribers

社保卡应用证书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 解释不同命名的规则 Rules for Interpreting Various Name Forms

依 X.500 甄别名命名规则解释，即 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 命名的唯一性 Uniqueness of Names

在社保卡应用证书的证书服务体系中，“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 Recognition, Authentication, and Role of Trademarks

社保卡应用证书的主体甄别名中不包含商标名。

3.2 初始身份确认 Initial Identity Validation

3.2.1 证明拥有私钥的方法 Method to Prove Possession of Private Key

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。

3.2.2 组织机构身份的鉴别 Authentication of Organization Identity

无规定。

3.2.3 个人身份的鉴别 Authentication of Individual Identity

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。

3.2.4 数据来源的准确性 Accuracy of Data Sources

社保卡应用证书的证书申请数据由社保卡管理部门提交给 DFCA 或其 RA，DFCA 在接收证书申请数据后，通过都证书申请数据进行签名验证，确保证书申请数据的有效性、完整性。

3.2.5 没有验证的订户信息 Non-Verified Subscriber Information

订户提交证明文件以外的信息为没有验证的订户信息。

3.2.6 授权确认 Validation of Authority

无规定。

3.2.7 互操作准则 Criteria for interoperation

对于其他的电子认证服务机构，可以与 DFCA 进行互操作，但是该电子认证服务机构的 CPS 必须符合本 CP 要求，并且与 DFCA 签署相应的协议。DFCA 将依据协议的内容，接受非 DFCA 的发证机构鉴别过的信息，并为之签发相应的证书。

截至目前，DFCA 未签发任何交叉证书。

如果国家法律法规对此有规定，DFCA 将严格予以执行。

3.3 密钥更新请求的标识与鉴别 Identification and Authentication for Rekey Requests

社保卡应用证书不支持密钥更新。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。

3.3.1 常规密钥更新的标识与鉴别 Identification and Authentication for Routine Rekey

无规定。

3.3.2 注销后密钥更新的标识与鉴别 Identification and Authentication for Rekey After Revocation

无规定。

3.4 注销请求的标识与鉴别 Identification and Authentication for Revocation Request

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。

如果是司法机关依法提出注销，DFCA 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本 CP 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；同时，将注销结果通知社保卡管理部门和订户。

4 证书生命周期操作要求 Certificate Life Cycle Operational Requirements

4.1 证书生命周期操作概述 Overview

本章阐述了 DFCA 根据本 CP 进行社保卡应用证书的申请、签发、管理、更新、注销等证书生命周期管理的全程过程，以及在这些过程中各参与方的责任与义务。

4.2 证书申请 Certificate Application

4.2.1 证书申请实体 Who Can Submit a Certificate Application

证书申请实体为持有社保卡的参保人。

4.2.2 申请过程与责任 Application Process and Responsibilities

4.2.2.1 申请过程 Application Process

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。

4.2.2.2责任 Responsibilities

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卡时由订户确认）；
2. 社保卡管理部门：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。在交付 DFCA 或其 RA 时，对订户身份进行确认；
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。

4.3 证书申请处理 Certificate Application Processing

4.3.1 执行识别与鉴别 Performing Identification and Authentication Functions

DFCA 或授权的 RA 按照本 CP 所规定的身份鉴别流程对申请人的身份进行鉴别。具体的鉴别流程详见“3.2.3 个人身份的鉴别”。

4.3.2 证书申请批准和拒绝 Approval or Rejection of Certificate Applications

4.3.2.1证书申请的批准 Approval of Certificate Applications

DFCA 或其 RA 根据本 CP 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，订户如果符合下述条件，DFCA 批准证书申请：

1. 该申请完全满足本 CP 第 3.2 节关于订户身份的标识和鉴别规定；
2. 申请者接受或者没有反对订户协议的内容和要求。

如果证书申请人通过本 CP 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社保卡应用证书。

4.3.2.2证书申请的拒绝 Rejection of Certificate Applications

DFCA 或其 RA 根据本 CP 所规定的身份鉴别流程对证书申请人进行身份鉴别，订户如果发生下列情形，DFCA 应拒绝证书申请：

1. 该申请不符合本 CP 第 3.2 节关于订户身份的标识和鉴别规定；
2. 申请者不能提供所需要的身份证明与证书申请信息；
3. 申请者反对或者不能接受订户协议的有关内容和要求；
4. DFCA 认为批准该申请将会对 DFCA 带来争议、法律纠纷或者损失。

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）。

4.3.3 处理证书申请的时间 Time to Process Certificate Applications

根据 DFCA 与社保卡管理部门约定的处理证书申请时间执行。

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 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。

