



---

---

# 中国移动 CMCA 全球信任证书证书策略和 电子认证业务规则

---

---

**<版本：V2.1>**

**生效日期：2023 年 6 月 1 日**

## **CMCA Global Trust Certificate Policy and Certification Practice Statement**

**<Version: V2.1>**

**Effective date: June 1, 2023**

**卓望数码技术（深圳）有限公司**

**Aspire Digital Technology (Shenzhen) Co., Ltd**

文档版本控制表			
名称及版本	主要修改说明	完成时间	修改人
V0.1	新建文档	2020.4.10	委员会工作组
V0.1A	修订文档	2020.4.22	委员会工作组
V1.0.1	修订文档	2021.8.10	委员会工作组
V2.0	修正文档格式，完善证书审核、证书更新、审计日志程序等表述	2022.6.30	委员会工作组
V2.1	增加附录证书信息；调整一些不恰当的描述，文字表达及格式等内容。	2023.6.1	委员会工作组
Control Table of Document Version			
Name and version	Main modification instructions	Completion time	Modified by
V0.1	New document	2020.4.10	SAPAC Working Team
V0.1A	Revised documentation	2020.4.22	SAPAC Working Team
V1.0.1	Revised documentation	2021.8.10	SAPAC Working Team
V2.0	Revised the document format, improve the expression of Certificate application processing, Certificate renewal, Audit log procedures.	2022.6.30	SAPAC Working Team
V2.1	Added certificate hierarchy information in the Appendix; Adjusted some inappropriate descriptions, wording, and formatting issues;	2023.6.1	SAPAC Working Team

# 目 录 TABLE OF CONTENTS

<b>1. 概括性描述 GENERAL DESCRIPTION .....</b>	<b>1</b>
1.1 概述 OVERVIEW .....	1
1.2 文档名称与标识 DOCUMENT NAME AND IDENTIFICATION .....	5
1.2.1 名称 Name .....	5
1.2.2 版本 Version .....	5
1.3 电子认证活动参与者 PARTICIPANTS OF ELECTRONIC AUTHENTICATION ACTIVITY .....	5
1.3.1 电子认证服务机构 Certification authority(CA) .....	5
1.3.2 注册机构 Registration Authority (RA) .....	6
1.3.3 订户 Subscriber .....	6
1.3.4 依赖方 Relying party .....	6
1.3.5 其他参与者 Other participants .....	7
1.4 证书应用 CERTIFICATE APPLICATION .....	7
1.4.1 适合的证书应用 Suitable certificate Application .....	7
1.4.2 限制/禁止的证书应用 Application of Restricted / Prohibited Certificates .....	8
1.5 策略管理 POLICY MANAGEMENT .....	9
1.5.1 策略文档管理机构 Management organization of policy document .....	9
1.5.2 联系人 Contact person .....	10
1.5.3 决定 CPS 符合策略的机构 Organization determining CPS suitability for the policy .....	10
1.5.4 CPS 批准程序 CPS approval procedure .....	11
1.6 定义和缩写 DEFINITIONS AND ACRONYMS .....	11
<b>2. 信息发布与信息管管理 INFORMATION PUBLICATION AND MANAGEMENT .....</b>	<b>13</b>
2.1 信息库 REPOSITORY .....	13
2.1.1 信息库监督、监控机制 Repositories supervision .....	13
2.1.2 信息库内部数据维护 Internal data maintenance of the information database .....	13
2.2 信息发布 INFORMATION PUBLICATION .....	15
2.2.1 CPS 的发布 CPS publication .....	15
2.2.2 公众信息的发布 Publication of public information .....	15
2.2.3 认证信息的发布 Publication of authentication information .....	16
2.3 发布的时间或频率 TIME OR FREQUENCY OF PUBLICATION .....	16
2.4 信息库访问控制 ACCESS CONTROLS ON REPOSITORIES .....	17
<b>3. 身份标识与鉴别 IDENTIFICATION AND AUTHENTICATION .....</b>	<b>18</b>
3.1 命名 NAMING .....	18
3.1.1 名称类型 Types of names .....	18
3.1.2 对名称有意义的要求 Need for names to be meaningful .....	18
3.1.3 订户的匿名或伪名 Anonymity or pseudonymity of subscriber .....	19
3.1.4 理解不同名称形式的规则 Rules for understanding different forms of names .....	19
3.1.5 名称的唯一性 Name uniqueness .....	19
3.1.6 商标的承认、鉴别和角色 Recognition, Identification and Role of Trademarks .....	20
3.2 初始身份确认 INITIAL IDENTITY VALIDATION .....	20

3.2.1 证明拥有私钥的方法 Method to prove possession of private key .....	20
3.2.2 组织机构身份的鉴别 Authentication of organization identity .....	21
3.2.3 个人身份的鉴别 Authentication of Individual Identity .....	34
3.2.4 没有验证的订户信息 Subscriber information not validated .....	34
3.2.5 授权确认 Validation of Authority .....	34
3.2.6 互操作准则 Interoperational guidelines .....	35
3.3 更新请求的标识与鉴别 IDENTIFICATION AND AUTHENTICATION FOR RENEWAL REQUEST .....	36
3.3.1 常规更新的标识与鉴别 Identification and authentication for renewal request .....	36
3.3.2 吊销后更新的标识与鉴别 Identification and authentication for renewal after revocation .....	37
3.4 吊销请求的标识与鉴别 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST .....	37
3.4.1 证书吊销情况 Certificate revocation condition .....	37
3.4.2 吊销操作 Revocation operation .....	38
<b>4. 证书生命周期操作要求 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS .....</b>	<b>38</b>
4.1 证书申请 CERTIFICATE APPLICATION .....	38
4.1.1 证书申请实体 Who Can Submit a Certificate Application .....	38
4.1.2 注册过程与责任 Enrollment process and responsibilities .....	38
4.2 证书审核 CERTIFICATE APPLICATION PROCESSING .....	40
4.2.1 执行识别与鉴别功能 Performing identification and authentication functions .....	40
4.2.2 CMCA 证书申请批准和拒绝 Approval and rejection of certificate application .....	43
4.2.3 处理证书申请的时间 Time to process certificate applications .....	43
4.3 证书签发 CERTIFICATE ISSUANCE .....	44
4.3.1 证书签发中注册机构和电子认证服务机构的行为 CA Actions during Certificate Issuance .....	44
4.3.2 电子认证服务机构和注册机构对订户的通告 Notification of Certificate Issuance ..	44
4.4 证书接受 CERTIFICATE ACCEPTANCE .....	44
4.4.1 构成接受证书的行为 Notification of Certificate Issuance .....	44
4.4.2 电子认证服务机构对证书的发布 Publication of the certificate by the CA .....	46
4.4.3 CMCA 对其他实体的通告 Notification of certificate issuance by the CA to other entities .....	47
4.5 密钥和证书的使用 KEY PAIR AND CERTIFICATE USAGE .....	47
4.5.1 订户私钥和证书的使用 Subscriber private key and certificate usage .....	47
4.5.2 依赖方公钥和证书的使用 Relying party public key and certificate usage .....	48
4.6 证书更新 CERTIFICATE RENEWAL .....	49
4.6.1 证书更新的原因 Circumstance for Renewal .....	49
4.6.2 请求证书更新的实体 Who may request renewal .....	49
4.6.3 证书更新流程 Processing for Renewal .....	50
4.6.4 颁发新证书时对订户的通告 Notification of new certificate issuance to subscriber ..	50
4.6.5 构成接受更新证书的行为 Conduct constituting acceptance of a renewal certificate	50
4.6.6 电子认证服务机构对更新证书的发布 Publication of the renewal certificate by the CA .....	50

4.6.7 电子认证服务机构对其他实体的通告 <i>Notification of certificate issuance by the CA to other entities</i> .....	50
4.7 证书密钥更新 <b>CERTIFICATE RE-KEY</b> .....	51
4.7.1 证书密钥更新的情形 <i>Circumstance for Re-key</i> .....	51
4.7.2 请求证书密钥更新的实体 <i>Who may request certification of a new public key</i> .....	51
4.7.3 证书密钥更新请求的处理 <i>Processing for Re-key</i> .....	51
4.7.4 颁发新证书时对订户的通告 <i>Notification of new certificate issuance to subscriber</i> ..	52
4.7.5 构成接受密钥更新证书的行为 <i>Conduct constituting acceptance of a re-keyed certificate</i> .....	52
4.7.6 电子认证服务机构对密钥更新证书的发布 <i>Publication of the re-keyed certificate by the CA</i> .....	52
4.7.7 电子认证服务机构对其他实体的通告 <i>Notification of certificate issuance by the CA to other entities</i> .....	52
4.8 证书变更 <b>CERTIFICATE MODIFICATION</b> .....	52
4.8.1 证书变更的原因 <i>Circumstance for Modification</i> .....	52
4.8.2 请求证书变更的实体 <i>Who may request certificate modification</i> .....	53
4.8.3 证书变更的流程 <i>Processing for Modification</i> .....	53
4.8.4 颁发新证书时对订户的通告 <i>Notification of new certificate issuance to subscriber</i> ..	53
4.8.5 构成接受变更证书的行为 <i>Conduct constituting acceptance of modified certificate</i> ..	53
4.8.6 电子认证服务机构对变更证书的发布 <i>Publication of the modified certificate by the CA</i> .....	53
4.8.7 电子认证服务机构对其他实体的通告 <i>Notification of certificate issuance by the CA to other entities</i> .....	54
4.9 证书吊销和挂起 <b>CERTIFICATE REVOCATION AND SUSPENSION</b> .....	54
4.9.1 证书吊销的情形 <i>Circumstances for Revocation</i> .....	54
4.9.2 请求证书吊销的实体 <i>Who Can Request Revocation</i> .....	58
4.9.3 吊销请求的流程 <i>Processing for Revocation</i> .....	59
4.9.4 吊销请求宽限期 <i>Revocation Request Grace Period</i> .....	62
4.9.5 电子认证服务机构处理吊销请求的时限 <i>Time within which CA Must Process the Revocation Request</i> .....	62
4.9.6 依赖方检查证书吊销的要求 <i>Revocation Checking Requirement for Relying Parties</i> ..	64
4.9.7 CRL 发布频率 <i>CRL issuance frequency</i> .....	64
4.9.8 CRL 发布的最大滞后时间 <i>Maximum Latency for CRLs</i> .....	65
4.9.9 在线状态查询的可用性 <i>On-line Revocation/Status Checking Availability</i> .....	65
4.9.10 在线状态查询要求 <i>On-line Revocation Checking Requirements</i> .....	68
4.9.11 吊销信息的其他发布形式 <i>Other Forms of Revocation Advertisements Available</i> ...	68
4.9.12 密钥损害的特别要求 <i>Special Requirements Related to Key Compromise</i> .....	69
4.9.13 证书挂起的情形 <i>Circumstances for Suspension</i> .....	69
4.9.14 请求证书挂起的实体 <i>Who Can Request Suspension</i> .....	69
4.9.15 挂起请求的流程 <i>Procedure for Suspension Request</i> .....	69
4.9.16 挂起的期限限制 <i>Limits on Suspension Period</i> .....	69
4.10 证书状态服务 <b>CERTIFICATE STATUS SERVICES</b> .....	70
4.10.1 操作特性 <i>Operational characteristic</i> .....	70

4.10.2 服务可用性 <i>Service availability</i> .....	70
4.10.3 可选特征 <i>Optional Features</i> .....	70
4.11 订购结束 <i>END OF SUBSCRIPTION</i> .....	70
4.12 密钥托管与恢复 <i>KEY ESCROW AND RECOVERY</i> .....	71
4.12.1 密钥恢复的策略与行为 <i>Key escrow and recovery policy and practices</i> .....	71
4.12.2 会话密钥的封装与恢复的策略与行为 <i>Session key encapsulation and recovery policy and practices</i> .....	72
<b>5. 认证机构设施、管理和操作安全控制 <i>FACILITY, MANAGEMENT AND OPERATIONAL SECURITY CONTROLS OF CERTIFICATION BODY</i> .....</b>	<b>72</b>
5.1 物理安全控制 <i>PHYSICAL SECURITY CONTROLS</i> .....	72
5.1.1 物理场地位置与建筑 <i>Physical location and architecture</i> .....	72
5.1.2 物理访问 <i>Physical access</i> .....	73
5.1.3 电力与空调 <i>Power and air conditioning</i> .....	73
5.1.4 水患防治 <i>Water protection</i> .....	75
5.1.5 火灾防护 <i>Fire prevention and protection</i> .....	75
5.1.6 介质存储 <i>Media storage</i> .....	75
5.1.7 废物处理 <i>Waste disposal</i> .....	76
5.1.8 异地备份 <i>Off-site backup</i> .....	76
5.1.9 时间戳服务器证书物理控制 <i>Physical control of timestamp server certificates</i> .....	77
5.2 流程安全控制 <i>PROCESS SECURITY CONTROLS</i> .....	77
5.2.1 可信角色 <i>Trusted roles</i> .....	77
5.2.2 每项任务需要的人数 <i>Number of people required per task</i> .....	78
5.2.3 每个角色的识别与鉴别 <i>Identification and identification of each role</i> .....	79
5.2.4 职责分割原则 <i>Responsibility division principle</i> .....	79
5.3 人员控制 <i>PERSONNEL CONTROLS</i> .....	80
5.3.1 资格、经历和无过失要求 <i>Qualifications, experience, and clearance requirements</i> .....	80
5.3.2 背景审查程序 <i>Background review procedures</i> .....	81
5.3.3 培训要求 <i>Training requirements</i> .....	82
5.3.4 再培训周期和要求 <i>Retraining frequency and requirements</i> .....	84
5.3.5 工作岗位轮换周期和顺序 <i>Job rotation cycle and sequence</i> .....	85
5.3.6 未授权行为的处罚 <i>Sanctions for unauthorized actions</i> .....	85
5.3.7 独立合约人的要求 <i>Requirements of Independent Contractors</i> .....	86
5.3.8 提供给员工的文档 <i>Supplements for personnel</i> .....	87
5.4 审计日志程序 <i>AUDIT LOG PROCEDURES</i> .....	87
5.4.1 记录事件的类型 <i>Types of event records</i> .....	87
5.4.2 处理日志的周期 <i>Frequency of processing log</i> .....	88
5.4.3 审计日志的保存期限 <i>Retention period for audit log</i> .....	88
5.4.4 审计日志的保护 <i>Protection of audit log</i> .....	89
5.4.5 审计日志备份程序 <i>Back procedures of audit log</i> .....	89
5.4.6 审计收集系统 <i>Audit collection system</i> .....	89
5.4.7 对导致事件实体的处理 <i>Processing to event-causing subject</i> .....	90
5.4.8 脆弱性评估 <i>Vulnerability assessments</i> .....	90
5.5 记录归档 <i>RECORDS ARCHIVAL</i> .....	91



