物联网装置嵌入式设备身份鉴权应用证书

证书策略

V1.0

发布日期：2017 年 7 月

生效日期：2017 年 7 月

东方新诚信数字认证中心公司

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）

本文档描述 DFCA 的物联网装置嵌入式设备身份鉴权证书（简称为“嵌入式设备证书”）的证书策略（CP），是 DFCA 开展嵌入式设备证书服务的策略声明，适用于所有由 DFCA 签发和管理的嵌入式设备证书及相关参与主体。

物联网装置嵌入式设备证书（简称为“嵌入式设备证书”）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。

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 证书策略架构 Certificate Policy Architecture

本 CP 是 DFCA 关于嵌入式设备证书的最高证书策略。DFCA 按照 CP 制定 CPS，按照本 CP 及相关 CPS 进行证书服务，订户、依赖方及其他相关实体按照本 CP 和相关的 CPS 决定对证书的使用、信任并履行相关的义务。

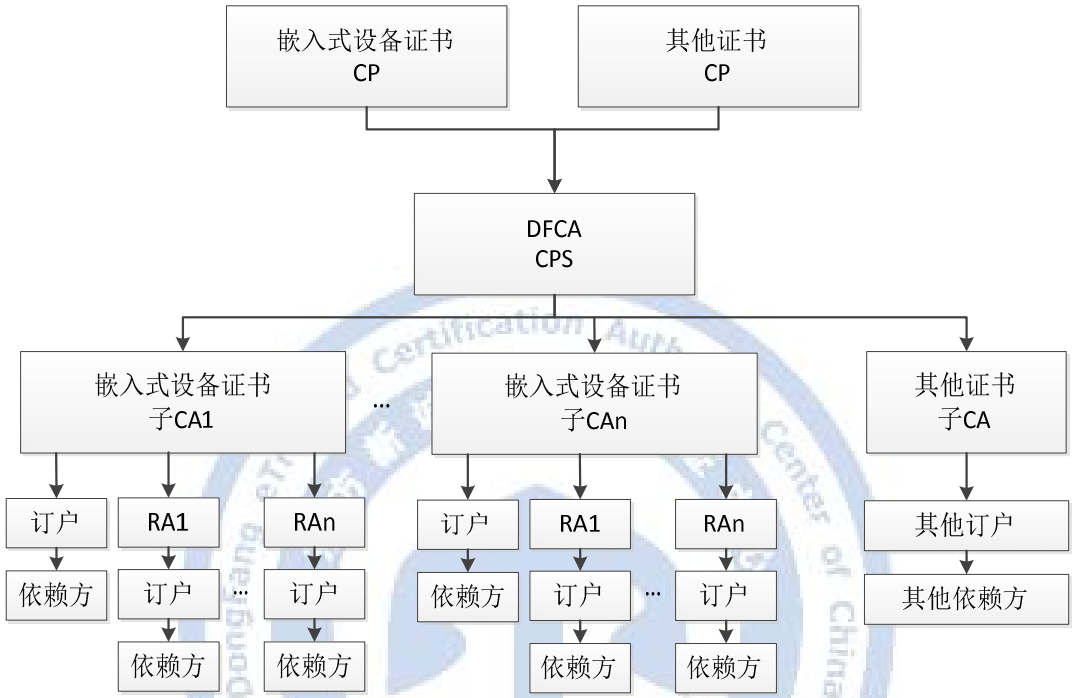

图 1-1 嵌入式设备证书的证书策略架构

1.1.4 证书层次架构 Hierarchical Architecture of Certificates

说明本 CP 所支持的证书信任链体系，包括密码算法、密钥长度、证书类型、根证书有效期等。

嵌入式设备证书的证书层次架构如图 1-2 所示。

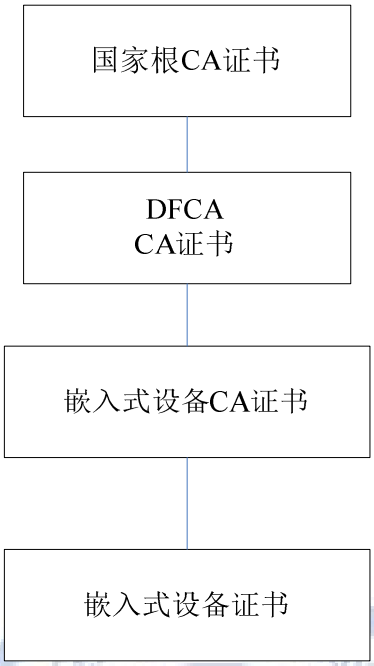

图 1-2 嵌入式设备证书层次架构

1. 国家根 CA 证书是国家密码主管部门的根证书。国家根 CA 证书的密码算法为 SM2，密钥长度为 256bit；

2. DFCA 的 CA 证书是 DFCA 的认证机构证书，密码算法为 SM2，密钥长度为 256bit。该 CA 证书由国家根 CA 证书签发；

3. 嵌入式设备 CA 证书由 DFCA 的 CA 根证书签发。密码算法为 SM2，密钥长度为 256bit；

4. 使用嵌入式设备 CA 证书签发每一个嵌入式设备证书，密码算法为 SM2，密钥长度为 256bit。

1.2 文档名称与标识 Document Name and Identification

本文档名称是《物联网装置嵌入式设备身份鉴权应用证书-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。

DFCA 是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。

1.3.2 注册机构 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用户的数据，不允许将用户数据透露给与证书申请无关的任何单位或个人，不允许将用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

订户，即证书持有人，是指从 DFCA 接收证书的实体，即该实体从 DFCA 接收嵌入式设备证书，将该证书集成在其拥有的物联网装置中的单位或个人。

订户代表着证书中公钥所绑定的唯一实体，拥有对与其证书唯一对应的私钥的最终控制权。订户在本 CP 的范围内使用证书，并承担本 CP 约定的义务。

1.3.4 依赖方 Relying Parties

依赖方是指任何使用 DFCA 签发的嵌入式设备证书进行网络作业的证书持有者和按照本 CP 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 DFCA 的嵌入式设备证书服务体系中，依赖方是信任 DFCA 所签发的嵌入式设备证书（以下简称为“证书”），可以对使用嵌入式设备证书机制生成的数字签名进行验证，使用嵌入式设备证书公钥的实体。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，除了未经验证的用户信息外，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

嵌入式设备证书包括签名证书、加密证书。嵌入式设备证书主要适合以下四方面的应用。

1. 身份认证：各类集成了嵌入式设备证书的物联网装置之间，可使用嵌入式设备证书进行相互之间的网络身份认证；

2. 电子签名：使用嵌入式设备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；