4.4 证书签发 Certificate Issuance

4.4.1 证书签发过程中 RA 和 CA 的行为 Actions During Certificate Issuance of RA and CA

DFCA 按本 CP 定义的证书格式，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。

4.4.2 CA 和 RA 通知订户证书的签发 Notifications to Subscriber by the CA and RA of Issuance of Certificate

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。

4.5 证书接受 Certificate Acceptance

4.5.1 构成接受证书的行为 Conduct Constituting Certificate Acceptance

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。

4.5.2 CA 对证书的发布 Publication of the Certificate by the CA

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发布到 LDAP 服务器中，供订户和依赖方查询和下载。

4.5.3 CA 对其他实体的通告 Notification of Certificate Issuance by the CA to Other Entities

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。

4.6 密钥对和证书的使用 Key Pair and Certificate Usage

4.6.1 订户私钥和证书的使用 Subscriber Private Key and Certificate Usage

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。订户接收到社保卡应用证书，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。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。

4.6.2 依赖方公钥和证书的使用 Relying Party Public Key and Certificate Usage

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. 用 DFCA 或其社保卡子 CA 的认证机构根证书验证证书中的签名，确认该证书是 DFCA 或其社保卡子 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。

4.7 证书密钥更新 Certificate Rekey

DFCA 不支持社保卡应用证书密钥更新，订户如有证书密钥更新情况，需要重新申请证书。

4.8 证书更新 Certificate Renewal

4.8.1 证书更新的情形 Circumstances for Certificate Renewal

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，订户需重新申请证书。

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。

4.8.2 请求证书更新的实体 Who May Request Renewal

证书的个人持有者可以请求证书更新。

4.8.3 证书更新请求的处理 Processing of Certificate Renewal Requests

对于订户的证书更新请求，由 DFCA 或其 RA 为订户进行处理。

RA 对申请证书更新订户的身份进行鉴别与验证，鉴别要求同本 CP 的 3.2.3 个人身份的鉴别。

4.8.4 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber

颁发新证书时对订户的通告同 4.4.2 CA 和 RA 通知订户证书的签发。

4.8.5 构成接受更新证书的行为 Conduct Constituting Acceptance of a Renewal Certificate

构成接受密钥更新证书的行为同 4.5.1 CA 构成接受证实书的行为。

4.8.6 CA 对更新证书的发布 Publication of the Renewal Certificate by the CA

CA 对密钥更新证书的发布同 4.5.2 CA 对证书的发布。

4.8.7 CA 对其他实体的通告 Notification of Certificate Issuance by the CA to Other Entities

对其他实体的通告同 4.5.3 CA 对其他实体的通告。

4.9 证书变更 Certificate Modification

DFCA 不支持社保卡应用证书变更；如有证书变更情形，订户需要按照本 CP “4.2 证书申请”相关规定申请新的证书。只有在订户（社保卡持卡人）的基础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证书。因此，社保卡应用证书没有证书变更业务。

4.10 证书注销 Certificate Revocation

4.10.1 证书注销的情形 Circumstances for Revocation

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。

4.10.2 请求证书注销的实体 Who Can Request Revocation

根据不同的情况，社保卡应用证书订户、DFCA、RA 或社保卡主管部门可以请求注销社保卡应用证书。

4.10.3 注销请求的流程 Procedure for Revocation Request

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注销申请，并注明注销原因；
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 注销订户证书后，RA 将通知订户证书被注销，订户的社保卡应用证书在 24 小时内进入 CRL，向外界公布；

4. 强制注销是指当 DFCA 或授权的 RA 确认订户有违反本 CP 的情况发生时，对订户证书进行强制注销，注销后将立即通知该订户。

4.10.3.1 订户注销申请 Subscribe Certificate Revocation Request

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。被注销的证书在 24 小时内进入 CRL，向外界公布。

4.10.3.2 强制注销申请 Compulsion Certificate Revocation Request

强制注销是指当 DFCA 或其 RA 确认订户有违反本 CP 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，注销后将依据本 CP“4.4.2CA 和 RA 通知订户证书的签发”相关规定通知该订户。

4.10.4 注销请求宽限期 Revocation Request Grace Period

订户一旦发现需要注销证书，应及时向 RA 提出注销请求。

4.10.5 CA 处理注销请求的时限 Time Within Which CA Must Process the Revocation Request

DFCA 接到注销请求后立即处理，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 LDAP 服务器，供请求者查询下载。