5.5.1 归档记录的类型 Types of records archived .....	91
5.5.2 归档记录的保存期限 Retention period for archived records .....	92
5.5.3 归档文件的保护 Protection of archive .....	92
5.5.4 归档文件的备份 Backup of archived records .....	92
5.5.5 记录时间戳要求 Requirements for time-stamping of records .....	93
5.5.6 归档收集系统 Archives collection system .....	93
5.5.7 获得和检验归档信息的程序 Procedures for obtaining and inspecting archived information .....	93
5.6 电子认证服务机构密钥更替 KEY REPLACEMENT .....	94
5.6.1 密钥更替操作 Key replacement operation .....	94
5.6.2 密钥更替操作管理 Key replacement operation management .....	95
5.7 损害与灾难恢复 DAMAGE AND DISASTER RECOVERY (DR) .....	95
5.7.1 事故和损害处理程序 Processing procedure of accident and damage .....	99
5.7.2 计算资源、软件和/或数据的损坏 Damage of computing resource, software and/or data .....	100
5.7.3 实体私钥损害处理程序 Damage treatment procedure of entity private key .....	100
5.7.4 灾难后的业务连续性能力 Business continuity ability after disaster .....	101
5.8 电子认证服务机构或注册机构的业务终止 CA OR RA TERMINATION .....	102
5.8.1 CA 终止原因 Termination reason of CA .....	102
5.8.2 终止通知 Termination notice .....	102
5.8.3 终止归档 Termination filing .....	102
5.8.4 终止措施 Termination measures .....	103
5.8.5 RA 的终止 Termination of RA .....	104
<b>6. 认证系统技术安全控制 TECHNICAL SAFETY CONTROL OF CERTIFICATION SYSTEM .....</b>	<b>105</b>
6.1 密钥对的生成和安装 GENERATION AND INSTALLATION OF KEY PAIR .....	105
6.1.1 密钥对的生成 Generation of CA key pair .....	105
6.1.2 私钥传送给订户 Public key transfer .....	106
6.1.3 公钥传送给证书签发机构 Public key transmission of CA .....	106
6.1.4 CMCA 电子认证服务机构公钥传送给依赖方 CMCA e-certification service agency public key is transmitted to the depending party .....	107
6.1.5 密钥的长度 Length of key .....	107
6.1.6 公钥参数的生成和质量检查 Generation and quality check of public key .....	108
6.1.7 密钥使用目的 Purpose of key use .....	108
6.2 私钥保护和密码模块工程控制 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....	109
6.2.1 密码模块的标准和控制 Cryptographic module standards and controls .....	109
6.2.2 私钥多人控制 Private key multi-person control .....	109
6.2.3 私钥托管 Private key trusteeship .....	109
6.2.4 私钥备份 Private key backup .....	110
6.2.5 私钥归档 Private key archival .....	110
6.2.6 私钥导入、导出密码模块 Private key transfer into or from a cryptographic module .....	111
6.2.7 私钥在密码模块的存储 Private key storage on cryptographic module .....	111

6.2.8 激活私钥 Private key activation .....	112
6.2.9 解除私钥激活状态 Private key deactivation .....	112
6.2.10 销毁私钥 Private key destruction .....	113
6.2.11 密码模块的评估 Evaluation of cryptographic module .....	114
6.3 密钥对管理的其他方面 OTHER ASPECTS OF KEY PAIR MANAGEMENT .....	114
6.3.1 公钥归档 .....	114
6.3.2 证书操作期和密钥对使用期 Certificate operational periods and key pair usage periods .....	114
6.4 敏感数据 SENSITIVE DATA .....	115
6.4.1 敏感数据的产生 Sensitive data generation .....	115
6.4.2 敏感数据的保护 Sensitive data protection .....	115
6.4.3 敏感数据的其他方面 Other aspects of sensitive data .....	116
6.5 计算机安全控制 COMPUTER SECURITY CONTROLS .....	117
6.5.1 具体的计算机安全技术要求 Computer security technical requirements .....	117
6.5.2 计算机安全评估 Computer security rating .....	118
6.6 系统生命周期控制 SYSTEM LIFE CYCLE CONTROLS .....	119
6.6.1 系统开发控制 System development controls .....	119
6.6.2 安全管理控制 Security management controls .....	119
6.6.3 生命周期的安全控制 Life cycle security control .....	119
6.7 网络的安全控制 NETWORK SECURITY CONTROLS .....	120
6.8 时间戳 DIGITAL TIME STAMP (DTS) .....	120
<b>7. 证书、证书吊销列表和在线证书状态协议 CERTIFICATE, CRL, AND OCSP PROFILES .....</b>	<b>121</b>
7.1 证书 CERTIFICATE PROFILE .....	121
7.1.1 证书版本号 Version Number(s) .....	131
7.1.2 证书扩展项 Certificate Content and Extensions; Application of RFC 5280 .....	131
7.1.3 算法对象标识符 Algorithm object identifier .....	135
7.1.4 名称形式 Name form .....	135
7.1.5 名称限制 Name Constraints .....	136
7.1.6 证书策略对象标识符 Certificate Policy Object Identifier .....	137
7.1.7 策略限制扩展项的用法 Usage of Policy Constraints Extension .....	138
7.1.8 策略限定符的语法和语义 Policy Qualifiers Syntax and Semantics .....	138
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 .....	138
7.2 证书吊销列表 CRL PROFILE .....	138
7.2.1 版本号 Version number(s) .....	139
7.2.2 CRL 和 CRL 条目扩展项 CRL and CRL entry extensions .....	139
7.3 在线证书状态查询协议 OCSP PROFILE .....	140
7.3.1 版本号 Version number(s) .....	140
7.3.2 OCSP 扩展项 OCSP extension .....	140
<b>8 认证机构审计和其他评估 AUDIT AND OTHER ASSESSMENTS OF CERTIFICATION BODY .....</b>	<b>141</b>



8.1 审计的频率或情形 FREQUENCY OR CIRCUMSTANCES OF AUDIT .....	141
8.2 审计者的资质 QUALIFICATION OF AUDITOR .....	141
8.3 审计者与中国移动 CMCA 的关系 RELATIONSHIPS BETWEEN AUDITORS AND CMCA .....	142
8.3.1 审计者与中国移动 CMCA 的关系 Relationships between auditors and CMCA .....	142
8.4 审计内容 AUDIT CONTENT .....	143
8.5 对问题与不足采取的措施 RESOLUTION FOR PROBLEMS AND DEFICIENCIES .....	143
8.6 评估结果的传达与发布 COMMUNICATIONS OF RESULTS .....	143
8.7 其他 OTHER .....	144
<b>9 法律责任和其他业务条款 LEGAL RESPONSIBILITY AND OTHER BUSINESS TERMS</b>	<b>144</b>
9.1 费用 FEES .....	144
9.1.1 证书签发和更新费用 Certificate fees .....	144
9.1.2 证书查询费用 Certificate inquiry fee .....	145
9.1.3 证书吊销或状态信息的查询费用 Query fee for certificate revocation or status information .....	145
9.1.4 其他服务费用 Other service charges .....	145
9.1.5 退款策略 Refund policy .....	145
9.2 财务责任 FINANCIAL RESPONSIBILITY .....	146
9.2.1 保险范围 Insurance coverage .....	146
9.2.2 其他资产 Other assets .....	147
9.2.3 对最终实体的保险或担保 Insurance or guarantee of end entity .....	147
9.3 业务信息保密 BUSINESS INFORMATION CONFIDENTIALITY .....	148
9.3.1 保密信息范围 Confidential information scope .....	148
9.3.2 不属于保密的信息 Information not within the scope of confidential information .....	148
9.3.3 保护保密信息的信息披露 Responsibility of business information confidentiality .....	149
9.4 个人隐私保密 PRIVACY OF INDIVIDUAL INFORMATION .....	149
9.4.1 隐私保密方案 Privacy plan .....	149
9.4.2 作为隐私处理的信息 Information treated as private .....	150
9.4.3 不被视为隐私的信息 Information not deemed private .....	151
9.4.4 保护隐私的责任 Responsibility to protect private information .....	151
9.4.5 使用隐私信息的告知与同意 Notice and Consent to Use Private Information .....	151
9.4.6 依法律或行政程序的信息披露 Information disclosure in accordance with legal or administrative procedures .....	152
9.4.7 其他信息披露情形 Other information disclosure .....	152
9.5 知识产权 INTELLECTUAL PROPERTY RIGHTS .....	153
9.6 陈述与担保 REPRESENTATIONS AND WARRANTIES .....	153
9.6.1 电子认证服务机构的陈述与担保 CA representations and warranties .....	153
9.6.2 注册机构的陈述与担保 RA representations and warranties .....	156
9.6.3 订户的陈述与担保 Subscriber representations and warranties .....	157
9.6.4 依赖方的陈述与担保 Representations and warranties of relying party .....	159
9.6.5 其他参与者的陈述与担保 Representations and warranties of other participants .....	160
9.7 担保免责 DISCLAIMERS OF WARRANTIES .....	160
9.8 有限责任 LIMITED LIABILITY .....	161
9.9 赔偿 INDEMNITIES .....	161

9.10 有效期限与终止 TERM AND TERMINATION .....	163
9.10.1 有效期限 <i>Term of validity</i> .....	163
9.10.2 终止 <i>Termination</i> .....	163
9.10.3 效力的终止与保留 <i>Termination and reservation of validity</i> .....	163
9.11 对参与者的个别通告与沟通 INDIVIDUAL NOTIFICATION AND COMMUNICATION TO PARTICIPANTS .....	164
9.12 修订 AMENDMENTS .....	164
9.12.1 修订程序 <i>Revision procedure</i> .....	164
9.12.2 通知机制和期限 <i>Notification mechanism and time limit</i> .....	164
9.12.3 必须修改业务规则的情形 <i>Situations where business rules have to be modified</i> ....	165
9.13 争议处理 DISPUTE RESOLUTION .....	165
9.14 管辖法律 GOVERNING LAWS .....	165
9.15 适用法律的符合性 APPLICABLE LAWS .....	166
9.16 一般条款 GENERAL TERMS .....	166
9.16.1 完整协议 <i>Entire agreement</i> .....	166
9.16.2 转让 <i>Assignment</i> .....	167
9.16.3 分割性 <i>Segmentation</i> .....	167
9.16.4 强制执行 <i>Enforcement</i> .....	167
9.16.5 不可抗力 <i>Force majeure</i> .....	168
9.17 其他条款 OTHER TERMS .....	168
附录：证书信息 APPENDIX: CERTIFICATE INFORMATION .....	0

# 1. 概括性描述 General Description

## 1.1 概述 Overview

卓望数码技术（深圳）有限公司是中国移动控股子公司，负责中国移动认证中心（China Mobile Certification Authority，简称 CMCA）的电子认证服务业务运营，是经中华人民共和国工业和信息化部颁发的电子认证服务许可资质的电子认证服务机构之一。

Aspire Digital Technology (Shenzhen) Co., Ltd is a subsidiary of China Mobile. Aspire Digital Technology (Shenzhen) Co., Ltd which is responsible for the electronic certification service business operation of China Mobile Certification Authority (CMCA). CMCA is a third-party authority approved by the Ministry of Industry and Information Technology of People's Republic of China.

证书策略及电子认证业务规则（CP/CPS）是关于认证机构（CA, Certification Authority）在全部数字证书（以下简称证书）服务生命周期（如签发、吊销、更新）中的业务实践所遵循规范的详细描述和声明，是对相关业务、技术和法律责任方面细节的描述。

The Certificate Policy and Certification Practice Statement (CP/CPS) is a detailed description and declaration of the specifications followed by the business practice of the certification body (CA, Certification Authority) in the full digital certificate (hereinafter referred to as certificate) service life cycle (e.g. issuance, revocation, renewal), and is a description of the details of the relevant business, technical and legal liability aspects.

中国移动证书信任体系（CMTCN）包括中国国内信任体系和全球信任体系，本 CP/CPS 是 CMCA 全球信任体系的证书业务规则声明，根据国家相关法律法规的要求，本 CP/CPS 详细阐述了中国移动 CMCA 开展全球信任证书认证业务的各项规范、流程和保障措施，以及电子认证服务参与各方所承担的责任与义务。The China Mobile Certificate Trust System (CMTCN) includes the China domestic trust system and the global trust system. This CP/CPS is a certificate

business rule statement CMCA the global trust system. In accordance with the requirements of relevant national laws and regulations, this CP/CPS describes in detail the specifications, procedures and safeguards of China Mobile's global trust certificate certification business, as well as the responsibilities and obligations of the participants in the e-certification service.

本文档的编写遵从《中华人民共和国电子签名法》、中华人民共和国工业和信息化部颁布的《电子认证服务管理办法》、《电子认证业务规则规范（试行）》，以及最新的 RFC3647、Guidelines for the Issuance and Management of Extended Validation Certificates（简称“EV Guidelines”）以及 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates（简称“Baseline Requirements”或“BR”）等。CMCA 遵循 <http://www.cabforum.org> 上发布的 Baseline Requirements、EV Guidelines 的最新版本进行签发和管理 SSL 证书。

This document is prepared in accordance with the Law of the People's Republic of China on Electronic Signatures, the Measures for the Administration of Electronic Certification Services promulgated by the Ministry of Industry and Information Technology of the People's Republic of China, the Code of Practice for Electronic Certification (Trial Implementation), and the latest RFC3647, Guidelines for the Issuance and Management of Extended Validation Certificates (hereinafter referred to as “EV Guidelines”) and Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (hereinafter referred to as “Baseline Requirements” or “BR”). CMCA conforms to the latest version of the Baseline Requirements and EV Guidelines published on the <http://www.cabforum.org> to issue and manage the publicly-trusted SSL certificates.

CMCA 已获得主管单位即工业和信息化部颁发的电子认证服务许可等资质，并处于资质有效期内。

CMCA has obtained the electronic certification service license issued by the competent unit, namely the Ministry of Industry and Information Technology,

and is within the validity period of the qualification.