3. 信息保护：使用嵌入式设备证书，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：使用嵌入式设备证书，对嵌入式设备的网络行为日志进行电子签名，确保嵌入式设备的网络行为的不可抵赖性。

在本 CP 中，为嵌入式设备证书的证书策略标识定义为：1.2.156.112559.1.34.1.2

1.4.2 限制的证书应用 Prohibited Certificate Uses

嵌入式设备证书仅用于嵌入式设备的应用。

除上述要求外，特别强调的其他限制的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；

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。

1.5 策略管理 Policy Administration

1.5.1 策略管理机构 Organization Administering the Policy

DFCA 安全策略委员会是本 CP 的最高管理机构，负责制定、维护和解释本 CP。

1.5.2 联系人 Contact Person

详细说明本 CP 的联系人信息

联系部门：行政管理部门

联 系 人：颜先生

邮件地址：dfca-cps@chinaonenet.com

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

邮政编码：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 安全策略委员会组织制定，报 DFCA 安全策略委员会批准执行，包括本 CP 的修订和版本变更。

DFCA 安全策略委员负责评估 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

1. DFCA 安全策略委员组织相关人员成立“CP 编制工作小组”，负责起草或修订本 CP；

2. CP 编制工作小组完成本 CP 的编制工作，提交 DFCA 安全策略委员审核批准；

3. 本 CP 经 DFCA 安全策略委员审批通过后，严格遵循国家相关管理办法的要求，向国家相关主管部门备案并对外发布。

1.5.5 CP 修订 CP Revision

DFCA 根据国家的政策、法律法规、技术要求、以及业务发展情况及时对本 CP 进行修订。

本 CP 每两年修订一次。如果没有内容改动，则只递增版本号，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. 电子认证服务机构

受用户信任，负责创建和分配用户密钥和公钥证书的权威机构。

2. 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挂起证书，处理订户撤销或挂起证书的请求，同意或拒绝订户更新其证书或密钥的请求。

3. 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。

4. 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。

5. 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。

6. 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。

1.6.2 缩略语 Acronyms

按国标体例要求编写本 CP 中的缩略语。

CA	电子认证服务机构（Certificate Authority）
CP	证书策略（Certificate Policy）
CPS	电子认证业务规则（Certificate Practice Statement）
CRL	证书撤销列表（Certificate Revoke List）
LDAP	轻量级目录访问协议（Lightweight Directory Access Protocol）
OCSP	在线证书状态协议（Online Certificate Status Protocol）
PIN	个人识别码（personal identification number）
RA	证书注册机构（Registration Authority）

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

2.1 信息库 Repositories

DFCA 为嵌入式设备证书建立专门的信息库。该信息库用于保存、取回嵌入式设备证书及相关的信息。嵌入式设备证书信息库包括但不限于以下内容：证书、CRL、嵌入式设备证书管理平台、CP、CPS、技术支持手册、DFCA 网站信息以及 DFCA 不定期发布的信息。