4.10.6 依赖方检查证书注销的要求 Revocation Checking Requirements for Relying Parties

在具体应用中，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：通过 LDAP 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。

4.10.7 CRL 发布频率 CRL Issuance Frequency

CRL 的发布周期为 24 小时，即每日发布一次 CRL。

4.10.8 CRL 发布的最大滞后时间 Maximum Latency for CRLs

发布的最长滞后时间为 24 小时。

4.10.9 在线状态查询的可用性 Online Revocation/Status Checking Availability

DFCA 应向订户和依赖方提供在线证书状态查询服务（OCSP 服务）。

4.10.10 在线状态查询要求 Online Revocation Checking Requirements

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社保卡应用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。

4.10.11 注销信息的其他发布形式 Other Forms of Revocation Advertisements Available

除了 CRL、OCSP 外，DFCA 暂不提供注销信息的其他发布形式。

4.10.12 对密钥遭受安全威胁的特别处理要求 Special Requirements related to Key Compromise

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，应立即申请注销证书。

4.10.13 证书冻结的情形 Circumstances for Suspension

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。

4.10.14 请求证书冻结的实体 Who Can Request Suspension

请求证书冻结的实体包括：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。

4.10.15 冻结请求的流程 Procedure for Suspension Request

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。被挂起的社保卡应用证书在 24 小时内进入 CRL，向外界公布。

4.10.16 冻结的期限限制 Limits on Suspension Period

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 或其 RA 有权自行注销证书。对此造成的任何后果，DFCA 不负责任。

4.11 证书状态服务 Certificate Status Services

4.11.1 操作特征 Operational Characteristics

订户可以通过 CRL、LDAP 目录服务、OCSP 查询证书状态。

4.11.2 服务可用性 Service Availability

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。

4.11.3 可选特征 Operational Features

无规定。

4.12 订购结束 End of Subscription

下列情况视为订户的订购行为为正式结束：

1. 证书到期后没有进行更新；
2. 证书到期前被注销。

4.13 密钥托管与恢复 Key Escrow and Recovery

4.13.1 密钥托管与恢复的策略与行为 Key Escrow and Recovery Policy and Practices

4.13.1.1 密钥托管策略与行为 Key Escrow Policy and Practices

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。

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。

4.13.1.2 密钥恢复策略与行为 Key Recovery Policy and Practices

密钥恢复是指加密密钥对的恢复，DFCA 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，DFCA 向密钥管理中心请求密钥恢复；密钥管理中心接受密钥恢复请求后，将订户密钥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。

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。

5 认证机构设施、管理和操作控制 Facility, Management, and Operational Controls

5.1 物理控制 Physical Controls

5.1.1 场地位置与建筑 Site Location and Construction

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 物理访问控制 Physical Access

进出每一个物理安全区的行为均需要被记录、审计和控制，从而保证进出每一个物理安全区的人均经过授权。DFCA 必须对物理访问控制进行详细的规定。

5.1.3 电力与空调 Power and Air Conditioning

DFCA 机房应有安全、可靠的电力供电系统和电力备用系统，以确保持续不间断的电力供应。

DFCA 应安装空调系统、新风系统，以控制运营设施的温度的湿度。

DFCA 应严格参照相关设施管理的规定，对电力、空调等设施进行维护和保养，而且每年对其是否符合运行要求进行检查。

5.1.4 防水 Water Exposures

机房应有专门的技术措施，防止、检测漏水的出现，并能够在出现漏水时最大程度减小对认证系统的影响。

5.1.5 火灾防护 Fire Prevention and Protection

机房应采取预防措施，并制定相应的程序来消除和防止火灾的发生。这些火灾防护措施应符合当地消防管理部门的安全要求。

5.1.6 介质存储 Media Storage

对物理介质的存放和使用应满足防火、防水、防震、防潮、防腐蚀、防虫害、防静电等的安全需求，并且建立严格的保护手段以防止对介质未经授权的使用和访问。

5.1.7 废物处理 Waste Disposal

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，使用信息无法恢复。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 Off-Site Backup

所备份的业务数据（光盘、移动存储介质等）均送到 DFCA 异地备份区，进行异地备份保存。

5.2 程序控制 Procedural Controls

5.2.1 可信角色 Trusted Roles

DFCA 或其授权的 RA 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 明确规定可信角色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》等标准规范与本 CP 的要求，制订其授权的证书服务机构（RA 等）的管理规范，规范证书服务机构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。DFCA 对授权的 RA 的责任进行合理划分，并通过系统和技术实现、管理的责任划分进行保证。