CMCA 全球信任体系遵循 WebTrust 相关要求，并通过外部第三方审计机构审计。

CMCA Global Trust System follows the relevant WebTrust requirements and is audited by external third - party auditors.

本 CP/CPS（V2.1）的生效日期是 **2023 年 6 月 1 日**。

Effective Date of this CP/CPS (V2.1) **2023 年 6 月 1 日**。

CMCA 全球信任证书体系的架构如下：

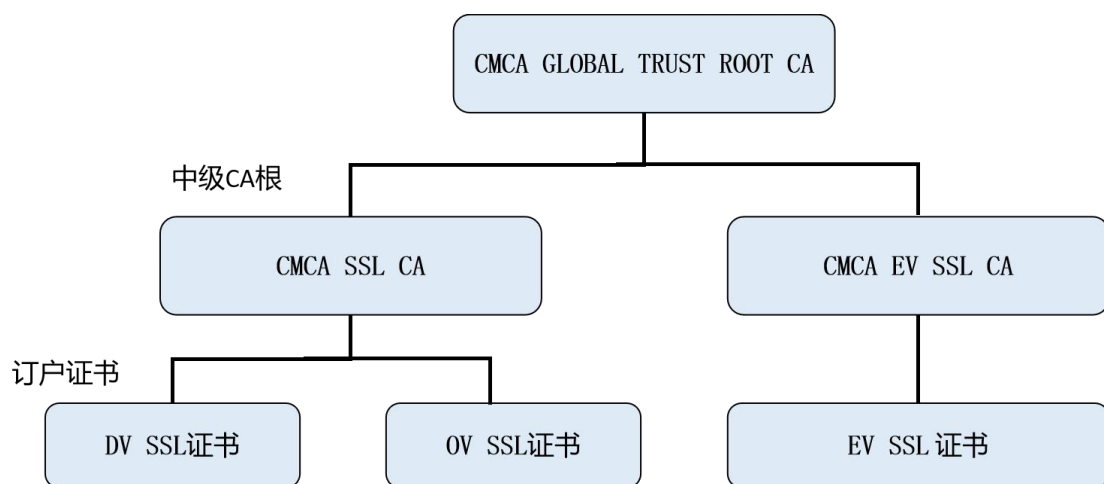


图 1 CMCA 全球信任全球信任证书体系架构

CMCA architecture of the global trust system is as follows:

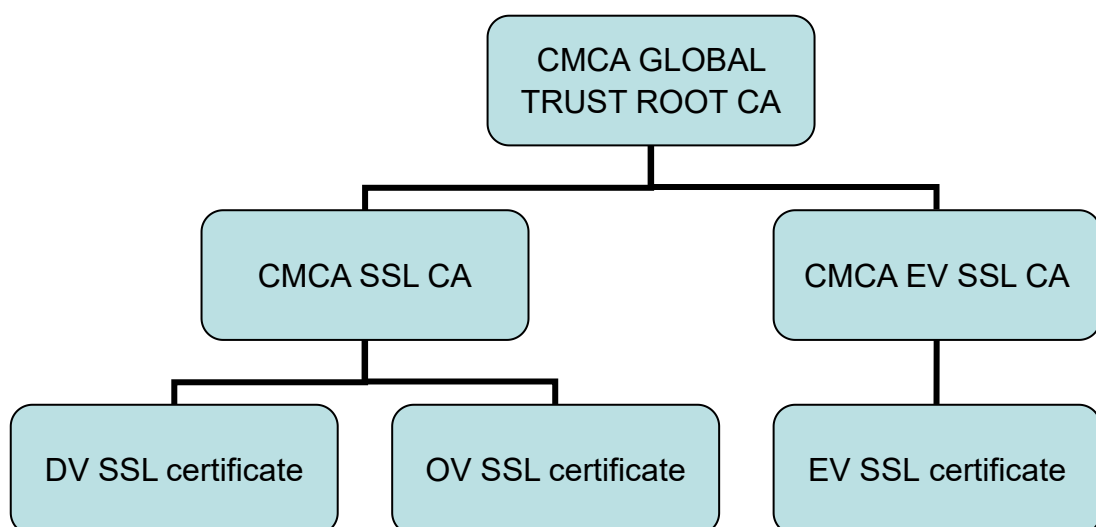


Figure 1 CMCA Global Trust Certificate Architecture

CMCA GLOBAL TRUST ROOT CA 根密钥长度为 RSA4096-bit，有效期

25 年，将于 2045 年 10 月 16 日到期。

CMCA GLOBAL TRUST ROOT CA 下设两个中级根：

- CMCA SSL CA 根密钥长度为 RSA4096-bit，有效期 20 年，将于 2040 年 10 月 16 日到期，签发普通 DV SSL 证书和 OV SSL 证书，订户证书有效期不超过 397 天。
- CMCA EV SSL CA 根密钥长度为 RSA4096-bit，有效期 20 年，将于 2040 年 10 月 16 日到期，签发 EV SSL 证书，订户证书有效期不超过 397 天。

CMCA GLOBAL TRUST ROOT CA Root key length RSA4096-bit, Valid for 25 years, will expire on October 16<sup>th</sup>, 2045.

CMCA GLOBAL TRUST ROOT CA has two subordinate CAs:

- CMCA SSL CA Root Key length is RSA4096-bit, valid for 20 years, will expire on October 16<sup>th</sup>, 2040, for issuing a general DV SSL certificate and OV SSL certificate, the subscriber certificate is valid for no more than 397 days.
- CMCA EV SSL CA key length is RSA4096-bit, valid for 20 years, will expire on October 16<sup>th</sup>, 2040, for issuing a EV SSL certificate, the subscriber certificate is valid for no more than 397 days.

CMCA 中级根的生成遵循严格的管理规范，由授权人员执行特定操作签发。并经由第三方审计机构见证，中级证书的生成过程将全程记录，本 CP/CPS 不做具体阐述。

The generation of subordinate CA follows strict management specifications and is issued by authorized personnel for specific operations. And through the third-party audit institutions witness, the generation process will be recorded, this CP/CPS does not do specific elaboration.



## 1.2 文档名称与标识 Document name and identification

### 1.2.1 名称 Name

本文档中文名称为《CMCA 全球信任体系电子认证业务规则》（英文名《CMCA Global Trust Certification Practice Statement》）。

DV SSL 证书对应的证书策略对象标识号符（OID）为 2.23.140.1.2.1。

OV SSL 证书对应的证书策略对象标识号符（OID）为 2.23.140.1.2.2。

EV SSL 证书对应的证书策略对象标识号符（OID）为 2.23.140.1.1。

The Chinese name of this document is 《CMCA 全球信任体系电子认证业务规则》(<CMCA Global Trust Certification Practice Statement>).

OID corresponding to DV SSL Certificate is 2.23.140.1.2.1.

OID corresponding to OV SSL Certificate is 2.23.140.1.2.2.

OID corresponding to the EV SSL certificate is 2.23.140.1.1.

### 1.2.2 版本 Version

本 CP/CPS 版本号为：V2.1。

The version No. is V2.1

## 1.3 电子认证活动参与者 Participants of electronic authentication activity

### 1.3.1 电子认证服务机构 Certification authority(CA)

电子认证服务机构 CA（Certification Authority）是颁发证书的实体，负责证书业务策略制定以及证书生命周期管理、密钥管理、信息库发布等工作，本文电子认证服务机构仅指 CMCA。

The certification authorities refer to the certificate certification body, which is

the entity to issue the certificate, namely the China Mobile Certification Authority, be responsible for certificate business policy formulation, certificate life-cycle management, key management, information base release and other work, this paper only refers to CMCA.

### 1.3.2 注册机构 Registration Authority (RA)

注册机构（Registration Authority，简称 RA）也称为注册审核机构，是为最终证书申请者建立注册过程的实体，对证书申请者进行身份鉴别和标识，发起或传递实体证书管理信息。

CMCA 全球信任体系下的注册机构均设在 CMCA 内部，由 CMCA 本身承担 RA 职责，并未委托外部机构行使 RA 机构职责。

Registration Authority (RA) is also called as registration and audit institution, which is the entity established by end certificate applicant during the registration process. It can conduct identity authentication and identification of certificate applicant, initiate or transfer entity certificate management information.

The registered agencies under CMCA Global Trust System are located within CMCA, which themselves assume RA responsibilities and do not entrust external agencies to exercise RA institutional responsibilities.

### 1.3.3 订户 Subscriber

订户是指向CMCA申请证书的实体。SSL 证书订户为企业机构。

The Subscriber is the entity pointing to which CMCA applies for a certificate. SSL certificate subscribers are enterprise institutions.

### 1.3.4 依赖方 Relying party

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的实体。

A dependent party is the entity that relies on the underlying trust relationship

demonstrated by the certificate and conducts business activities accordingly.

### 1.3.5 其他参与者 Other participants

除 CMCA、订户和依赖方以外的参与者称为其它参与者。

Participants other than CMCA, subscribers and dependencies are called other participants.

## 1.4 证书应用 Certificate application

### 1.4.1 适合的证书应用 Suitable certificate Application

签发 CA	签发证书类型
CMCA SSL CA	DV SSL 全球服务器证书
	OV SSL 全球服务器证书
CMCA EV SSL CA	EV SSL 全球服务器证书

CA issued	Type of certificate issued
CMCA SSL CA	DV SSL Global server certificate
	OV SSL Global server certificate
CMCA EV SSL CA	EV SSL Global Server Certificate

CMCA GLOBAL TRUST ROOT CA仅用于签发中级CA证书，不签发最终订户证书。

CMCA GLOBAL TRUST ROOT CA is only used to issue subordinate ca certificate, not final subscriber certificate.

#### 1.4.1.1SSL 全球服务器证书 SSL global server certificate

SSL 全球服务器证书包含 DV SSL 全球服务器证书和 OV SSL 全球服务器证书，均支持通配符证书、多域名证书、单域名证书类型。该类证书适合用于在订户浏览器与 Web 服务器之间建立安全通道，实现数据信息在客户端与服务器之间的加密传输，防止数据信息的泄露。

DV SSL 全球服务器证书和 OV SSL 全球服务器证书由 CMCA SSL CA 签

发 SHA256 证书，密钥长度为 RSA-2048。

SSL Global Server certificate contains DV SSL Global server certificate and OV SSL Global server certificate, all supported wildcard certificates, multiple domain name certificates, and single domain name certificate type. Such certificate is suitable for establishing secure channels between the subscriber browser and Web server to realize encrypted transmission of data information between client and server and to prevent leakage of data information.

DV SSL Global server certificate and OV SSL Global server certificate issued by CMCA SSL CA certificate, the key length is RSA-2048.

#### 1.4.1.2 EV SSL 全球服务器证书 EV SSL Global Server Certificate

CMCA EV SSL 全球服务器证书包含单域名证书、多域名证书，该类证书适合用于在订户浏览器与 Web 服务器之间建立安全通道，实现数据信息在客户端与服务器之间的加密传输，防止数据信息的泄露。

CMCA EV SSL 全球服务器证书由 CMCA EV SSL CA 签发 SHA256 证书，密钥长度为 RSA-2048。

CMCA EV SSL global server certificate contains single domain name certificate and multi-domain name certificate, this kind of certificate is suitable for establishing a secure channel between the subscriber browser and the Web server, realizing the encrypted transmission of data information between the client and the server, and preventing the leakage of data information.

CMCA EV SSL global server certificate issued by CMCA EV SSL CA SHA256 certificate, key length is RSA-2048.

### 1.4.2 限制/禁止的证书应用 **Application of Restricted / Prohibited Certificates**

CMCA全球信任体系下的证书根据其类型在功能上有所限制，比如EV SSL 服务器证书只能用于经过严格认证的WEB服务器。

CMCA certificates under the global trust system are functionally limited by their type, such as EV SSL server certificates can only be used for strictly

authenticated WEB servers.

各类证书的密钥用法在订户证书中的扩展项中进行了限制。然而基于证书扩展项限制的有效性取决于应用软件，如果参与方不遵守相关约定，其对证书的应用超出本 CP/CPS 限定的应用范围，将不受 CMCA 的保护。

The key usage of all kinds of certificates is limited in the subscriber certificate. However, the validity of the certificate extension restriction is based on the application software, and if the participant does not comply with the relevant agreement, the certificate is beyond the scope limited by this CP/CPS and will not be protected by CMCA.

CMCA 全球信任体系下签发的证书不能在如下领域使用：任何与国家或地方法律、法规规定相违背的应用系统。

Certificates issued CMCA the global trust system cannot be used in any application system that is contrary to national or local laws and regulations.

## 1.5 策略管理 Policy management

### 1.5.1 策略文档管理机构 Management organization of policy document

本 CP/CPS 由卓望数码技术（深圳）有限公司安全认证策略委员会组织制定并负责管理。委员会下设工作组，当需要编写或修订本 CP/CPS 时，由工作组组织编写，由委员会审批后正式发布。

This CP/CPS is formulated and managed by the Security Authority Policy Administration Committee(SAPAC), which is established by Aspire Digital Technology(Shenzhen) Co., Ltd. SAPAC has a working group. When this CP/CPS needs to be prepared or revised, it is organized by the working group and issued after approval by the committee.

## 1.5.2 联系人 Contact person

中国移动 CMCA 将对 CP/CPS 进行严格的版本控制和文档管理, 由 CMCA 安全认证策略委员会, 由专门的 CP/CPS 管理人员负责日常维护, 指定运营服务部负责对外联络。

CMCA shall conduct the strict version control and document management of CP/CPS, and the Security Authentication Policy Management Committee (SAPAC) is responsible for the management. The specified CP/CPS management personnel carry out the maintenance, in addition, the specified Operation Service Department takes charge of the external liaison.

联系部门: 安全业务部

电话: 86-755-66820666

传真: 86-755-66820001

地址: 深圳高新技术产业园区南区深港产学研基地大楼六楼

电子邮件: [cmca@aspirecn.com](mailto:cmca@aspirecn.com)

联络网站: [www.cmca.net](http://www.cmca.net)

Contact department: Security Business

Tel.: 86-755-66820666

Fax: 86-755-66820001

Address: 6th Floor, West Shengang IER Building, South District, Shenzhen High-tech Industry Park, Shenzhen

E-mail: [cmca@aspirecn.com](mailto:cmca@aspirecn.com)

Contact website: [www.cmca.net](http://www.cmca.net)

## 1.5.3 决定 CPS 符合策略的机构 Organization determining CPS suitability for the policy

CMCA 安全认证策略委员会对本 CP/CPS 文件具有决定权和最终解释权。  
SAPAC has the decision-making power and the final interpretation right for this



CP/CPS document.