信息库不会对 DFCA 发出的任何证书和证书注销信息进行修改，只会准确地描述上述信息。

2.2 认证信息的发布 Publication of Certification Information

DFCA 在官方网站 http://www.dfca.cn 发布信息库。

DFCA 通过 LDAP 发布嵌入式设备证书的状态和 CRL，订户和依赖方可通过访问 DFCA 的 LDAP 获取嵌入式设备证书的状态、CRL 等。

DFCA 提供嵌入式设备证书的 OCSP 服务。其他信息库可以通过访问 DFCA 官方网站：http://www.dfca.cn 查询。

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

1. 证书/CRL 的发布时间与频率

(1) 证书一经签发，就即时在 DFCA 的目录服务器上发布；

(2) 嵌入式设备证书的 CRL 每 24 小时发布一次；在紧急情况下，DFCA 可自行决定 CRL 的发布时间与频率。

2. 其他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 http://www.dfca.cn 发布与嵌入式设备

证书相关的公告与通知；

(2) 这类信息不定期发布，DFCA 将保证在第一时间发布信息。

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 等信息，DFCA 允许公众自行通过网站和目录服务器进行查询与下载。

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。

只有经授权的系统管理员可以查询信息库中其他数据。

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

DFCA 的嵌入式设备证书符合 X.509 标准，配给证书持有者的甄别名（DN, Distinguished Name）采用 X.500 的命名方式。

3.1.2 对命名有意义的要求 Needs for Names to be meaningful

DN 是嵌入式设备证书的唯一甄别名，在数字证书的主体名称域中，用来唯一标识一个物联网装置的身份。

3.1.3 订户的匿名或伪名 Anonymity or Pseudonymity of Subscribers

无规定。

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。

3.1.5 命名的唯一性 Uniqueness of Names

DFCA 保证其签发的嵌入式设备证书，其主体甄别名在 DFCA 的信任域内是唯一的。

3.1.6 商标的识别、鉴别和角色 Recognition, Authentication, and Role of Trademarks

无规定。

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

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 Authentication of Organization Identity

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。鉴别组织机构的身份时，指定证书申领者须向发证机构提供有效证明文件，在填写申领表时加盖机构公章以证明该申领的有效性。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 Authentication of Individual Identity

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，包括但不限于个人身份证或军官证等由政府机构颁发的能够证明个人身份的有效证件。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 没有验证的订户信息 Non-Verified Subscriber Information

无规定。

3.2.5 授权确认 Validation of Authority

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。

3.2.6 互操作准则 Criteria for interoperation

对于其他的电子认证服务机构，也可与 DFCA 进行互操作。该电子认证服务机构的 CPS 须符合本 CP 的要求，并且与 DFCA 签署相应的协议。DFCA 根据协议，接受其他电子认证服务机构鉴别过的信息，并为订户签发嵌入式设备证书。

如果国家法律法规对此规定，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

3.3.1 概述 Overview

嵌入式设备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。

嵌入式设备证书不支持证书更新、密钥更新等业务。

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

无规定。

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

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。

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

证书注销请求的标识与鉴别流程见本 CP 的 4.10.3。

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

4.1 概述 Overview

本章阐述了 DFCA 根据公布的本 CP 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）。

4.2.2 申请过程与责任 Application Process and Responsibilities

4.2.2.1 申请过程 Application Process

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。

4.2.2.2 责任 Responsibilities

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。

4.3 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。

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 或授权的 RA 对订户提交的申请材料及身份信息进行鉴别，鉴别其是否完整、真实、有效。经鉴别符合要求后，将批准证书申请。

4.3.2.2证书申请的拒绝 Rejection of Certificate Applications

DFCA 或授权的 RA 对订户提交的申请材料及身份信息进行鉴别，鉴别其是否完整、真实、有效。经鉴别不符合要求，将拒绝证书申请。

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

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。

4.4 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

嵌入式设备证书采用了预植证书的方式。DFCA 按本 CP 定义的证书格式，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。

4.4.2 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 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，通知订户到注册机构领取数字证书；

2. 注册机构把证书等直接提交给用户，来通知订户证书信息已经正确生成；

3. 邮政信函通知用户；

4. 其他 DFCA 认为安全可行的方式通知用户。

4.5 证书接受 Certificate Acceptance

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

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。

4.5.2 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目录服务器中，供用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 所签发的嵌入式设备证书后，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。订户接收到嵌入式设备证书，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。只有在接受了所申请的嵌入式设备证书之后，用户才能使用证书对应的私钥。在证书被注销之后，用户必须停止使用该证书对应的私钥。

4.6.2 信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嵌入式设备证书，依赖方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以下内容：