5.2.2 每项任务需要的人数 Number of Persons Required per Task

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 个可信人员中的 2 个共同完成。
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 Identification and Authentication for Each Role

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；进入系统需要使用社保卡应用证书进行身份鉴别。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 Roles Requiring Separation of Duties

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、注销、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、注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 Personnel Controls

5.3.1 资格、经历和无过失要求 Qualifications, Experience, and Clearance Requirements

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 运行的其他兼职工作、无同行业重大错误记录、无违法犯罪记录等。

5.3.2 背景审查程序 Background Check Procedures

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 Training Requirements

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 Retraining Frequency and Requirements

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 工作岗位轮换周期和顺序 Job Rotation Frequency and Sequence

DFCA 将根据业务的安排进行工作岗位轮换。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 Sanctions for Unauthorized Actions

DFCA 应建立并维护本机构管理办法，对未授权行为进行适当处罚，包括解除或终止劳动合同、调离工作岗位、罚款、批评教育、提交司法机构处理等方式。这些处罚行为应当符合法律法规的要求。

5.3.7 独立合约人的要求 Independent Contractor Requirements

对不属于 DFCA 内部的工作人员，但从事 DFCA 业务有关工作的业务人员、管理人员等独立合约人，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 Documentation Supplied to Personnel

为使得系统正常运行，必须提供给员工与其工作相关的文档。

5.4 审计日志程序 Audit Logging Procedures

5.4.1 记录事件的类型 Types of Events Recorded

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 Frequency of Processing Log

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 Retention Period for Audit Log

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 Protection of Audit Log

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 Audit Log Backup Procedures

DFCA 所有的审查记录与审查总结都按照第三方 CA 机构管理部门的管理要求进行备份。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 Audit Collection System

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 Notification to Event-Causing Subject

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 Vulnerability Assessments

DFCA 应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 Records Archival

5.5.1 归档记录的类型 Types of Records Archived

需求归档的记录，除本 CP 第 5.4.1 节规定的内容外，还应对如下记录进行归档：

1. 证书申请信息；
2. 证书签发过程中的支持文档。

5.5.2 归档记录的保存期限 Retention Period for Archive

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 Protection of Archive

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 Archive Backup Procedures

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 Requirements for Time-Stamping of Records

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 Archive Collection System

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 Procedures to Obtain and Verify Archive Information

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 Key Changeover

CA 证书到期时，DFCA 将对 CA 证书进行更新。

CA 证书的签名密钥由密码机产生，在生成新的 CA 密钥对时，须严格遵守 DFCA 关于密钥管理的规范。新的密钥对产生时，由国家主管部门签发新的 CA 证书。DFCA 及时进行发布。

CA 密钥更替时，须保证整个证书链的顺利过渡。

5.7 损害与灾难恢复 Compromise and Disaster Recovery

5.7.1 事故和损害处理程序 Incident and Compromise Handling Procedures

发生事故时，DFCA 按照制定的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 Computing Resources, Software, and/or Data Are Corrupted

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 实体私钥损害处理程序 Entity Private Key Compromise Procedures

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，订户应按照本 CP 的规定，首先申请注销证书，然后按照规定重新申请新的证书。

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 启动重大事件应急处理程序，由安全策略委员会和相关专家进行评估，制定行动

计划。若需要注销 CA 证书，将采用以下措施：

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. 立即注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，按照本 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、LDAP 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，订户应按照本 CPS 的规定，首先申请注销证书，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 Business Continuity Capabilities After a Disaster

针对 DFCA 的核心业务系统和核心数据库，DFCA 应在其 CPS 中制订相应的备份策略，确保系统的高可靠性和可用性。

发生自然或其他不可抗力性灾难后，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 CA 或 RA 的终止 CA or RA Termination

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 Technical Security Controls

6.1 密钥对的生成和安装 Key Pair Generation and Installation

6.1.1 密钥对的生成 Key Pair Generation

6.1.1.1 CA 密钥对的生成 Key Pair Generation to CA

社保卡应用证书的 CA 密钥对由加密机独立生成，加密机保存在屏蔽机房中，操作人员只能在屏蔽机房中对密钥进行操作。

6.1.1.2订户密钥对的生成 Key Pair Generation to Subscriber

社保卡应用证书的加密密钥对和签名密钥对由密钥管理中心生成。

6.1.2 私钥传送给订户 Private Key Delivery to Subscriber

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。

6.1.3 公钥传送给证书签发机构 Public Key Delivery to Certificate Issuer

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。

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。

6.1.4 CA 公钥传送给依赖方 CA Public Key Delivery to Relying Parties

依赖方可从 DFCA 业务网站下载相应根证书，得到 DFCA 的公钥。

6.1.5 密钥的长度 Key Sizes

DFCA 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，DFCA 将会完全遵从。

6.1.6 公钥参数的生成和质量检查 Public Key Parameters Generation and Quality Checking

公钥参数由国家密码管理局许可的密码设备和应用系统产生。

公钥参数质量的检查由国家密码管理局许可的密码设备和应用系统进行。

6.1.7 密钥使用目的 Key Usage Purposes

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 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 密码模块的标准和控制 Cryptographic Module Standards and Controls