### 1.5.4 CPS 批准程序 CPS approval procedure

在中国移动 CMCA 证书策略及认证业务声明做出任何变动之前，CMCA 安全认证策略委员会将对提供的变动建议进行研究，做出变更决定。策略委员会至少每年一次组织对 CP/CPS 内容进行审查，明确 CP/CPS 是否要修订以及修订的内容，并组织工作组进行编写，经策略委员会批准后予以更新发布。

Before making any change of CMCA CP/CPS, the Security Authentication SAPAC of CMCA will research the change suggestions provided and make the change decision. The Strategy Committee organizes a review of the CP/CPS content at least every year, clarifying whether the CP/CPS will be revised and revised, and to be prepared and updated with the approval of the Strategy Committee.

## 1.6 定义和缩写 Definitions and acronyms

CMCTN	中国移动证书信任体系 (China Mobile Certificate Trust Network)
CP	证书策略 (certification policy)
CPS	电子认证业务规则或电子认证业务说明 (certification practice statement )
CRL	证书吊销列表或证书黑名单 (certificate revocation list)
CSR	证书签名请求 (Certificate Signing Request)
HTTP	超文本传输协议 (Hypertext Transfer Protocol)
HTTPS	安全套接层下的超文本传输协议 (Hypertext Transfer Protocol with SSL)
CA	电子认证服务机构 (certificate authority)
RA	注册机构 (registration authority)
LRA	本地注册受理点或本地受理点 (local registration authority)
PIN	个人授权码 (personal identification number)

OCSP	在线证书状态查询协议 (online certificate search protocol)
LDAP	轻量目录访问协议 (Lightweight Directory Access Protocol)
PKCS	公共密钥加密标准 ( <i>Public Key Cryptography Standards</i> )
PKI	公共密钥基础设施 (public key infrastructure)
SSL	加密套阶字协议层 ( <i>Secure Sockets LRAyer</i> )
URL	指定的信息位置 ( <i>uniform resource locator</i> )
WWW or Web	万维网 (World Wide Web)
X.509	国际电信同盟认证体系的证书标准 ( the ITU-T standard for certificates and their corresponding authentication framework)

CMCTN	China Mobile Certificate Trust Network
CP	certification policy
CPS	certification practice statement
CRL	certificate revocation list
CSR	<i>Certificate Signing Request</i>
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
CA	certificate authority
RA	registration authority
LRA	local registration authority
PIN	personal identification number
OCSP	online certificate search protocol
LDAP	Lightweight Directory Access Protocol
PKCS	<i>Public Key Cryptography Standards</i>
PKI	public key infrastructure
SSL	<i>Secure Sockets LRAyer</i> )
URL	<i>uniform resource locator</i> )
WWW or Web	World Wide Web
X.509	the ITU-T standard for certificates and their corresponding authentication framework

## 2. 信息发布与信息管 Information publication and management

### 2.1 信息库 Repository

CMCA 信息库面向订户及证书应用依赖方提供信息服务。信息库包括但不限于以下内容：证书、CRL、CP/CPS、证书服务协议、技术支持手册以及 CMCA 网站信息等。

CMCA information database provides information services to subscribers and certificate application relying parties. The information database includes, but is not limited to, the following: certificates, CRL, CP/CPS, certificate service agreement, technical support manual, and CMCA website information.

#### 2.1.1 信息库监督、监控机制 Repositories supervision

CMCA 针对信息库建立监督、监控机制，以此保障信息库安全可靠，并确保信息库、分发库的证书和签发出的证书一致、订户获取的证书与签发证书一致，证书准确发放给了订户。

CMCA establishes the supervision and monitoring mechanism for the information database. This ensures that the information base is secure and reliable, that the information base, the certificates issued by the distribution base and the certificates issued are consistent, that the certificates obtained by the subscribers are consistent with the certificates issued, and that the certificates are issued accurately to the individual subscribers.

#### 2.1.2 信息库内部数据维护 Internal data maintenance of the information database

CMCA 将维护内部数据记录，用于记录所有曾经因为网络钓鱼可疑或可能被其他欺诈手段利用的原因被吊销或拒绝申请的证书信息（包括 EV 证书），这

些证书的申请机构在今后的身份验证中标识为可能的高风险证书申请。

CMCA will maintain internal data records for all certificate information (including EV certificates) that has been revoked or denied for suspected phishing suspect or may be exploited by other fraud , which applicant agencies identify as possible high - risk certificate applications in future authentication.

在进行身份验证时 CMCA 将申请机构与一些高风险机构名单进行比对，主要是指最有可能成为网络钓鱼或其他身份欺诈目标的组织机构，自动在申请阶段将其标记为“高风险申请者”，确保证书在签发前申请机构的身份得到充分验证。

For authentication purposes CMCA the list of applicant institutions is compared with the list of high-risk institutions, mainly those organizations that are most likely to be the target of phishing or other identity fraud, which are automatically marked as "high-risk applicants" at the application stage to ensure that the identity of the applicant institution before issuance is fully verified.

这些组织名单有：

1) 参考国际反钓鱼工作组（APWG）及中国反钓鱼联盟（APAC）公布的钓鱼目标名单；

2) CMCA 将因为可能遭到网络钓鱼或其他身份欺诈攻击而吊销其 OV SSL 全球服务器、EVSSL 全球服务器证书，CMCA 将把这些被拒绝的申请者的组织机构标记为“高风险申请者”，并且作为今后识别高风险申请机构的依据。

These lists of organizations have:

1 ) Refer to the list of fishing targets published by the International Anti-Fishing Working Group (APWG) and the China Anti-Fishing Alliance (APAC) for information;

2) CMCA will revoke their certificates OV SSL global servers and EVSSL global servers for possible phishing or other identity fraud attacks, and will mark the organization of these rejected applicants as "high-risk applicants" and serve as a basis for future identification of high-risk applicants.

CMCA 将拒绝处于高风险信息库中的证书申请。

CMCA will reject applications for certificates in a high-risk repository

## 2.2 信息发布 Information publication

### 2.2.1 CPS 的发布 CPS publication

本 CP/CPS 结构遵循 RFC 3647 且包含其要求的所有内容。

本 CP/CPS 以及相关的技术支持信息等在 CMCA 网站上发布。

本 CP/CPS 发布的内容为 CMCA 全球信任证书业务的基线要求，如有版本更新，以最新版本为准。

CMCA 遵循 <http://www.cabforum.org> 上发布的 Baseline Requirements、EV Guidelines 的最新版本。如果本文档和 Baseline Requirements、EV Guidelines 之间有任何不一致，以 <http://www.cabforum.org> 上发布的为准。

This CP/CPS structure is in compliance with RFC 3647 and contains all content required by it.

This CP/CPS and related technical support information are released on CMCA website.

Content released by this CP/CPS constitutes the baseline requirement of CMCA's global trust certificate business. For any version update, the latest version shall prevail.

CMCA follows the latest version of Baseline Requirements and EV Guidelines released on <http://www.cabforum.org>. In event of any inconsistency between this document and the Baseline Requirements and EV Guidelines, the Baseline Requirements and EV Guidelines shall prevail.

### 2.2.2 公众信息的发布 Publication of public information

中国移动 CMCA 将及时在网站上公布相关的公众信息

CMCA will publish relevant public information on the website in time

## 2.2.3 认证信息的发布 Publication of authentication information

证书在签发成功后，中国移动 CMCA 自动将证书副本发布到目录服务器上。

中国移动 CMCA 定期公布的证书有效期内被废止的数字证书可从中国移动 CMCA 的 CRL 发布站点获取。

证书客户可以在中国移动 CMCA 的网站中查询获得其证书有关信息。

After the certificate is successfully issued, CMCA automatically publishes the certificate copies to the LDAP server. The digital certificate repealed in certificate effective date published by CMCA regularly can be obtained from CRL publication site of CMCA.

The certificate customer can inquire and obtain the relevant certificate information in CMCA website.

## 2.3 发布的时间或频率 Time or frequency of publication

证书相关方可通过中国移动 CMCA 信息库 7x24 小时获取 CP/CPS。

中国移动 CMCA 有权利对其 CP/CPS 进行改动和版本升级，其发布时间及频率由中国移动 CMCA 决定，至少每年对 CP/CPS 进行审查一次，至少每年更新一次。

中国移动 CMCA 的网站实时更新，会在第一时间发布和证书业务相关的信息。

证书签发成功后，CMCA 自动将证书副本发布到目录服务器上。

中国移动 CMCA 通常在 24 小时内自动发布最新证书吊销列表 CRL，发布时间为每天的凌晨，也可人工发布最新 CRL。证书客户可在中国移动 CMCA 网站上查询、下载数字证书以及 CRL。

CP/CPS are available through the repository as 7\*24 service.

CMCA has the right to make changes and upgrades to its CP/CPS, and its



publication time and frequency are determined by CMCA. CMCA will publish the latest version of CP/CPS on the website, and the related parties of certificate can obtain CP/CPS through CMCA repository within 7x24 hours. Review the CP/CPS at least once a year, and update at least annually.

CMCA website will update real time, and will publish the information related to certificate business in the first time.

After the certificate is successfully issued, CMCA automatically publishes the copy of the certificate to the LDAP.

CMCA LDAP usually automatically publishes the latest CRL within 24 hours, and the publication time is the morning of each day. While the latest CRL can also be published manually. The certificate customers can inquire, download digital certificate and CRL on CMCA website.

## 2.4 信息库访问控制 Access controls on repositories

2.2 节中所发布信息的查询、获取是公开的，没有任何限制。

中国移动 CMCA 设置了信息访问控制和安全审计措施，保证只有经过授权的中国移动 CMCA 工作人员才能编写和修改中国移动 CMCA 在线的公告版本和公布信息。

The information published in section 2.2 is open and without constraints.

CMCA has set up information access controls and security audit measures to ensure that only authorized CMCA staff can prepare and modify CMCA online announcement version and publish the information.

## 3. 身份标识与鉴别 Identification and authentication

### 3.1 命名 Naming

#### 3.1.1 名称类型 Types of names

根据证书主体类型不同，中国移动 CMCA 签发的证书的主体名字可以是域名、公网 IP 等，命名符合 X.500 定义的甄别名规范。

According to the type of certificate subject, the subject name of the certificate issued by CMCA can be domain name, public network IP, etc. The naming conforms to the distinguished name specification defined by X.500.

#### 3.1.2 对名称有意义的要求 Need for names to be meaningful

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

**EV SSL全球服务器证书**的甄别名称中的通用名只能是订户机构所拥有的域名，结合该订户机构的其他信息一起被鉴别和认证。

**DV SSL全球服务器证书、OV SSL全球服务器证书**的甄别名称中的通用名可以是订户所拥有的域名或者公网IP，结合该订户的其他信息一起被鉴别和认证。

**DN (Distinguished Name)** :A unique screening name, in the domain of the subject name of the digital certificate, is used to uniquely identify the X.500 name of the subject of the certificate. It is necessary to fill in the content which reflects the true identity of the subject of the certificate and has practical significance and does not conflict with the law.

The universal name under the discriminated name of EV SSL global server certificate can only be domain name of the subscriber organization, which can be authenticated and certified together with other information of the subscriber. SSL common name in the screening name of DV SSL global server certificate

and OV SSL global server certificate can be a domain name owned by the subscriber or a public network IP, identified and authenticated together with other information of the subscriber.

### **3.1.3 订户的匿名或伪名 Anonymity or pseudonymity of subscriber**

中国移动 CMCA 所签发的全球信任证书不可以使用匿名或伪名。

The subscribers (certificate applicants) shall not be anonymous or pseudo.

### **3.1.4 理解不同名称形式的规则 Rules for understanding different forms of names**

DN(Distinguished Name)的命名规则由 CMCA 定义, 详见本 CP/CPS 7.1. 的说明。

The naming rules for DN (Distinguished Name) are defined by CMCA, as described in this CP/CPS 7.1.

### **3.1.5 名称的唯一性 Name uniqueness**

CMCA 保证其签发的证书, 其主题甄别名, 在 CMCA 的信任域内是唯一的。不同的订户的证书的主体甄别名不能相同, 但对于同一订户, CMCA 可以用其唯一的主题甄别名为其签发多张证书。当证书申请中出现不同订户存在相同名称时, 遵循先申请者优先使用, 后申请者增加附加识别信息予以区别的原则。

CMCA guarantee that the certificate issued by it, its subject screening name, is unique in CMCA trust domain. Different subscribers' certificates cannot have the same subject identification name, but for the same subscriber, CMCA can use their unique subject identification to issue multiple certificates. When different subscribers have the same name in the certificate application, follow the principle that the applicant first uses it first, and then the applicant adds

additional identification information to distinguish it.

### **3.1.6 商标的承认、鉴别和角色 Recognition, Identification and Role of Trademarks**

CMCA 签发的证书的主体甄别名不包含任何商标或者可能对其他机构构成侵权的信息。

CMCA the subject identification name of the certificate issued does not contain any trademark or information that may constitute infringement on other institutions.

## **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**

中国移动 CMCA 通过使用经数字签名的 PKCS#10 格式的证书请求，验证证书申请者拥有私钥。

CMCA should verify that the certificate applicant has the private key by using the certificate request in PKCS#10 format with digital signature.

CMCA 在为申请者签发证书前，系统将自动使用其公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断申请者拥有私钥。

Before CMCA issues a certificate for the applicant, the system will automatically use its public key to verify the validity of its private key signature and the integrity of the application data, in order to determine that the applicant has a private key.

### 3.2.2 组织机构身份的鉴别 Authentication of organization identity

订户在申请CMCA全球信任体系签发的证书前，应提供有效机构身份证明文件、证书申请文件，并接受证书申请的有关条款，同意承担相应的责任。

Before applying for a certificate issued CMCA the Global Trust System, subscribers shall provide valid institutional identity documents, certificate application documents, and accept the relevant terms of the certificate application and agree to bear the corresponding responsibilities.