1. 获取数字签名对应的证书和 CA 证书；
2. 确认该签名对应的证书与 CA 证书是依赖方信任的证书；
3. 确认数字签名与证书的适用范围一致；
4. 使用证书公钥对数字签名进行验证；
5. 验证数字签名对应的证书的状态正常，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 证书更新 Certificate Renewal

4.7.1 证书更新的情形 Circumstances for Certificate Renewal

嵌入式设备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。

嵌入式设备证书不支持证书更新业务。

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

无规定。

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

无规定。

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

无规定。

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

无规定。

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

无规定。

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

无规定。

4.8 证书密钥更新 Certificate Rekey

4.8.1 证书密钥更新的情形 Circumstances for Certificate Rekey

嵌入式设备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。

嵌入式设备证书不支持证书密钥更新业务。

4.8.2 请求证书密钥更新的实体 Who May Request Certification of a New Public Key

无规定。

4.8.3 证书密钥更新请求的处理 Processing of Certificate Rekeying Requests

无规定。

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

无规定。

4.8.5 构成接受密钥更新证书的行为 Conduct Constituting Acceptance of a Rekeyed Certificate

无规定。

4.8.6 CA 对密钥更新证书的发布 Publication of the Rekeyed Certificate by the CA

无规定。

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

无规定。

4.9 证书变更 Certificate Modification

4.9.1 证书变更的情形 Circumstances for Certificate Modification

嵌入式设备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。

嵌入式设备证书不支持证书变更业务。

4.9.2 请求证书变更的实体 Who May Request Certificate Modification

无规定。

4.9.3 证书变更请求的处理 Processing of Certificate Modification Requests

无规定。

4.9.4 证书变更时对订户的通告 Notification of New Certificate Issuance to Subscriber

无规定。

4.9.5 构成接受变更证书的行为 Conduct Constituting Acceptance of Modified Certificate

无规定。

4.9.6 CA 对变更证书的发布 Publication of the Modified Certificate by the CA

无规定。

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

无规定。

4.10 证书注销 Certificate Revocation

4.10.1 证书注销的情形 Circumstances for Revocation

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) 订户不能实际履行本 CP。

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。

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

在符合本 CP4.10.1 所述的情形下，请求证书注销的实体与本 CP4.10.1 证书申请实体相同。

另外，DFCA、证书依赖方、订户所属组织机构也可以在本 CP4.10.1 所述的情形下注销（或申请注销）订户的证书。

4.10.3 注销请求的流程 Procedure for Revocation Request

在主动注销的情况下，证书注销请求的流程说明如下。

1. 证书注销的申请人通过在线方式或离线方式填写《证书注销申请表》，并注明注销原因；
2. DFCA 或其授权的 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，订户的证书在 24 小时内进入 CRL，向外界公布。

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。

4.10.4 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 DFCA 或其授权的 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目录服务器，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。

4.10.7 CRL 发布频率 CRL Issuance Frequency

CRL 的发布周期为一日，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 向订户和依赖方提供在线证书状态查询服务。该服务 7*24 小时可用。

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。

4.10.11 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，应立即注销证书。

4.10.13 证书挂起的情形 Circumstances for Suspension

证书挂起是证书撤销的一种特殊情形， 由于某种原因暂停使用证书。

嵌入式设备证书不支持证书挂起业务。

4.10.14 请求证书挂起的实体 Who Can Request Suspension

无规定。

4.10.15 挂起请求的流程 Procedure for Suspension Request

无规定。

4.10.16 挂起的期限限制 Limits on Suspension Period

无规定。

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、OCSP 等方式，查询证书状态。

4.11.2 服务可用性 Service Availability

原则上，DFCA 提供 365 天×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，每天用户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正式结束：

1. 证书被注销。

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

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。

4.13.2 会话密钥的封装与恢复的策略与行为 Session Key Encapsulation and Recovery Policy and Practices

无规定。

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. 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》。

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。

其他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

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，UPS 可以保证供电 8 小时，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。

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。

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 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

所备份的业务数据磁带（光盘、移动存储介质等）均送到位于异地的 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

16. 其他

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 应在具体业务规范中对关键任务进行严格控制，确保多个可信角色共同参与完成一些敏感任务。

1. 密钥和密码设备的操作，需要 3 个（或 3 个以上）密钥管理人员的半数以上密钥管理人员共同完成；

2. 证书认证系统中有关人员管理、权限分配等操作，需要 2 名可信人员共同完成；

3. 审核和签名证书，需要 2 名可信人员共同完成。

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 Roles Requiring Separation of Duties