DFCA 所用的密码设备都是经国家密码管理部门许可和批准的产品。东方新诚信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 Private Key Multi-Person Control

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 Private Key Escrow

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 Private Key Backup

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 Private Key Archival

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 Private Key Transfer Into or From a Cryptographic Module

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 Private Key Storage on Cryptographic Module

6.2.7.1CA 私钥在密码模块中的存储 CA Private Key Storage on Cryptographic Module

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 Subscriber Private Key Storage on Cryptographic Module

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。

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。

6.2.8 激活私钥的方法 Method of Activating Private Key

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 3 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 冻结私钥的方法 Method of Deactivating Private Key

对于 CA 私钥，由具有相关权限的密钥管理员登录密码设备，启动密钥管理程序，进行冻结私钥的操作。至少需要三名密钥管理员同时在场，方可进行该项操作。

对于订户私钥，由订户自行决定提出私钥冻结请求。

6.2.10 解除私钥激活状态的方法 Method of Destroying Private Key

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，需要三名管理员同时在场。

6.2.11 销毁 CA 私钥的方法 Method of Destroying CA Private Key

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。

6.2.12 密码模块的评估 Cryptographic Module Rating

DFCA 使用国家密码主管部门批准和许可的密码模块。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，选择所需要的密码模块。

6.3 密钥对管理的其他方面 Other Aspects of Key Pair Management

6.3.1 公钥归档 Public Key Archival

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，由 DFCA 定期归档。

6.3.2 证书操作期和密钥对使用期限 Certificate Operational Periods and Key Pair Usage Periods

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 Activation Data

6.4.1 激活数据的产生和安装 Activation Data Generation and Installation

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。

6.4.2 激活数据的保护 Activation Data Protection

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 Other Aspects of Activation Data

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 Computer Security Controls

6.5.1 特别的计算机安全技术要求 Specific Computer Security Technical Requirements

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 Computer Security Rating

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 Life Cycle Technical Controls

6.6.1 系统开发控制 System Development Controls

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 Security Management Controls

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 Life Cycle Security Controls

整个系统从设计到实现，系统的安全性始终是首要保护的。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 Network Security Controls

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 Time-Stamping

DFCA 未采用时间戳技术。

7 证书、证书注销列表和在线证书状态协议 Certificate, CRL, and OCSP Profiles

7.1 证书 Certificate Profile

社保卡应用证书采用 X.509 V3 格式，符合国家相关标准的要求。

7.1.1 版本号 Version Number(s)

X.509 V3。

7.1.2 证书扩展项 Certificate Extensions

社保卡应用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。

7.1.3 算法对象标识符 Algorithm Object Identifiers

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 Name Forms

DFCA 签发的社保卡应用证书中的主体 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）应为证书主体或者社保卡发卡机构的部门名称全称；

O 应为证书主体或者社保卡发卡机构的名称全称；

E（Email）证书主体邮箱地址；

L（City）证书主体所在城市；

S（Province）证书主体所在省份；

CN（Common Name）中的内容分为 1 种：

1. 持卡人姓名

2. 社会保障号码。

7.1.5 名称限制 Name Constraints

证书名称的使用采用实名制，要求证书主体名称与证书持有者法定身份证件上的姓名相符。

7.1.6 证书策略对象标识符 Certificate Policy Object Identifier

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与证书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 Usage of Policy Constraints Extension

在系统策略中可以设定扩展项结果的分页返回条数，查询结果可进行分页显示。这样，可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 Policy Qualifiers Syntax and Semantics

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 Processing Semantics for the Critical Certificate Policies Extension

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 证书注销列表 CRL Profile

DFCA 签发的证书注销列表符合 X.509 V2 格式。

7.2.1 版本号 Version Number(s)

X.509 V2。

7.2.2 CRL 和 CRL 条目扩展项 CRL and CRL Entry Extensions

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 Online Certificate Status Protocol

社保卡应用证书为订户提供在线证书状态查询服务（OCSP 服务）。

7.3.1 版本号 Version Number(s)