CMCA 接受订户的证书申请后，应对订户的身份真实性进行审核，应使用可靠的数据源（所使用的数据源需经 CA 评估为可靠数据源，可靠数据源的评估包括信息所提供的时间、信息更新的频率、数据的收集和提供目的、数据可用性的公开可访问性、伪造和篡改相关困难）对订户身份的真实性进行审核，并按照双方的约定妥善保存订户申请材料。

After CMCA accepts the certificate application, review the identity authenticity of the subscriber , review the authenticity using the reliable data source (the data source used needs to be evaluated by CA , including the time of reliable data source , the frequency of information provided , the purpose of data collection and provision , public accessibility of data availability , forgery and tampering difficulties) and properly preserve the subscriber application materials as agreed by both parties.

CMCA对订户身份的鉴别过程如下：

Whether CMCA or its authorized agency auditing organization meets the requirements, and the identity authentication methods are as follows:

业务受理人员收集订户的申请材料，并对订户身份以及材料进行线下审核。

The business receptionist collects the subscriber's application materials and reviews the subscriber's identity and materials offline.

RA操作员录入订户申请信息，RA审核员再次审核操作员录入信息并协助订户下载证书。

RA the operator to enter the subscriber application information, RA the auditor

to review the operator input information again and assist the subscriber to download the certificate

### 3.2.2.1 身份 Identity

如果主题身份信息包括了机构的名称或者地址，CA应验证该组织机构的身份和地址，并且该地址是申请人的存在或运营地址。CA 应使用以下机构提供的文件验证申请人的身份和地址，或通过以下至少一项沟通：

1. 管辖范围内批准申请人合法设立、存在或认可的政府机构；
2. 定期更新并被视为可靠数据源的第三方数据库；
3. CA 或作为 CA 代理的第三方进行的现场访问；
4. 证明信。

此外，CA可以使用公用事业账单、银行对账单、信用卡对账单、政府签发的税务文件或其他CA 认为可靠的身份证明来验证申请人的地址（非申请人的身份）。

If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

Alternatively, the CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card



statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

订户如需要申请EV SSL、OV SSL或DV SSL全球服务器证书,可以向CMCA提交申请。

Subscribers who need to apply for EV SSL, OV SSL or DV SSL global server certificates may submit applications to CMCA.

EV SSL全球服务器证书只能是Web服务器的域名,并且域名不能包含通配符\*,不受理IP地址的申请, EVSSL全球服务器证书可以是单域名或多域名证书。EVSSL global server certificate can only be the domain name of the Web server, and the domain name cannot contain wildcard \*, the application for IP address is not accepted, EVSSL the global server certificate can be a single domain name or multi-domain name certificate.

OV SSL,DV SSL 全球服务器证书可以包含单域名、多域名、通配符证书、公网 IP 证书。

订户申请 EVSSL、OVSSL、DVSSL 全球服务器证书时,应提交如下材料:OVSSL、DVSSL global server certificate may contain single domain name, multi-domain name, wildcard certificate, public network IP certificate. Subscribers apply EVSSL、OVSSL、DVSSL global server certificates, the following information should be submitted:

	EV SSL 证书	OV SSL 证书	DV SSL 证书
1	CMCA 全球信任体系证书申请表		
2	至少一种机构信息证明材料（特殊情况下需额外提供其他机构证件）	\	
3	证书申请文件（Certificate Signing Request, CSR 文件）		
4	律师函及律师资格文件，或其他根据 CA/B 论坛 EVSSL 证书鉴别要求中认可的补充文件	对应顶级域名的所有命名空间的控制权的有效证明或 CA/B 论坛认可的拥有公网 IP 的证明	\

	EV SSL certificates	OV SSL certificates	DV SSL certificates
1	CMCA Global Trust System Certificate Request Form		
2	At least one institutional information certificate (additional other institutional documents in special circumstances )	\	
3	Certificate Signing Request, CSR file		
4	Lawyer Letter and Lawyer Qualification Documents, Or other supplementary documents approved under the CA/B Forum EVSSL Certificate requirements	Valid proof of control over all namespaces corresponding to a top-level domain name or proof of ownership of a public network IP endorsed CA/B the Forum.	\

CMCA除对申请者的身份、地址信息、国家信息等进行鉴别外，还要对域名、IP及CSR合规性进行鉴别。其鉴别要求、流程及方法如下：

CMCA also identifies domain name, IP, national information, in addition to applicant identity, address information, and CSR compliance. The identification requirements, process and methods are listed below:

- 1、 机构
  - 企事业单位、组织、社会团队
    - (1) 获得当地监管机构承认的合法组织，或获得当地政府的特许；
    - (2) 监管机构认定的注册代表处或注册公司；
    - (3) 不在组织/监管机构的“停业”、“无效”、“过期”、“失信”名单之列；
    - (4) 至少有一个合法有效的授权代表；
    - (5) 在订户申请材料中必须明确单位的授权代表；
    - (6) 拥有固定的营业场所；
    - (7) 机构注册或营业场所所在地法律允许CA签发证书的国家；
    - (8) 不在中国的政府黑名单之列。

## 1、Organization

- Enterprises, organizations, social teams

(1) Legal organizations recognized by local regulators or licensed by local governments;

(2) A registered representative office or registered company recognized by a regulatory body;

(3) Not included in the "closure "," invalidation "," expiration" and "breach of trust" lists of organizations/regulators;

(4) At least one duly authorized representative;

(5) The authorized representative of the unit must be specified in the subscriber application materials;

(6) Have a business premises;

(7) Country where agency registration or business place location law permits CA to issue a certificate;

(8) Government blacklist not in China.

- 政府机构：比如公安局、税务局等，应满足以下条件：

(1) 经由上级按照其职能批准建立；

(2) 所在国家允许CA签发证书；

(3) 不在中国的政府黑名单之列。

- Government agencies, such as the Public Security Bureau and the Tax Bureau, should meet the following conditions:

(1) Established by superiors according to their functions;

(2) Country allows the CA to issue a certificate;

(3) Government blacklist not in China.

- 国际组织

(1) 由一国政府机构签署成立的私人基金、财团或等同机构。CAB论坛会维护可以申请EV证书的国际机构列表；

(2) 国际机构总部所在地必须允许CMCA从事电子认证业务或认可CMCA数字证书有效性；

(3) 国际机构不能在任何政府所列的禁止名单（如贸易禁运）上。其子机构或分支机构根据准则要求也可申请EV证书。

- international organization

(1) Private fund , consortium or equivalent institution signed by a government body of a State .The CAB Forum maintains a list of international

agencies that can apply for EV certificates;

(2) The location of the headquarters of an international institution must allow CMCA to engage in e-certification operations or to recognize the validity CMCA digital certificates;

(3) International agencies can-not be on prohibited lists (such as trade embargoes) listed by any Government. A subsidiary or branch may also apply for a EV certificate in accordance with the requirements of the guidelines.

## 2、 域名及IP

### 2、 Domain Name and IP

申请机构拥有EVSSL证书中的域名、OVSSL证书中的域名或公网IP的所有权或唯一使用权;

The applicant has the ownership or sole right to use the domain name in the EVSSL certificate, the domain name in the OVSSL certificate or the public network IP;

域名注册信息应公开在WHOIS数据库, 包括申请机构名称、地址和联系方式; 通过域名注册信息查询(whois)功能, 得到所申请域名证书的域名注册者资料, 查看域名注册者是否和域名证书申请者一致, 初步审核确定域名证书申请者确实拥有此域名。同时, CMCA将验证申请人对域名的所有权或控制权: 通过信函、传真、SMS或者邮递将一个随机值(有效期为从产生该随机值开始30天, 且在每个电子邮件、传真、短信或邮政邮件中是唯一的。)发送给域名联系人, 并收到使用该随机值的确认回复。

The domain name registration information should be made public in the WHOIS database, including the name, address and contact information of the applicant; through the domain name registration information query (whois) function, the domain name registrant information of the domain name certificate applied for is obtained, and the domain name registrant is consistent with the domain name certificate applicant. Meanwhile, CMCA will verify the applicant's ownership or control of the domain name: a random value (valid for 30 days from the date that the random value was generated and unique in each e-mail, fax, text message, or postal mail) by letter, fax, SMS, or mail. ) sent to the domain name contact and received a confirmation reply using the random value.

如申请证书的域名与知名网站域名比较相似、或含有知名商标, 则CMCA会

进行多层审查，并通过高风险信息库进行比对，以防止相似欺诈域名申请证书。

If the domain name of the application certificate is similar to the domain name of the well-known website or contains a well-known trademark, CMCA will conduct a multi-level review and compare it through the high-risk information base to prevent similar fraud domain name application certificate.

对于公网IP的鉴别，通过信函、传真、SMS或者邮递将一个随机值（有效期为从产生该随机值开始30天，且在每个电子邮件、传真、短信或邮政邮件中是唯一的。）发送给IP地址联系人，并收到使用该随机值的确认回复，以验证申请人对IP地址的控制权。

To identify a public IP, a random value (valid for 30 days from the date the random value is generated and unique in each e-mail, fax, text message, or post) is sent by letter, fax, SMS, or mail. Send to the IP address contact and receive a confirmation reply using the random value to verify the applicant's control over the IP address.

如果申请通配符域名证书，CMCA将鉴别其拥有的二级域名。对于多域名证书，CMCA将对所有列举的域名进行鉴别。

If you apply for a generic domain name certificate, CMCA will identify the secondary domain name it owns. For multi-domain certificates, CMCA will identify all listed domain names.

### 3、 申请机构角色

### 3、 Application Agency Role

申请单位需要如下的角色：

The applicant needs the following roles:

- ✓ 申请经办人：申请单位经办人员
- ✓ 申请确认人：申请单位的主管人员，确认申请信息的准确性和有效性

证书申请机构可授权一个人来完成所有的角色，也可以分别让多个人来完成。以上角色必须是申请单位的职员或被授权的代理人，申请单位需确认申请角色的信息真实准确并以CMCA认可的方式（包括但不限于注册公章、注册法人人名章、角色手印等方式）进行声明，对于不实的申请角色信息，CMCA有权拒绝申请，并对已发放的证书进行吊销。

个人身份的认证：居民身份证、护照等。

- ✓ Application agent : applicant
  - ✓ Confirmation person: the person in charge of the applicant to confirm the accuracy and validity of the application information

The certificate applicant may authorize one person to complete all roles or by multiple individuals respectively. The above role must be the employee or authorized agent of the applicant. The applicant unit shall confirm the authenticity and accuracy of the application role information through CMCA approval (including but not limited to the registered official seal, registered legal person seal, role fingerprints, etc.). For the false application role information, CMCA has the right to refuse the application and revoke the issued certificate.

Personal identity certification: resident ID card, passport, etc.

#### 4、CSR符合性鉴别CSR conformity identification

对于CSR文件的鉴别主要包含，CSR中的信息是否与申请表中的申请信息一致，是否符合相关规范，比如DN的顺序等，并验证其是否拥有私钥。

The identification of CSR files mainly includes whether the information in the CSR is consistent with the application information in the application form, whether it conforms to the relevant specifications, such as the order of DN, and verifies whether it has a private key.

#### 5、EVSSL、OVSSL、DVSSL全球服务器证书公钥证书分发

#### 5、Distribution EVSSL、OVSSL Global Server Certificate 、DVSSL Global Server Certificate Public Key Certificate

CMCA为订户签发公钥证书，并以邮件方式将签发的公钥证书交付给订户。CMCA issue the public key certificate for the subscriber and deliver the issued public key certificate to the subscriber by mail.

### 3.2.2.2 DBA/商业名称的鉴别 DBA/tradename

若证书主题包含 DBA 或商业名称，CMCA 将通过以下方式中的至少一种确认申请者有权使用该 DBA 或商业名称。

- 1) 政府机构提供的可证明申请者合法成立、存在或认可的有效文档
- 2) 可靠的数据来源（如邓白氏编码）
- 3) 与负责管理此类 DBA 或商业名称的政府机构的沟通；
- 4) 附有证明文件的证明信；
- 5) 公用事业账单、银行对账单、信用卡对账单、政府签发的税务文件或 CA 认为可靠的其他身份证明形式。

If the certificate subject contains a DBA or tradename, the CA or the

authorized RA shall verify the applicant's right to use the DBA or tradename using at least one of the following ways.

- 1) Valid documents provided by a government agency in the jurisdiction of the applicant's legal creation, existence, or recognition.
- 2) A reliable data source. (eg: Dun & Bradstreet)
- 3) Communication with a government agency responsible for the management of such DBAs or tradenames;
- 4) An Attestation Letter accompanied by documentary support; or
- 5) A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

### 3.2.2.3 国别验证 Verification of Country

若证书主题中包含国家选项，CMCA将通过以下方式中的至少一种进行国家的鉴别。

- 1) 通过权威第三方数据查询网站DNS记录显示的IP地址或申请者的IP地址来确认所在国家，确保申请人的IP地址所在国与申请人实际所在国一致。
- 2) 请求域名的ccTLD。
- 3) 域名注册机构提供的信息。
- 4) 通过本文第3.2.2.1节中申请者提供的机构证明信息所在国家的确认。

If the certificate subject contains an option of country, the CA or the authorized RA shall verify the country using one of the following ways.

(1) Confirm the host country by checking the IP address displayed by the DNS record of the website or the IP address of the applicant through an authoritative third-party database, and ensure that the country where the applicant's IP address is located is consistent with the actual country where the applicant is located.

(2) The ccTLD of the requested domain name.

(3) Information provided by the domain name registrar.

(4) Confirm the country through the information provided by the applicant in Section 3.2.2.1 of this CP/CPS.



### 3.2.2.4 域名的确认和鉴别 Validation of Domain Authorization or Control

对于域名的验证,被验证的实体可以是申请者的母公司、子公司或联营公司,CMCA将采用以下鉴别方式中的一种,确认申请者拥有该域名。

For the verification of a domain name, the verified entity may be the applicant's parent company, subsidiary company or affiliate, and the CA or the authorized RA shall adopt one of the following authentication methods to confirm that the applicant owns the domain name.