为保证系统安全，遵循可信角色分离的原则，DFCA 的可信角色应由不同的人担任。需要职责分割的角色包括但不限于：

1. 证书业务受理：应通过业务办理人员（或录入人员）、审核人员、鉴别验证人员、业

务执行人员等多个角色进行才能完成；

2. CA 密钥管理：至少半数以上的密钥管理员，才能进行密钥管理的操作；

3. 系统人员管理：需要 2 名系统管理员，才能对下辖的可信人员进行管理与授权；

4. 系统工程实施：在系统遇到紧急情况需要联合抢修时，DFCA 至少派遣 1 名工作人员在场。抢修人员需在 DFCA 工作人员陪同下，执行许可的操作。所有的操作、修改都保留记录。

5. 安全审计：由审计管理员负责授权审计员，审计员负责安全审计工作。

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

DFCA 对可信人员的资格要求如下：

1. 具备良好的社会和工作背景；
2. 无民事不良记录、违法犯罪记录；
3. 遵守国家法律、法规，服务 DFCA 的统一安排与管理；
4. 遵守 DFCA 有关安全管理的规范、规定的制度；
5. 具备良好的个人素质、修养以及认真负责的工作态度；
6. 具备良好的团队合作精神；
7. 无影响 DFCA 运行的其他兼职工作；
8. 无电子认证服务行业重大错误或失信记录。

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，完成对可信人员的背景调查。

所有的可信人员和申请调入的可信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. 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，与员工签订保密协议，以约束员工不许泄漏 CA 证书服务的所有保密和敏感信息；
5. DFCA 将按照本机构的人员管理相关条例对所有承担可信角色的在职人员进行职位考察，以持续验证这些人员的可信程度和工作能力。

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：

1. DFCA 的安全原则和机制、岗位职责；
2. PKI 基础基础；
3. 电子认证系统相关软、硬件的安装与维护；
4. 电子认证系统的操作与使用；
5. DFCA 的业务管理相关的流程、标准与规范；
6. DFCA 的运行管理相关的规章、制度与管理办法；
7. 国家电子认证相关的法律法规与政策；
8. 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 DFCA 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 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 应建立并维护一套管理办法，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 必须记录与运行系统相关的事件。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，应包含以下信息：

1. 事件发生的时间
2. 日志的记录号
3. 事件的内容
4. 事件相关的实体
5. 事件的结果状态
6. 日志的来源

DFCA 应记录的事件包括但不限于：

1. CA 密钥生命周期的管理事件，包括 CA 密钥生成、存储、使用、注销、归档、备份、恢复、销毁、私钥泄露等；

2. 密钥设备生命周期的管理事件，包括设备的接收、安装、激活、使用、维修等；

3. 证书申请事件，包括申请数据的接收、验证、存储等；

4. 证书生命周期内的管理事件，包括证书的申请、注销、挂起等；

5. 系统管理事件，包括 CA 系统的安装、使用、配置、维护、升级、运行故障等；

6. 主机管理事件，包括 CA 系统相关的软、硬件设备（例如服务器、存储设备、数据库系统、操作系统等）的安装、使用、维修、升级、运行异常等；

7. 网络环境的管理事件，包括防火墙、入侵检测系统、漏洞扫描系统、交换机等网络安全系统和网络设备记录的网络安全事件；

8. 物理环境的管理事件，包括物理分区的进出，以及屏蔽系统、电源、门禁、视频、消防等物理环境设施的安装、操作、维修等；

9．可信人员管理记录，包括网络权限的账号申请记录、系统权限的申请、变更、创建申请记录，人员情况变化等。

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 应妥善保存电子认证服务的审计日志，保存期限为 10 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，另外对日志进行异地备份。审计日志的制作和访问进行岗位分离。

DFCA 将审计日志存储到磁带中，并存放到异地，实行安全保管。

5.4.5 审计日志备份程序 Audit Log Backup Procedures

DFCA 保证所有的审查记录和审查总结均按照 DFCA 备份标准和程序进行备份。根据记录的性质和要求，分为按天、按周、按月和按年等多种形式的备份，采用在线和离线两种方式的备份工具。

审计文档由管理员每月进行一次归档。所有档案安全存放在文档库内。

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

审计记录报告一个事件时，应通知引起该事件的个人、组织机构。

5.4.8 脆弱性评估 Vulnerability Assessments

DFCA 每年对系统进行脆弱性评估，并根据评估报告采取补救措施。

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

所有归档记录的保存期限应符合国家电子认证服务主管部门对归档记录的要求。

5.5.3 归档文件的保护 Protection of Archive

归档文件存放在专门的档案室中，具有适当的物理防护措施。

只有授权的可信人员可按照特定的安全方式访问归档文件，防止未经授权的浏览、修改、删除或其他的篡改行为。

5.5.4 归档文件的备份程序 Archive Backup Procedures

对于系统生成的电子归档记录，定期地进行备份。备份文件存放在从银行租赁的保险柜中。

对于书面的归档资料，不需要进行备份，采取严格的措施保证其安全性。

5.5.5 记录时间戳要求 Requirements for Time-Stamping of Records

无规定。

5.5.6 归档收集系统 Archive Collection System

DFCA 和各 RA 均在内部建设归档收集系统。

5.5.7 获得和检验归档信息的程序 Procedures to Obtain and Verify Archive Information

由审计员、业务管理员分别保留归档数据的两个拷贝。在获得完整档案信息时，须对这两个拷贝进行比较。

DFCA 每年组织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 Key Changeover

CA 证书到期时，DFCA 将生成新的 CA 签名密钥对，并对 CA 证书进行更新。

在生成新的 CA 签名密钥对时，须严格遵守 DFCA 关于密钥管理的规范。新的密钥对产生时，由国家密码主管部门签发新的 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