使用 OCSP 版本 1（OCSP V1）。

7.3.2 OCSP 扩展项 OCSP Extensions

目前未使用 OCSP 扩展项。

8 认证机构审计和其他评估 Compliance Audit and Other Assessments

8.1 评估的频率或情形 Frequency and Circumstances of Assessment

审计是为了检查、确认 DFCA 是否按照本 CP 及 DFCA 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、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 Identity/Qualifications of Assessor

DFCA 无条件接受电子认证主管部门的审计评估，评估者所具有的资质由电子认证主管部门和商用密码主管部门决定。

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，并且熟悉本 CP 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 Assessor's Relationship to Assessed Entity

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 Topics Covered by Assessment

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 Actions Taken as a Result of Deficiency

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 Communications of ResultS

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。

8.7 其他评估 Other Assessments

无规定。

9 法律责任和其他业务条款 Other Business and Legal Matters

9.1 费用 Fees

社保卡应用证书的收费标准按照与客户所签订的协议执行。

9.1.1 证书签发和更新费用 Certificate Issuance or Renewal Fees

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 Certificate Access Fees

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 Revocation or Status Information Access Fees

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 Fees for Other Services

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 与订户签订的协议中约定。

9.1.5 退款策略 Refund Policy

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

订户接受社保卡应用证书，DFCA 将不办理退证、退款手续。

如果订户在证书服务期内退出社保卡应用证书服务体系，DFCA 将不退还剩余时间的服务费用。

9.2 财务责任 Financial Responsibility

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 Insurance Coverage

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 未能及时注销证书，导致订户或者依赖方遭受损失的。

9.2.2 其他资产 Other Assets

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 Insurance or Warranty Coverage for End-Entities

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 Confidentiality of Business Information

9.3.1 保密信息范围 Scope of Confidential Information

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社保卡应用证书以外的信息。

9.3.2 不属于保密的信息 Information Not Within the Scope of Confidential Information

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。

订户社保卡应用证书及注销信息可以通过 LDAP 服务器等方式向外公布。

9.3.3 保护保密信息的责任 Responsibility to Protect Confidential Information

DFCA、RA、订户以及与认证业务相关的参与方等，均有义务按照本 CP 的规定，承担相应的保护保密信息的责任，必须通过有效的技术手段和管理程序对其进行保护。

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，需对这种申请进行书面授权，DFCA 方可满足其要求。若这种披露保密信息的行为涉及任何其他方的赔偿责任，DFCA 不应承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者应承担与此相关的或由于公开保密信息所引起的所有赔偿责任。

当 DFCA 在任何法律、法规、法院以及其他公权力部门通过合法程序的要求下，必须提供本 CP 规定的保密信息时，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。

9.4 个人隐私保密 Privacy of Personal Information

9.4.1 隐私保密方案 Privacy Plan

DFCA 应制定隐私保密方案对订户的个人信息保密。

9.4.2 作为隐私处理的信息 Information Treated as Private

订户提供的不构成社保卡应用证书内容的信息，被视为隐私信息。

9.4.3 不被视为隐私的信息 Information Not Deemed Private

订户提供的用来构成社保卡应用证书内容的资料不认为是隐私信息。

社保卡应用证书是公开的，通过 LDAP 服务器等方式向外公布。

9.4.4 保护隐私的责任 Responsibility to Protect Private Information

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 Notice and Consent to Use Private Information

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 Disclosure Pursuant to Judicial or Administrative Process

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 Other Information Disclosure Circumstances

其他信息的披露遵循国家的相关规定处理。

9.5 知识产权 Intellectual Property Rights

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。

按本 CP 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 Representations and Warranties

9.6.1 CA 的陈述与担保 CA Representations and Warranties

DFCA 对证书订户必须做出如下担保：

1. DFCA 签发给订户的证书完全符合本 CP 的所有实质性要求；

2. 验证证书中所包含的全部信息的准确性（organizationalUnitNameb 除外）；

3. DFCA 保证 CA 私钥得到安全的存放和保护，DFCA 建立和执行的安全机制符合国家相关政策与标准的规定；

4. DFCA 将按本 CP 的规定，及时注销证书；

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. 验证申请者对列在证书主题字段及主题别名扩展中的域名及 IP 地址拥有使用权或控制权；