- 1) 通过邮件方式发送随机值,然后接收一个使用该随机值的确认响应,确认申请人对FQDN的所有权。随机值必须发送到WHOIS注册备案的域名联系人电子邮件地址。(根据Baseline Requirements v2.0.1第3.2.2.4.2的域名验证方法)
- 2) 通过邮件方式发送随机值,然后接收一个使用该随机值的确认响应,确认申请人对FQDN的所有权。随机值必须发送到标识为域名联系人的电子邮件地址'adimn', 'adiministrator', 'webmaster', 'hostmaster' 或 'postmaster', 后面是 ("@" )之后跟着授权域名。(依据Baseline Requirements v2.0.1 第3.2.2.4.4的域名验证方法)
- 3) 通过在"/.well-known/ pki-validation"目录下对约定的信息进行改动,确认订户对FQDN的所有权。(依据Baseline Requirements v2.0.1 第3.2.2.4.18的域名验证方法)
- 4) 通过在DNS CNAME、TXT或CAA记录中是否存在已约定的随机值,以确认订户对域名的所有权。要求: 1) 授权域名; 或者2) 一个前缀以下划线字符开头的域名授权。(依据Baseline Requirements v2.0.1 第3.2.2.4.7的域名验证方法)

上述验证方法中用到的随机值有效期为从产生该随机值开始的30天。

CMCA不为.onion形式的域名签发SSL全球服务器证书。

- 1) Send a random value by email, and receive a confirming response using the random value to confirm the applicant's ownership of the FQDN. The random value must be sent to the domain name contact email address registered by WHOIS. (Based on the domain name validation method of Baseline Requirements v2.0.1 Section 3.2.2.4.2)
- 2) Send a random value by email, and receive a confirming response using the random value to confirm the applicant's ownership of the FQDN. The random value must be sent to the email address identified as the domain

name contact or created by using ' admin,' administrator',' webmaster', hostmaster' or ' postmaster', followed by the at-sign("@"), followed by an authorized domain name. (Based on the domain name validation method of Baseline Requirements v2.0.1 Section 3.2.2.4.4)

- 3) Confirm the subscriber's ownership of the FQDN by making changes to the agreed information under the "/. well-known/pki-validation" directory. (Based on the domain name validation method of Baseline Requirements v2.0.1 Section 3.2.2.4.18)
- 4) Confirm the subscriber's ownership of the domain name by confirming the presence of a negotiated random value in a DNS CNAME, TXT or CAA record.

Requirements: 1) authorized domain name; or 2) an authorized domain name with a prefix starting with underline character. (Based on the validation method of domain name in Baseline Requirements v2.0.1 Section 3.2.2.4.7).

The random value used in the above validation method remains valid for no more than 30 days from the time of creation. CMCA does not issue SSL Global Server Certificates for domain names in the form of .onion.

### 3.2.2.5 IP 地址的验证 Verification of IP address

组织机构如向 CMCA 申请全球服务证书，CMCA 将验证申请人对 IP 地址的所有权或控制权，IP 地址控制权验证方法使用如下方式：

通过信函、传真、SMS 或者邮递将一个随机值（有效期为从产生该随机值开始 30 天，且在每个电子邮件、传真、短信或邮政邮件中是唯一的。）发送给 IP 地址联系人，并收到使用该随机值的确认回复，以验证申请人对 IP 地址的控制权，按照 BR v2.0.1 章节 3.2.2.5.2 执行。

CMCA will verify the applicant's ownership or control of the IP address if the organization applies to CMCA for a global service certificate, IP address control verification methods use the following:

A random value (valid for 30 days from the date the random value is generated and unique in each e-mail, fax, text message, or post) by letter, SMS, or post.) sent to the IP address contact and received a confirmation reply using the

random value to verify the applicant's control over the IP address, executed in accordance with section BR v2.0.1 section 3.2.2.5.2.

### 3.2.2.6 通配符域验证 Wildcard domain validation

对于通配符“\*”右侧直接接顶级域名的申请，除非申请者能够有效证明其对于该顶级域名的所有命名空间的控制权，否则 CMCA 将拒绝该类申请。同时，将通过 Baseline Requirements v2.0.1 第 3.2.2.4.2、3.2.2.4.4、3.2.2.4.7 节的鉴别方式来核实通配符右侧的域名确实已被有效注册，并归属于该申请者。

For applications directly connected to the top domain name on the right side of the wildcard "\*", CMCA will reject the application unless the applicant can effectively prove its control over all namespace of the top domain name. At the same time, the authentication in 3.2.2.4.2, 3.2.2.4.4, and 3.2.2.4.7 of the Baseline Requirements v2.0.1 will verify that the domain name on the right side of the wildcard is effectively registered and belongs to the applicant

### 3.2.2.7 数据源的准确性 Accuracy of data sources

CMCA 采用准确、可靠的第三方数据源来验证证书申请者的信息。在选择是否依赖一个数据源之前，CMCA 会对该数据源的可依赖性、数据的准确性以及数据的抗更改和抗伪造性进行评估。将考虑以下几个方面：

- 1) 所提供的信息的年限；
- 2) 该数据源更新的频率，确保数据保持更新；
- 3) 数据的供应方，以及数据收集的目的；
- 4) 数据的公开可用性及可访问性；
- 5) 伪造或更改数据的难度。

对于 SSL 证书的验证数据源，若获得可依赖数据或文件的时间不超过本 CP/CPS 第 6.3.2 节中约定的证书最大有效期，则可复用。

CMCA uses accurate and reliable third - party data sources to verify the information of certificate applicants. CMCA evaluates the dependence on the data source, the accuracy of the data, and data change and forgery resistance

before choosing whether to rely on a data source. The following aspects will be considered:

- 1) Years of information provided;
- 2) The frequency of data source updates to ensure that data is kept up to date;
- 3) The supply side of the data and the purpose of data collection;
- 4) Open availability and accessibility;
- 5) Difficulty in falsifying or altering data.

For data sources that validate SSL certificates, you can reuse data or files that are dependent for no more than the maximum validity period of the certificate as stipulated in Section 6.3.2 of this CP/CPS.

### 3.2.2.8 CAA 记录 CAA records

CMCA 在签发 SSL 证书之前，将对签发证书主题别名扩展项中的每一个 `dNSName` 做 CAA 记录检查，并遵循查询到的指示。如果签发证书，必须在 CAA 记录的 TTL 时间或 8 小时内（两者更大者）。

CMCA will check for CAA records for each `dNSName` in the certificate SubjectAlternative Name extension before issuing the SSL certificate and follow the instructions found. If a certificate is issued, it must be within the TTL time or 8 hours of the CAA record (the greater one).

CMCA 根据 RFC8659 的规定处理 “issue”、“issuewild” 及 “iodef” 的属性标签：若 “issue”、“issuewild” 标签存在并且其中不包含 “cmca.net”，则 CMCA 不签发对应的证书；若 CAA 记录中存在 “iodef” 标签，则 CMCA 与申请者沟通后决定是否为其颁发证书。

CMCA shall process the property tags of "issue", "issuewild" and "iodef" as specified in RFC8659: if the "issue", "issuewild" tags exist and do not contain "cmca.net", CMCA will not issue the corresponding certificate, if the "iodef" tag appears in the CAA record, CMCA will communicate with the applicant and then decide whether to issue the certificate.

CMCA 以下列 CAA 记录查找失败情况作为可签发证书的条件：1) 在非 CMCA 的基础设施中查询 CAA 记录失败；2) 至少尝试过一次重新查找 CAA 记录；3) 域名所在区域不存在指向 ICNNA 根区域的 DNSSEC 验证链。

CMCA is permitted to treat a record lookup failure as permission to issue if:

- 1) The failure is outside the CA's infrastructure.
- 2) The lookup has been retried at least once.
- 3) the domain's zone does not have a DNSSEC validation chain to the ICANN root.

### **3.2.3 个人身份的鉴别 Authentication of Individual Identity**

CMCA 不受理个人证书业务，此部分要求仅针对企业申请授权办理人员的身份鉴别。中国移动 CMCA 将核对证书申请人信息与提供的身份证信息是否一致，并将数字证书申请人身份证复印归档备案。

CMCA objects individual certificate business. This requirement is only targeted for identity authentication of authorized clerks for corporate application. CMCA will check whether the certificate applicant information is consistent with the ID card information provided, and file the digital certificate applicant ID card.

### **3.2.4 没有验证的订户信息 Subscriber information not validated**

CMCA 签发的证书信息没有未经过验证的信息。

The certificate information issued by CMCA has no unverified information.

### **3.2.5 授权确认 Validation of Authority**

当申请者代表组织机构订户申请证书时，需要出示足够的证明信息以证明申请者是否已获得组织机构的授权。CMCA 有责任确认该授权信息，并将授权信

息妥善保存。

当机构授权经办人办理证书业务时，应当进行的核实验证流程参照本 CP/CPS 相关要求。

CMCA 允许申请者指定独立个人来申请证书。若申请者以书面形式指定证书申请人，则不接受在该指定人员以外的其他人提交证书申请请求。在收到申请者确认的书面请求时，应向申请者提供其已授权人员的清单。

When the applicant applies for a certificate on behalf of the organization subscribers, sufficient certification information is required to demonstrate whether the applicant has been authorized by the organization. CMCA has the responsibility to confirm the authorization information and properly preserve the authorization information.

When the agency authorizes the handler to engage in certificate business, the verification procedure should refer to requirements of this CP/CPS.

CMCA gives its consent to applicants to designate independent individuals to apply for certificates. In case the applicant appoints the certificate applicant in writing, submission of certification application request by people other than the designated clerks is prohibited. Upon receipt of the written request confirmed by the applicant, the applicant shall be provided with a list of its authorized personnel.

### 3.2.6 互操作准则 Interoperational guidelines

对于申请 CMCA 全球信任体系下的 DV 证书、OV 证书及 EV 证书，CMCA 承担对订户身份的鉴别职能，暂不委托其他机构行使此职责。

CMCA 不签发任何交叉认证的证书。

For applying for DV certificates, OV certificates and EV certificates under CMCA Global Trust System, CMCA undertakes the identification function of subscriber identity and temporarily does not entrust other agencies to perform this responsibility .

CMCA refrains from issuing any cross-certified certificates.

### 3.3 更新请求的标识与鉴别 Identification and authentication for renewal request

在订户证书到期前，订户需要获得新的证书以保持证书使用的连续性。证书更新请求包含“密钥更新”和“证书更新”，对于“密钥更新”，中国移动 CMCA 一般要求订户产生一个新的密钥对代替过期的密钥，具体参考（同 4.7）；对于“证书更新”，CMCA 暂不支持该服务。客户申请更新证书时，需重新填写证书更新表，按照初始身份验证步骤提交相关资料（同 4.1），并由中国移动 CMCA 审核。

Before the subscriber certificate expires, the subscriber needs to obtain a new certificate to maintain the continuity of the certificate use. Certificate Update requests include both Key Update and Certificate Update. For key update, CMCA generally requires subscribers to produce a new key pair instead of expired key with specific reference (as 4.7), CMCA will not complete the certificate update form and submit the information (as 4.1) and reviewed by CMCA.

#### 3.3.1 常规更新的标识与鉴别 Identification and authentication for renewal request

由于证书到期、证书信息更改或密钥更新等情况，证书需要更新。

经中国移动 CMCA 签发证书有效期一般为 1 年，有效期不超过 397 天。

证书到期前一个月，中国移动 CMCA 会提醒证书持有者进行证书更新。

证书客户申请更新证书时，填写证书更新表，按照初始身份验证步骤提交相关资料（同 3.2），并由中国移动 CMCA 或其授权机构审核。

Prior to the expiry of the subscriber certificate, the subscriber needs to obtain the new certificate to keep the certificate usage continuity.

The certificate issued by CMCA is generally 1 year, not more than 397 days.

One month before the certificate expires, CMCA reminds the certificate holder to make the certificate update.



Certificate customer applies for renewal certificate, fill out certificate update form, submit relevant information according to initial authentication step (same as 3.2), and be reviewed by CMCA or its authorized organization.

### **3.3.2 吊销后更新的标识与鉴别 Identification and authentication for renewal after revocation**

吊销后的证书必须重新生成新的公私钥对并按照 3.2 的规定申请新的证书。  
The revoked certificate must regenerate the new public-private key pair and apply for the new certificate in accordance with 3.2.

## **3.4 吊销请求的标识与鉴别 identification and authentication for revocation request**

### **3.4.1 证书吊销情况 Certificate revocation condition**

订户本人申请吊销证书，其身份鉴别使用初始身份确认相同的流程，详见 3.2。

如果是 CMCA 主动发起吊销，如订户没有履行本 CP/CPS 所规定的义务，则不需要对订户身份进行标识和鉴别。由 CA\RA 发出的吊销操作应有相应的 request 记录能够标识出是由 CA\RA 主体发起的吊销。

Subscriber himself applies for revocation of the certificate, its identity using the same process of initial identification, see 3.2 for details.

When CMCA initiates the revocation, if the subscriber fails to fulfill the obligations stipulated in this CP/CPS, there is no need to identify and identify the subscriber identity. The revocation operation issued by the CA\RA should have the corresponding request record to identify the revocation initiated by the CA\RA subject.

### 3.4.2 吊销操作 Revocation operation

证书客户申请吊销证书时，填写证书吊销申请表，通过一定的方式，如邮寄、邮件、传真等，向中国移动 CMCA 提交，并由中国移动 CMCA 审核。

When the certificate customer applies for revocation of the certificate, fill in the certificate revocation application form and submit it to the CMCA by certain means, such as mail, mail, fax, etc., and be examined by the CMCA.

## 4. 证书生命周期操作要求 Certificate life cycle operational requirements

### 4.1 证书申请 Certificate application

#### 4.1.1 证书申请实体 Who Can Submit a Certificate Application

任何实体需要使用 CMCA 全球信任体系下签发的证书时，均可提出证书申请。

Any entity that needs to use a certificate issued under the CMCA global trust system can submit a certificate application.

#### 4.1.2 注册过程与责任 Enrollment process and responsibilities

申请者应事先了解订户协议、本 CP/CPS 等文件约定的事项，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。

申请者应向 CMCA 递交证书申请表及相应证明文件，此行为即意味着申请者已经了解和接受订户协议。

The applicant shall have prior knowledge of the matters stipulated in the Subscriber Agreement, this CP/CPS, in particular those relating to the scope of

application, rights, obligations and guarantees of the certificate.

Applicants should submit a certificate application form and corresponding supporting documents to CMCA, which means that the applicant has understood and accepted the subscriber agreement.