如果出现计算机资源、软件或数据损坏事件，DFCA 立即启动事故处理程序。如有必要，可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有关政府主管部门汇报，通过网站和其他公共媒体对订户进行通告，采取措施保证用户利益不受损失；
2. 立即注销所有已经被签发的证书，更新 CRL，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 CA 证书；

3. 新的 CA 证书签发以后，按照本 CP 关于证书签发的规定，重新签发下级 CA 证书和订户证书；

4. 新的 CA 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。

5.7.4 灾难后的业务连续性能力 Business Continuity Capabilities After a Disaster

1、对于核心业务系统，证书签发系统和证书接口系统采用备份方式；

2、对于核心数据库，采用磁盘阵列方式来确保数据库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 或其 RA 需要停止其业务时，必须严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》及相关法规中对认证机构终止电子认证服务的规定要求进行有关工作。

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、用户信息、系统文件、CP、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 RA 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。

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

CA 密钥对的生成由国家密码主管部门批准和许可的硬件密码设备生成。密钥的生成、管理、存储、备份和恢复应符合国家关于数字认证系统的相关标准规范。

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

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 Private Key Delivery to Subscriber

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 Public Key Delivery to Certificate Issuer

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

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

依赖方可以从 DFCA 的网站或目录服务器下载 CA 证书，从而得到 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。

DFCA 遵从国家密码主管部门对密码算法的规定和要求。

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

公钥参数须使用国家密码主管部门批准和许可的硬件密码设备产生。公钥参数质量的检查也由这类密码设备进行。

6.1.7 密钥使用目的 Key Usage Purposes

嵌入式设备证书采用 X.509 V3 证书格式，证书包含了密钥用法扩展项。如果 DFCA 在其签发证书的密钥扩展项指明了密钥用途，订户和依赖方应必须按照该指明的用途使用密钥。

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 应使用经国家密码主管部门批准和认可的硬件密码设备。

6.2.2 私钥的多人控制 Private Key Multi-Person Control

CA 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 M 选 N 方式，将私钥的管理权限分散到 M 张密钥卡中，只有其中 N 人在场并许可的情况下，才能对私钥进行上述操作。其中，M 为不少于 3 的奇数，N 不小于 M 的二分之一。

用户的签名私钥存储在安全的嵌入式芯片中，DFCA 不保留任何备份。

6.2.3 私钥托管 Private Key Escrow

订户证书的签名私钥由自己保管，DFCA 不负责托管。

6.2.4 私钥备份 Private Key Backup

1. CA 密钥的备份，采用密码设备提供密钥备份机制。其中，备份数据应采用本 CP 第 6.2.2 节要求的安全控制技术；

2. 订户证书的签名密钥 DFCA 不予备份；加密密钥由 DFCA 的密钥管理中心进行备份，备份数据以密文形式保存。

6.2.5 私钥归档 Private Key Archival

1. CA 私钥到期后，使用满足本 CP 第 6.2.1 节要求的硬件密码设备归档保存。归档期限应满足本 CP 第 5.5.2 节的要求；

2. 订户签名私钥由订户保管，DFCA 不留存备份，没有归档业务；订户加密私钥到期

后，通过数据库备份出来，存储在脱机存储介质上进行归档保存。归档期限应满足本 CP 第 5.5.2 节的要求。

6.2.6 私钥导入、导出密码模块 Private Key Transfer Into or From a Cryptographic Module

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，DFCA 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 Private Key Storage on Cryptographic Module

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 Method of Activating Private Key

1. 对于 CA 私钥，其激活数据按本 CP 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，嵌入式设备证书签发后默认为激活状态。

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

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，进行冻结私钥的操作；

2. 对于订户私钥，不支持私钥冻结。

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

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，应妥善保存一定期限，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，需将 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 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，方可进行该操作。

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。

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

DFCA 应将 CA 证书和订户证书归档。归档的证书可存放在数据库中。

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

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。

对于嵌入式设备证书，不支持证书到期后，使用原密钥对证书进行更新。

6.4 激活数据 Activation Data

嵌入式设备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 Activation Data Generation and Installation