7. 验证申请者授权了证书的签发以及申请者代表得到了授权，以代表申请者申请证书；

8. 采取验证措施以减小证书主题中所包含的信息存在误导的可能性；

9. 根据本 CP 第 3.2 节的要求验证申请人的身份；

10. 若 DFCA 与订户无关联，则 DFCA 与订户是合法有效且可执行的订户协议的双方。若 DFCA 与订户为关联，则申请人代表已订可使用条款；

11. 针对所有未过期的证书的当前状态信息（有效或已注销）建立及维护全天候的公开信息库。

DFCA 对依赖方必须做出如下担保：

1. 除未经验证的订户信息外，证书中的其他订户信息均为准确的；

2. DFCA 完全遵照本 CP 的规定签发证书；

3. 在 DFCA 信息库中发布的证书已经签发给了订户，并且订户已经按照本 CP 的规定接受了该证书。

9.6.2 RA 的陈述与担保 RA Representations and Warranties

1. 提供给证书订户的注册过程完全符合本 CP 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 CP 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 Subscriber Representations and Warranties

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. 在证书的有效期内进行数字签名；

2. 订户在申请证书时向 RA 提供的信息均为真实、完整和准确的，愿意承担任何提供虚假、伪造等信息的法律责任；

3. 若存在代理人，那么订户和代理人两者负有连带责任，订户有责任就代理人所作的任何不实陈述与遗漏、通知 DFCA 或其授权的证书服务机构；

4. 与订户证书所含公钥相对应的私钥进行的每一次签名，均为订户自己的签名，并且在签名时，证书是有效证书（证书未过期、注销），证书的私钥为订户本身访问和使用；

5. 除非经订户和发证机构间书面协议明确规定，订户保证不从事发证机构（或类似机构）所从事的业务；

6. 一经接受证书，既表示订户知悉和接受本 CP 中所有条款和条件，并知悉和接受相应的订户协议；

7. 一经接受证书，订户就应当承担如下责任：始终保持对其私钥的控制，使用可信的系统，采取合理的预防措施来防止私钥的遗失、泄露、被篡改或未经授权使用；

8. 不得拒绝任何来自 DFCA 公示过的声明、改变、更新、升级等，包括但不限于策略、

规范的修改和证书服务的增加和删减等；

9. 证书在本 CP 中规定的使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的；

10. 采取安全、合理的措施来防止私钥的遗失、泄露、被篡改或未经授权使用等事件。

9.6.4 依赖方的陈述与担保 Relying Party Representations and Warranties

1. 遵守本 CP 的所有规定；

2. 在依赖证书前，确认证书在规定的范围和期限使用；

3. 在依赖证书前，对证书的信任链进行验证；

4. 在依赖证书前，通过查询 CRL 或 OCSP 确认证书是否被注销；

5. 一旦由于疏忽或其他原因违背了合理检查的条款，依赖方愿意就此而给 DFCA 带来的损失进行赔偿，并且因此造成怕自身或他人的损失；

6. 不得拒绝任何来自 DFCA 公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

9.6.5 其他参与者的陈述与担保 Representations and Warranties of Other Participants

其他参与者应遵守本 CP 的规定。

9.7 担保免责 Disclaimers of Warranties

除本 CP 的第 9.6.1 中明确承诺外，DFCA 不承担其他任何形式的保证和义务：

1. 不保证订户、依赖方、其他参与者的陈述内容；

2. 不对电子认证活动中使用的任何软件做出保证；

3. 不对证书在超出规定目的以外的应用承担任何责任；

4. 对由于不可抗力，如战争、自然灾害等造成的服务中断并由此造成的客户损失承担责任；

5. 订户违反本 CP 的第 9.6.3 之承诺时，或依赖方违反本 CP 的第 9.6.4 之承诺时，得以免除 DFCA 之责任。

9.8 有限责任 Limitations of Liability

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 Indemnities

9.9.1 认证机构的赔偿责任 Indemnification by DFCA

若 DFCA 违反本 CP 第 9.6.1 节中的陈述，订户、依赖方等实体可申请 DFCA 赔偿责任（法定或约定免责除外），包括以下情形：

1. DFCA 将证书错误地签发给订户以外的第三方，导致订户或依赖方遭受损失的；

2. 在订户提交信息或资料准确、属实的情况下，DFCA 签发的证书出现了错误信息，导致订户或依赖方遭受损失的；

3. 在 DFCA 明知订户提交信息或资料存在虚假谎报的情况，但仍然向订户签发证书，导致依赖方遭受损失的；

4. 由于 DFCA 的原因导致 CA 私钥的泄露；

5. DFCA 未能及时注销证书，导致依赖方遭受损失的。

9.9.2 订户赔偿责任 Indemnification by Subscribers

在如下情况下，订户对自身原因造成的 DFCA、依赖方损失，应当承担赔偿责任：

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；

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；

3. 订户使用证书的行为，有违反本 CP 及相关操作规范，或者将证书用于非本 CP 规定的业务范围；

4. 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，若该证书被用以进行非法交易，或者进行交易时产生纠纷的，若 DFCA 按照本 CP 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；