## 1、最终订户

最终订户即申请证书的实体，最终订户须明确表示其愿意接受本CP/CPS中所规定的相关责任与义务（本CP/CPS及相关CP公布在CMCA网站上），并需要按照3.2.2的要求提供真实、准确的申请信息；根据《中华人民共和国电子签名法》的规定，申请者未向CMCA提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、CMCA造成损失的，订户应承担相应的法律及赔偿责任。订户有责任保护其拥有的证书私钥安全。

### 1、Subscribers

The subscribers, the entity applying for the Certificate, shall expressly express its willingness to accept relevant responsibilities and obligations under this CP/CPS (this CP/CPS are published on CMCA website) and shall provide true and accurate application information as required by 3.2.2. According to Electronic Signature Law of the People's Republic of China, If the applicant fails to provide true, complete and accurate information to CMCA, or has other faults, causing losses to the electronic signature relying party and CMCA, the subscriber shall bear corresponding legal and compensation liabilities. The subscriber has the responsibility to secure the certificate private key that it owns.

## 2、认证及注册机构

订户可以直接向CMCA申请证书，由CMCA审核订户信息并处理订户的请求。注册机构对订户提供的身份信息参照3.2.2的要求进行鉴别，CMCA对通过鉴别后的订户签发证书。CMCA作为电子认证机构，应妥善保管证书订户申请信息。CMCA应在适当时间将证书订户的信息归档，同时应履行本CP/CPS中所规定的相关责任与义务。

### 2、Certification and Registration Authority

Subscribers can apply for certificates directly from CMCA, and the subscriber information is audited by CMCA and the subscriber's request is processed. According to the requirements of 3.2.2, the registered institution identifies the identity information provided by the subscriber CMCA issues a certificate to the authenticated subscriber. CMCA as an electronic certification body, the certificate subscriber application information should be properly kept. CMCA shall file the information of the certificate subscriber at the appropriate time, and shall fulfill the relevant responsibilities and obligations stipulated in this CP/CPS.

## 4.2 证书审核 Certificate Application Processing

### 4.2.1 执行识别与鉴别功能 Performing identification and authentication functions

1. CMCA 处理证书申请至少需要设置 3 个可信角色：信息录入、信息审核、签发证书。其中信息录入、信息审核需要职责分离。

1. At least three trusted roles need to be set up CMCA processing certificate applications: information entry, information validation, and issuance of certificates. Separation of responsibilities is required for information entry and information validation.

2. 对于证书申请处理，签发证书人员需对申请机构信息做最终审核：

1) 对所有用以验证申请机构证书申请的信息和文件进行复核，查找冲突的信息或需要进一步验证的信息；

2) 如复核人提出的问题确实需要得到进一步验证，CMCA 必须从申请机构、协议签署人、申请审批人或其他合格的独立信息来源取得进一步验证的资料或证据；

3) CMCA 必须保证已收集的与证书申请相关的信息和资料，足以确保签发的证书不包含 CMCA 已知或应发现的错误信息，否则 CMCA 将会拒绝证书的申请并通知申请机构；

4) 如果部分或所有的身份验证资料内容使用语言不是 CMCA 的官方语

言，那么CMCA将会使用经过适当的培训、具备足够的经验和判断能力的人员完成最终的交叉审核和尽职调查。CA通过以下方法执行交叉审核与尽职调查：

4.1) 依赖翻译的材料内容；

4.2) 依赖拥有此语言能力的代理机构完成此步骤，CMCA复核代理机构的检查结果，并且复核证书标准中的CMCA自我审核要求。

5) 根据CA/BForum的相关指引，CMCA在执行识别和鉴别职责时，将对客户提交的域名信息进行CAA查询，CMCA会查询订户是否有指定的CA机构，具体通过查询CAA公开数据来判断，如果订户有指定CA机构，则CMCA将不再受理证书申请；反之，CMCA正常受理证书业务申请。如果签发证书，必须在CAA记录的TTL时间或8小时内（两者更大者）。并在审核记录中体现。

2. For certificate application processing, certificate issuing personnel shall make final review on the basis of application agency information:

1 ) Review all information and documents used to verify the application agency certificate application , to find conflicting information or information requiring further verification ;

2 ) If the questions raised by the reviewer do need to be further verified, CMCA must obtain further verified data or evidence from the application agency , the agreement signatory , the application approver or other qualified independent sources of information ;

3 ) CMCA must ensure that the information and information collected in connection with the certificate application is sufficient to ensure that the certificate issued does not contain CMCA known or detected error information, otherwise CMCA will reject the certificate application and notify the applicant;

4 ) Where part or all of the authentication content is in a language that is not the official language of CMCA, the final cross-audit and due diligence will be completed using appropriately trained personnel with sufficient experience and judgment. CA performs cross-checking and due diligence by:

4.1) Material content dependent on translation;

4.2) Relying on an agent with this language capability to complete this step , CMCA reviews the inspection results of the agents , and reviews CMCA self - audit requirements in the certificate criteria .

5 ) According to the relevant guidance of CA/B Forum , CMCA will CAA

query the domain name information submitted by the customer when performing the identification and identification responsibilities, CMCA will inquire whether the subscriber has a designated CA institution, and judge by inquiring the CAA public data. If the subscriber has a designated CA institution, CMCA will no longer accept the certificate application; otherwise, CMCA normally accepts the certificate business application. If a certificate is issued, it must be within TTL or 8 hours of CAA (larger).

And reflected in the audit records.

### 3. CMCA 建立高风险证书请求额外验证机制:

- 1) 建立高风险申请人列表, 获取信息的渠道包括但不限于反钓鱼联盟、防病毒厂商、负责网络安全事务的政府机构、媒体的公开报道等;
- 2) 对于出现在高风险申请人列表的机构, **CMCA** 有权直接拒绝证书申请或请其提供额外的验证材料, 对于已签发的证书也应定期根据高风险申请人列表进行复核, 如出现在列表中, 并采取适当行动 **CMCA** 有权直接吊销证书申请或请其提供额外的验证材料。

### 3. CMCA establishes additional verification mechanisms for high-risk certificate requests:

- 1) Establish a list of high-risk applicants and access to information includes, but is not limited to, anti-fishing unions, anti-virus manufacturers, government agencies responsible for cybersecurity, public media coverage, etc;
- 2) For institutions appearing on the list of high risk applicants, CMCA has the right to directly reject certificate applications or to provide additional verification materials, Certificate issued should also be regularly reviewed based on the list of high - risk applicants, if appearing in the list and take appropriate action CMCA has the right to directly revoke the certificate application or request them to provide additional verification materials.

## **4.2.2 CMCA 证书申请批准和拒绝 Approval and rejection of certificate application**

CMCA将在合理的时间内完成证书申请处理。在申请者提交的资料齐全且审核通过的情况下，1-3个工作日处理完成。EVSSL全球服务器证书处理证书申请时间不超过5个工作日，特殊情况最长不超过10个工作日。

CMCA拒绝签发包含内部名称的证书。

CMCA拒绝签发包含匿名、伪名证书。

CMCA will complete the certificate application processing within a reasonable time. If the information submitted by the applicant is complete and approved, the processing is completed within 1-3 working days. EVSSL Global Server Certificate Processing Certificate Application does not exceed 5 working days and 10 working days in special cases.

CMCA refused to issue certificates containing internal names.

CMCA refused to issue a certificate containing anonymity and pseudonym.

## **4.2.3 处理证书申请的时间 Time to process certificate applications**

在证书申请者提交资料齐全并符合要求的情况下，CMCA在3个工作日内完成证书申请的处理，EVSSL全球服务器证书处理证书申请时间不超过5个工作日，特殊情况最长不超过10个工作日。

If the certificate applicant submits complete information and meets the requirements, CMCA will complete the processing of the certificate application within 3 working days, and the EV SSL Global Server certificate processing certificate application time is not more than 5 working days, and not more than 10 working days in special circumstances.



## 4.3 证书签发 Certificate Issuance

### 4.3.1 证书签发中注册机构和电子认证服务机构的行为 CA

#### Actions during Certificate Issuance

CMCA 在订户申请通过鉴别后，RA 系统操作员录入订户申请信息，并提交 RA 系统审核员审核；RA 系统审核员审核通过后，向 CA 系统提交申请；CA 系统向 RA 系统返回证书，由 CA 以安全的形式将证书反馈给订户。

CMCA after the subscriber application has passed the authentication, RA the system operator input the subscriber application information and submit it to the RA system auditor for review; after the RA system auditor approves, submit the application to the CA system; Return the certificate to the RA system by the CA in a secure form.

### 4.3.2 电子认证服务机构和注册机构对订户的通告

#### Notification of Certificate Issuance

CMCA 无论是拒绝还是批准订户的证书申请，CMCA 有义务告知订户申请结果。CMCA 会以电话、电子邮件或其他方式对订户进行通告。

CMCA is obliged to inform the subscriber of the result of the application, whether it is to reject or approve the subscriber's certificate application. CMCA will notify subscribers by telephone, email or otherwise.

## 4.4 证书接受 Certificate acceptance

### 4.4.1 构成接受证书的行为 Notification of Certificate Issuance

证书申请者从获得证书起就被视为已同意接受证书。证书申请者接受数字证书后，应妥善保管其证书对应的私钥。

一旦接受中国移动 CMCA 发证机构签发的证书，从接受之时起直至证书的整个使用有效期内，如果证书申请者不另行通知，那么证书申请者被视为向中国移动 CMCA、注册机构及所有依赖方出如下保证：

- 1)客户的每一次数字签名，都是证书申请者自己的数字签名，并且在进行数字签名时，证书是有效证书并已被证书申请者接受；
- 2)未经授权的人员从未访问过证书申请者私钥；
- 3)证书申请者向发证机构陈述的所有证书申请相关的信息是真实的；
- 4)包含在证书中的信息，都是真实的；
- 5)证书将按中国移动 CMCA 电子认证业务规则的规定，只用于经过授权的或其它合法的使用目的；
- 6)证书申请者是最終证书申请者而不是发证机构。除非经证书申请者和发证机构间的书面协议明确批准，证书申请者保证不从事发证机构（或类似机构）所从事的功能，例如：把与证书中所含的公钥所对应的私钥用于签发任何证书（或认证其他任何形式的公钥）或证书吊销列表。
- 7)一经接受证书，既表示证书申请者知悉和接受中国移动 CMCA 认证业务声明中的所有条款和条件，并知悉和接受相应的证书订户协议。

The certificate applicant is deemed to have agreed to accept the certificate from the time of obtaining the certificate. After the certificate applicant accepts the digital certificate, the private key corresponding to his certificate shall be properly preserved.

Once a certificate issued by the CMCA issuer is accepted, from the time of the acceptance until the entire period of the use of the certificate without notice:

- 1) Each digital signature of the customer is the own digital signature of the certificate applicant , and in the digital signature , the certificate is a valid certificate and has been accepted by the certificate applicant ;
- 2) Un authorized person has never accessed the certificate applicant private key;
- 3) All the information related to the certificate application stated by the certificate applicant to the certificate issuing institution is true;

- 4) The information contained in the certificate is true;
- 5) Certificates will be used only for authorized or other legitimate purposes as stipulated in the CMCA Electronic Certification Business Rules;
- 6) The certificate applicant is the final certificate applicant and not the issuing agency. Unless expressly approved by a written agreement between the certificate applicant and the issuing agency, the certificate applicant undertakes not to perform the functions performed by the issuing agency (or similar institution), For example, the private key corresponding to the public key contained in the certificate is used to issue any certificate (or to authenticate any other form of public key) or certificate revocation list.
- 7) As soon as the certificate is accepted, it means that the certificate applicant is aware of and accepts all the terms and conditions in the CMCA Certification Business statement, and knows and accepts the corresponding certificate subscriber agreement.

#### **4.4.2 电子认证服务机构对证书的发布 Publication of the certificate by the CA**

对于最终订户证书，CMCA将根据用户的意愿采取适当形式的发布；订户没有要求发布的，CMCA将不发布最终订户证书。

The final subscriber certificate will CMCA be issued in the appropriate form according to the user's wishes; if the subscriber does not require publication, CMCA will not issue the final subscriber certificate.

### **4.4.3 CMCA 对其他实体的通告 Notification of certificate issuance by the CA to other entities**

对于CMCA签发的证书，CMCA不对其他实体进行通告，依赖方可以在信息库上自行查询。

For certificates issued by CMCA, CMCA does not notify other entities, and dependent parties can query themselves on the information database.

## **4.5 密钥和证书的使用 Key Pair And Certificate Usage**

### **4.5.1 订户私钥和证书的使用 Subscriber private key and certificate usage**

订户的私钥和证书应用于规定的、批准的用途（在本CP/CPS1.4.1节定义），订户在使用证书时必须遵守本CP/CPS的要求，妥善保存其私钥，避免他人未经本人授权而使用本人证书情形的发生，否则其应用是不受保障的。

The private key and certificate of the subscriber shall be used for the specified and approved purposes (as defined in section 1.4.1). The subscriber must comply with the requirements of this CP/CPS when using the certificate, keep its private key properly, and avoid the occurrence of the use of my certificate by others without my authorization, otherwise its application is not guaranteed.

#### **1、证书持有者的公钥和证书使用**

证书持有者只能在指定的应用范围内使用私钥和证书，证书持有者只有在接受了相关证书后才能使用对应的私钥，并且在证书到期或被吊销后，须停止使用该证书及对应的私钥。

#### **2、依赖方的公钥和证书使用**

当依赖方接受到签名的信息后，应该：

- ◆ 获得对应的证书及信任链；
- ◆ 验证证书的有效性；
- ◆ 确认该签名对应的证书是依赖方信任的证书；

- ◆ 证书的用途适用于对应的签名；令使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

当依赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密。

#### 1、Public key and certificate usage of certificate holder

The certificate holder can only use the private key and certificate within the specified scope of application. The certificate holder can only use the corresponding private key after accepting the relevant certificate, and after the certificate expires or is revoked, the certificate and the corresponding private key shall be stopped.

#### 2、Dependent party public key and certificate usage

When the relying party receives the signed information, it should:

- ◆ Obtain corresponding certificates and trust chains;
- ◆ Validation of certificates;
- ◆ Confirm that the certificate corresponding to the signature is the certificate trusted by the relying party;
- ◆ The purpose of the certificate applies to the corresponding signature; ordered to verify the signature using the public key on the certificate.

Any of the above links fails, and the dependent party should refuse to accept the signature information.

When the relying party needs to send the encryption information to the receiving party, it must first obtain the encryption certificate of the receiving party through the appropriate way, and then use the public key on the certificate to encrypt the information.