无规定。

6.4.2 激活数据的保护 Activation Data Protection

无规定。

6.4.3 激活数据的其他方面 Other Aspects of Activation Data

无规定。

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 已通过国家密码主管部门组织的安全性审查。

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。

所有设备从采购到上线前，均进行安全性检查。密码设备的采购与安装，在更加严格的安全控制机构下，进行检验、安装与验收。

对废旧设备进行处理时，必须确认其是否有影响认证业务安全性的信息存在。

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主管部门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 暂不采用时间戳。

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

7.1.1 证书格式 Certificate Format

嵌入式设备证书遵循 X.509 V3 版证书格式。

7.1.2 版本号 Version Number(s)

V1.0。

7.1.3 证书扩展项 Certificate Extensions

嵌入式设备证书使用 X.509 V3 版证书标准扩展项。

7.1.4 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。

7.1.5 名称形式 Name Forms

DFCA 签发的嵌入式设备证书采用 X.500 定义的甄别名称（DN）标准来唯一标识一张证书使用者的身份信息。DN 必须包括以下四部分：

（1） CN

CN 部分包括 10 个字符，由数字和字母组成，字母区分大小写：

前 2 位由发证机构自行定义；

后 7 位表示各发证机构发放的证书数量，按照各发证机构发放证书的顺序，逐渐累加；

最后 1 位为随机产生的校验码。

示例：CN=A100002619, CN=2E00011206

（2） OU

OU 部分用来表示此证书为嵌入式设备证书的类型，具体表示为：

OU＝QRSshebei

（3） O

O 部分：用来表示 CA 系统的英文简称，表示为：

O=DFCA Embedded CA

（4） C

C 部分用来表示中国的英文简称，全部大写。

C=CN

7.1.6 名称限制 Name Constraints

DFCA 签发的嵌入式设备证书，其名称须严格按照 7.1.5 的规则来定义。

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

嵌入式设备证书的证书名称中包含了证书类型，标识证书所使用的证书策略。

7.1.8 策略限制扩展项的用法 Usage of Policy Constraints Extension

无规定。

7.1.9 策略限定符的语法和语义 Policy Qualifiers Syntax and Semantics

无规定。

7.1.10 关键证书策略扩展项的处理规则 Processing Semantics for the Critical Certificate Policies Extension

无规定。

7.2 证书注销列表 CRL Profile

DFCA 签发的嵌入式设备证书注销列表符合 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

DFCA 为用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)

OCSP 版本 V1.0 。

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

1. DFCA 应每季度进行一次内部审计，每次审计抽取不少于 5%的证书进行评估，以保证证书服务的可靠性、安全性和可控性。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。

2. 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、本 CP、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 Identity/Qualifications of Assessor

DFCA 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：

1. DFCA 的安全负责人及安全管理人员；
2. DFCA 业务负责人；
3. 认证系统及信息系统负责人；
4. 人事负责人；
5. 其他需要的人员。

外部审计机构的资质，应具备以下资质：

1. 必须是有执业资格的评估机构，有良好的声誉；
2. 熟悉计算机信息安全、电子认证服务相关的要求、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. 具备独立审计的能力或案例。

8.3 评估者与被评估者之间的关系 Assessor's Relationship to Assessed Entity

1. DFCA 的内部审计人员与本机构的系统管理员、业务管理员、业务操作员等工作岗位不能重叠；

2. 外部评估者和 DFCA 之间是独立关系，无业务往来、无财务关联。或者无其他任何厉害关系，该关系足以影响评估的客观性。

8.4 评估内容 Topics Covered by Assessment

审计所涵盖的主题包括：

1. 安全策略是否得到充分的实施；

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、业务规范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。

8.5 对问题与不足采取的措施 Actions Taken as a Result of Deficiency

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 DFCA 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，DFCA 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 Communications of ResultS

除非国家法律法规或相关管理办法的明确要求，一般不公开评估结果。

对于关联方，将依据签署的协议来公布评估结果。

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

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

根据证书实际应用的需要，DFCA 与客户在公平公正的商业氛围中签订协议进行收取。若 DFCA 签署的协议中指明的价格与 DFCA 公布的价格不一致，以协议中的价格为准。

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。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。