5. 证书中的信息发生变更，但未停止使用证书并及时通知 DFCA 和依赖方；

6. 没有对私钥采取有效的保护措施，导致私钥丢失或被损害、窃取、泄露等；

7. 在得知私钥丢失或存在危险时，未停止使用证书并及时通知 DFCA 和依赖方；

8. 证书到期但仍在使用证书；

9. 订户的证书信息侵犯了第三方的知识产权；

10. 在规定的应用范围外使用证书，如从事违法犯罪活动。

9.9.3 依赖方的赔偿责任 Indemnification by Relying Parties

在如下情况下，依赖方对自身原因造成的 DFCA、订户损失，应当承担赔偿责任：

1. 没有履行 DFCA 与依赖方的协议和本 CP 规定的义务；

2. 未能依照本 CP 规范进行合理审核，导致 DFCA 及其授权的证书服务机构或第三方遭受损害；

3. 在不合理的情形下依赖证书，如依赖方明知证书存在超范围、超期限使用的情形或证书已经或有可能被人窃取的情形，但仍然依赖证书；

4. 依赖方没有对证书的信任链进行验证；

5. 依赖方没有通过查询 CRL 或 OCSP 确认证书是否被注销。

9.10 有效期限与终止 Term and Termination

9.10.1 有效期限 Term

本 CP 在生效之日零时起正式生效，上一版本的 CP 同时失效。

本 CP 在下一版本 CP 生效之日或本 CP 终止之日时失效。

9.10.2 终止 Termination

DFCA 有权终止本 CP（包括其修订版本）。本 CP（包括其修订版本）自 DFCA 在其官网站公布终止声明的 30 日后终止。

9.10.3 效力的终止与保留 Effect of Termination and Survival

本 CP 的终止，意味着认证机构的认证业务的终止，但认证业务的终止不意味着认证机构的责任终止。认证机构的业务终止后应采取合理的措施，将认证服务转让到其他认证机构，保证订户的利益。

9.11 对参与者的个别通告与沟通 Individual Notices and Communications with Participants

认证机构在必要的情况下，如主动注销订户证书、发现订户将证书用于规定外用途和订户其他违反订户协议的行为，可通过适当方式，如电子邮件等，个别通知订户、依赖方。

9.12 修订 Amendments

9.12.1 修订程序 Procedure for Amendment

经 DFCA 的安全策略委员会授权，DFCA 行政管理部门每年至少审查一次本 CP，确保

其符合国家法律法规、主管部门的要求以及相关国家标准，符合认证业务开展的实际需求。

本 CP 的修订，由 DFCA 安全策略管理委员会指定 CP 编写小组负责起草 CP 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；CP 编写小组依据策略管理委员会评审意见完成 CP 修改、确定 CP 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 Notification Mechanism and Period

本 CP 在 DFCA 的网站上发布。

版本更新时，最新版本的 CP 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 Circumstances Under Which CP Must be Changed

如果出现下列情况，DFCA 必须对本 CP 进行修改：

1. 密码技术出现重大发展，足以影响现有 CP 的有效性；

2. 有关认证业务的相关标准进行更新；

3. 认证系统和有关管理规范发生重大升级或改变；

4. 法律法规和主管部门要求；

5. 现有 CP 出现重要缺陷。

9.13 争议处理 Dispute Resolution Provisions

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，根据本 CP 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 或授权机构就本 CP 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 Governing Law

本 CP 受中华人民共和国法律和法规的管辖，包括但不限于《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》等。

9.15 与适用法律的符合性 Compliance with Applicable Law

本 CP 必须符合《中华人民共和国电子签名法以》、《电子认证服务管理办法》、《电子认证服务密码管理办法》以及其他中华人民共和国法律法规的规定。

9.16 一般条款 Miscellaneous Provisions

9.16.1 完整协议 Entire Agreement

本 CP 将替代先前的、与主题相关的书面或口头解释。CPS、CP、订户协议、依赖方协议及其补充协议构成各参与者之间的完整协议。

9.16.2 转让 Assignment

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 Severability

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 Enforcement

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 Force Majeure

依据本 CP 制定的 CPS 应包括不可抗力条款，以保护各方的利益。

9.17 其他条款 Other Provisions

DFCA 对本 CP 拥有最终解释权。