若用户提出的特殊需求，需要 DFCA 支付额外的费用。DFCA 根据证书实际应用的需要，与客户在公平公正的商业氛围中签订协议进行收取。

9.1.3 证书注销或状态信息的查询费用 Revocation or Status Information Access Fees

对于证书注销或状态信息的查询服务，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。

若用户提出特殊需求，需要 DFCA 支付额外的费用，DFCA 根据证书实际应用的需要，与客户在公平公正的商业氛围中签订协议进行收取。

9.1.4 其他服务的费用 Fees for Other Services

可根据请求者的要求，订制各类通知服务。

具体服务费用，在 DFCA 与订制者签订的协议中约定。

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。一旦订户接受数字证书，DFCA 将不办理退款手续。

9.2 财务责任 Financial Responsibility

9.2.1 保险范围 Insurance Coverage

保险范围主要针对本 CP 第 9.9 节中所规定的赔偿。

9.2.2 其他资产 Other Assets

无规定。

9.2.3 对最终实体的保险或担保 Insurance or Warranty Coverage for End-Entities

订户一旦接受 DFCA 的证书，或者通过协议完成对证书服务的接受，意味着该订户已经接受了本 CP 关于保险和担保的规定和约束。

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

保密信息包括但不限于以下方面：

1. 订户的签名私钥；

2. DFCA 的审计记录，包括：认证系统日志、服务器日志、归档日志等。除法律要求

外，不可在公司外部发布；

3. 除本 CP 第 9.3.2 节规定的信息外，其他由 DFCA 和 RA 保存的订户信息。

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

1. DFCA 签发的证书、以及证书中的公钥和订户信息；

2. DFCA 签发的 CRL；

3. 本 CP

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

证书申请人提供的不构成数字证书内容的信息，被视为隐私信息。

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

订户证书内包括的信息，以及该证书的状态等，是可以公开的，不被视隐私信息。

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

DFCA 在其认证业务范围内使用所获得的任何订户信息，只用于订户身份识别、管理和服务订户的目的。在使用这些信息时，无论是否涉及到隐私，DFCA 均没有告知订户的义务，也无需得到订户的同意。

DFCA 在任何法律法规或法院以及公权力部门通过合法程序的要求下，或者信息所有者书面授权的情况下，向特定对象披露隐私信息时，也没有告知订户的义务，并且无需得到订户的同意。

若 DFCA、RA 需要将订户隐私信息用于双方约定的用途以外的目的，事前必须告知订户并获得订户的同意和授权，而且这种同意和授权要用可归档的方式（信函、传真等）。

9.4.6 依法律或行政程序的信息披露 Disclosure Pursuant to Judicial or Administrative Process

由于法律执行、法律授权的行政执行的需要，DFCA 将订户的隐私信息提供给有关执法机构、行政执行机关是允许的。包括：

1．政府法律法规的规定并且经相关部门通过合法程序提出申请；

2．法院以及公权力部门处理因使用证书产生的纠纷时合法地提出申请；

3．具有合法司法管辖权的仲裁机构的正式申请。

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

1. DFCA 享有并保留对证书以及 DFCA 提供的所有软件的全部知识产权；

2. DFCA 对数字证书系统软件具有所有权、名称权、利益分享权；

3. DFCA 网站上公布的一切信息均为 DFCA 财产。未经 DFCA 书面许可，他人不能转载用于商业行为；

4. DFCA 发行的证书和 CRL 均为受 DFCA 支配的财产；

5. 对外运营策略和规范为 DFCA 财产；

6. 用于表示目录中 DFCA 域中实体的甄别名以及该域中颁发给终端实体的证书，均为 DFCA 的财产。

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 签发给订户的嵌入式设备证书完全符合本 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，则申请人代表拟定可使用条款；

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、注册机构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注册机构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，DFCA 只承担法律范围内的有限责任和本 CP 第 9.9.1 节中规定的有限责任。

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，如电话、电子邮件、信函等，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 行政管理部门提出公告，获得 DFCA 安全策略委员会批准，由 DFCA 行政管理部门负责组织修订。修订后的 CP 经 DFCA 安全策略委员会批准后正式对外发布。

9.12.2 通知机制和期限 Notification Mechanism and Period

本 CP 在 DFCA 的网站上发布。

在版本更新时，最新版本的 CP 立即在 DFCA 的网站发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，DFCA 将在合理的时间内通知有关各方。合理的时间应保证有关方受到的影响最小。

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（如密码算法更替等），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

当 DFCA、订户、依赖方之间出现争议时，有关方面应依据协议通过协议解决，协议解决不了的，可通过法律解决。

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《中华人民共和国密码法》、《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《中华人民共和国密码法》、《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

根据本 CP 中详述的认证实体各方的权利和义务，各方当事人不能通过任何形式转让给其他方。

9.16.3 分割性 Severability

如果本 CP 的任何条款或其应用由于与 DFCA 所在管辖区的法律产生冲突而被判定为无效或不不具执行力时，DFCA 应在最低要求的限度下修订该条款，使其继续有效，其他部分不受影响，DFCA 应在此章节披露修订的内容。

若法律不再适用，则本章节中任何对 DFCA 业务操作的调整不再继续适用。

上述就业务操作进行的相关调整，对 DFCA 的 CPS 的修订，应在 5 天内完成。

9.16.4 强制执行 Enforcement

无规定。

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。