### **4.5.2 依赖方公钥和证书的使用 Relying party public key and certificate usage**

依赖方信赖CMCA全球信任体系签发的证书所证明的信任关系时需要：

- 1) 获取并安装该证书对应的证书链；
- 2) 在信赖证书所证明的信任关系前确认该证书为有效证书，包括：检查CMCA公布的最新CRL，或者通过CMCA提供的OCSP服务确认该证书

未被吊销；检查该证书路径中所有出现过的证书的可靠性；检查该证书的有效期；以及检查其他能够影响证书有效性的信息；

- 3) 在信赖证书所证明的信任关系前确认该证书记载的内容与所要证明的内容一致。

Creditors' trust CMCA the relationship of trust evidenced by certificates issued by the global trust system need to:

- 1) Obtain and install the certificate chain corresponding to the certificate;
- 2) Confirm that the trust certificate is valid before the trust relationship. These include: checking the latest CRL, published by CMCA or confirming that the certificate has not been revoked through the OCSP service provided by the certificate; checking the reliability of all certificates that have appeared in the certificate path; checking the validity of the certificate; and checking other information that can affect the validity of the certificate;
- 3) Prior to the trust relationship proved by the trust certificate, confirm that the contents of the certificate are consistent with the contents to be proved.

## 4.6 证书更新 Certificate renewal

CMCA不提供全球信任证书更新服务。

CMCA does not provide a Global Trust Certificate Update service.

### 4.6.1 证书更新的原因 Circumstance for Renewal

不适用。

Not applicable.

### 4.6.2 请求证书更新的实体 Who may request renewal

不适用。

Not applicable.

### **4.6.3 证书更新流程 Processing for Renewal**

不适用。

Not applicable.

### **4.6.4 颁发新证书时对订户的通告 Notification of new certificate issuance to subscriber**

不适用。

Not applicable.

### **4.6.5 构成接受更新证书的行为 Conduct constituting acceptance of a renewal certificate**

不适用。

Not applicable.

### **4.6.6 电子认证服务机构对更新证书的发布 Publication of the renewal certificate by the CA**

不适用。

Not applicable.

### **4.6.7 电子认证服务机构对其他实体的通告 Notification of certificate issuance by the CA to other entities**

不适用。

Not applicable.



## 4.7 证书密钥更新 Certificate Re-key

证书密钥更新是指订户生成新的密钥对并申请为新公钥签发新证书 CMCA。

Certificate key update means that the subscriber generates a new key pair and applies for the issuance of a new certificate new public key.

### 4.7.1 证书密钥更新的情形 Circumstance for Re-key

- 1、当订户证书密钥遭到损坏时；
  - 2、当订户证实或怀疑其证书密钥不安全时；
  - 3、其它可能导致密钥更新的情形。
1. When the subscriber certificate key is corrupted;
  2. When the subscriber confirms or suspects that its certificate key is not secure;
  3. Other circumstances that may result in key updates.

### 4.7.2 请求证书密钥更新的实体 Who may request certification of a new public key

已经申请过 CMCA 证书的订户可申请证书密钥更新。

Subscribers who have applied for a CMCA certificate can apply for a certificate key update.

### 4.7.3 证书密钥更新请求的处理 Processing for Re-key

同 3.3。

Same as 3.3.

#### **4.7.4 颁发新证书时对订户的通告 Notification of new certificate issuance to subscriber**

同 4.3.2。

Same as 4.3.2.

#### **4.7.5 构成接受密钥更新证书的行为 Conduct constituting acceptance of a re-keyed certificate**

同 4.4.1。

Same as 4.4.1.

#### **4.7.6 电子认证服务机构对密钥更新证书的发布 Publication of the re-keyed certificate by the CA**

同 4.4.2。

Same as 4.4.2.

#### **4.7.7 电子认证服务机构对其他实体的通告 Notification of certificate issuance by the CA to other entities**

同 4.4.3。

Same as 4.4.3.

### **4.8 证书变更 Certificate Modification**

#### **4.8.1 证书变更的原因 Circumstance for Modification**

不适用。

Not applicable.

#### **4.8.2 请求证书变更的实体 Who may request certificate modification**

不适用。

Not applicable.

#### **4.8.3 证书变更的流程 Processing for Modification**

不适用。

Not applicable.

#### **4.8.4 颁发新证书时对订户的通告 Notification of new certificate issuance to subscriber**

不适用。

Not applicable.

#### **4.8.5 构成接受变更证书的行为 Conduct constituting acceptance of modified certificate**

不适用。

Not applicable.

#### **4.8.6 电子认证服务机构对变更证书的发布 Publication of the modified certificate by the CA**

不适用。

Not applicable.

### 4.8.7 电子认证服务机构对其他实体的通告 Notification of certificate issuance by the CA to other entities

不适用。

Not applicable.

## 4.9 证书吊销和挂起 Certificate revocation and suspension

### 4.9.1 证书吊销的情形 Circumstances for Revocation

#### 4.9.1.1 订户证书吊销的原因 Reasons for Revoking a Subscriber Certificate

如有下列情况中的任何一种情况发生，则必须在24小时之内撤销证书：

- 1) 订户书面申请吊销数字证书；
- 2) 订户通知CA最初的证书申请未经有效授权；
- 3) 订户相信或怀疑密钥泄漏或遭受攻击，存放证书的服务器损坏或被锁定等情形；或者CA有证据表明订户证书私钥泄露的情形；
- 4) CMCA获知已出现了经过验证的订户私钥泄露方法，该方法可基于公钥很容易地计算出订户私钥（例如 Debian 弱密钥，请参阅 <http://wiki.debian.org/SSLkeys>）；
- 5) CA机构获得证据，证书中所包含的域名或IP地址的控制权验证已不再可靠。

The subscriber's certificate must be revoked within 24 hours if any of the following occurs:

- 1) The subscriber applies for revocation of digital certificate in writing;
- 2) Subscriber notices CA original certificate application is not validly authorized;
- 3) Sub scribers believe or suspect that the key is leaking or attacked , the server where the certificate is damaged or locked ; or CA has evidence of

the private key disclosure of the subscriber certificate;

4) CMCA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see <https://wiki.debian.org/SSLkeys>);

5) CMCA obtains evidence that the validation of domain authorization or control for any Fully- Qualified Domain Name or IP address in the Certificate should not be relied upon.

CA 应该在 24 小时内撤销证书，如有下列其中一项或多项，必须在 5 天内撤销证书：

1. 证书不再符合Mozilla Root Store Policy或CA/Browser论坛的Baseline第Requirements中第6.1.5及6.1.6节的规定；

2. CA取得证书被滥用的证据；

3. CA获悉订户已违反订户协议或使用条款项下的一项或多项重要义务；

4. CA 机构得知订户不再能合法使用证书中包含的域名或 IP 地址，如法院或仲裁停止了域名注册商使用某域名的权限，或域名注册商与申请人之间的使用许可或服务协议终止了；

5. CA 了解到某通配符证书被用于验证具有欺诈误导性质的域名；

6. CA获悉证书所载的信息有重大改变；

7.发现并证实某证书没有根据 CA/浏览器论坛（CA/Browser Forum）发布的最新版本 Guidelines 、 Baseline Requirement 以及CP/CPS 要求的程序而签发；

8. CA确定或知悉证书内的任何信息不准确；

9. CA 签发证书的权利已届满或被撤销或终止，除非 CA 已作出安排，继续维护 CRL/OCSP；

10. CA的CP及/或CP/CPS规定撤销证书；

11. 证书的技术内容或格式造成了对应用软件供应商或依赖方不可接受的风险，如 CA/浏览器论坛决定弃用某种算法或密钥长度，认为其风险水平不可接受，在一定期限内 CA 应撤销此类证书。

CA should revoke the certificate within 24 hours, if one or more of the following must be revoked within 5 days:

1. The certificate no longer complies with Cla uses 6.1.5 and 6.1.6;

2. CA obtained evidence of certificate abuse;

3. CA was informed that the subscriber has breached one or more important obligations under the subscriber agreement or the terms of Use;

4. CA agency learns that the subscriber can no longer legally use the domain or IP address contained in the certificate, such as the court or arbitration has stopped the permission of the domain registrar to use a domain name, or that the use license or service agreement between the domain registrar and the applicant is terminated;

5. CA learned that a wildcard certificate is used to verify a domain name that is fraudulent and misleading;

6. The CA was informed of significant changes in the information contained in the certificate;

7. Found and confirmed that a certificate was not issued under the latest version of Guidelines 、 Baseline Requirement released by the CA/ browser forum (CA/Browser Forum) and the program required by CP/CPS;

8. CA identified or knew the inaccuracy of any information in the certificate

9. CA's right to issue certificates has expired or been revoked or terminated unless CA makes arrangements to continue to maintain CRL/OCSP;

10. CA's CP/CPS regulations provide to revoke the certificate;

11. The technical content or format of the certificate poses an unacceptable risk to the application supplier or relying party, such as the decision of the CA/ browser forum to discard an algorithm or key length, which considers its risk level unacceptable, and within a certain period of time CA such certificate should be revoked.

#### 4.9.1.2 吊销下级 CA 证书的原因 Reasons for Revoking a Subordinate CA Certificate

撤销下级 CA 证书的情形:

若发生下列一种或多种情况, 签发 CA 应在七(7)天内撤销下级 CA 证书:

1. 下级核证机关要求书面撤销;

2. 下级 CA 通知签发 CA，原来的证书请求没有得到授权，并且没有后续补充授权；
3. 签发 CA 取得证据，证明其所属 CA 与证书上的公钥对应的私钥发生了密钥泄露或不再符合第 6.1.5 和 6.1.6 条的要求；
4. 签发 CA 取得证书被滥用的证据；
5. 签发 CA 意识到证书不是按照 CA/浏览器论坛（CA/Browser Forum）发布的最新版本的 EV Guidelines 、 Baseline Requirement 以及 CP/CPS 要求签发的，或者下级 CA 没有遵守 CA/浏览器论坛（CA/Browser Forum）发布的最新版本的 EV Guidelines 、 Baseline Requirement 以及 CP/CPS 要求；
6. 签发 CA 确定证书所载的任何信息不准确或有误导性；
7. 签发 CA 或附属 CA 因任何理由而停止运作，并没有安排其他 CA 为该证书提供撤销支持；
8. 签发 CA 或下级 CA 签发证书的权利已届满或被撤销或终止，除非 CA 已做出安排，继续维护 CRL/OCSP；
9. 签发 CA 的 CP/CPS 规定撤销证书。

#### Case of of lower CA certificate

The issuance of the CA shall be revoked within seven (7) days from the lower CA certificate if one or more of the following occurs:

1. Lower certification authorities require written revocation;
2. The original certificate request CA, the lower CA notice was not authorized and there was no subsequent supplementary authorization;
3. The issuing CA to obtain evidence that the private key corresponding to the public key on the certificate to which it belongs been disclosed or no longer meets the requirements of articles 6.1.5 and 6.1.6;
4. Evidence of abuse in issuing CA obtaining certificates;
5. The issuing CA is aware that the certificate is not issued in accordance with the EV Guidelines; Baseline Requirement and CP/CPS requirements of the latest version issued by the CA/ Browser Forum (CA/Browser Forum), or that the subordinate CA does not comply with the EV Guidelines, Baseline



Requirement and CP/CPS requirements of the latest version issued by the CA/Browser Forum;

6. Determineing that any information contained in the certificate is inaccurate or misleading;

7. Issuing CA or affiliated CA ceased operations for any reason and did not arrange other CA to provide revocation support for the certificate;

8. Issuing CA or subordinate CA to issue certificates has expired or has been revoked or terminated unless the CA has arranged to continue to maintain the CRL/OCSP;

9. CP/CPS provision for revocation of certificates issued.

#### **4.9.2 请 求 证 书 吊 销 的 实 体 Who Can Request Revocation**

可要求撤销证书的实体包括：订阅者、RA、CA、法院、政府主管部门及其他公权力部门。此外，订阅者、依赖方、应用软件供应商和其他第三方可以通过在线提交或者邮件等方式（详见 [www.cmca.net](http://www.cmca.net) 官网联系方式）提交证书问题报告，通知发出证书的 CA 撤销证书的合理原因。

同时，CMCA也可在4.9.1所述的情形下主动吊销订户的证书。

The entities that may require certificate revocation include subscribers, RA, CA, courts, government authorities and other public authorities. In addition, subscribers, dependent parties, application software suppliers and other third parties can submit a certificate issue report by online submission or email (see the [www.cmca.net](http://www.cmca.net) official website contact information for details) to notify the CA reason to revoke the certificate.

At the same time, CMCA may voluntarily revoke the subscriber's certificate in the circumstances described in 4.9.1.

### 4.9.3 吊销请求的流程 Processing for Revocation

CMCA提供7x24稳定的系统服务，可以实时接受和响应证书吊销请求和证书问题报告。订阅者、依赖方、应用软件供应商和其他第三方如发现或怀疑证书存在问题，可以通过CMCA官网及时报告，包括不限于以下情形可疑的私钥泄漏、证书误用或其他类型的欺诈、折衷、误用、不当行为或与证书相关的任何其他事项。

CMCA provides 7x24 stable system services, can accept and respond to certificate revocation requests and certificate problem reports in real time. Subscribers, relying parties, application vendors and other third parties may report problems with certificates in a timely manner through CMCA website, including private key leaks, certificate misuse or other types of fraud, tradeoffs, misuse, misconduct or any other matters related to certificates that are not limited to the following suspicious circumstances.

吊销分为主动吊销和被动吊销。主动吊销是指订户提出吊销申请，由CMCA审核通过后吊销证书的情形；被动吊销是指当CMCA确定订户违反证书使用规定、约定、或是订户主体已经消亡等情况发生时，采取吊销证书的手段已停止对该证书的证明。

Revocation is divided into active revocation and passive revocation. Active revocation refers to the case where the subscriber applies for revocation and cancels the certificate after CMCA passes the certificate; passive revocation refers to the certificate by the revocation of the certificate.

#### 4.9.3.1 主动吊销 Active revocation

订户申请吊销证书前应指定并书面授权证书吊销申请代表，提供有效身份证明文件及证书吊销申请文件，并接受证书吊销申请的有关条款，同意承担相应的责任。

The subscriber shall appoint and authorize the certificate revocation application representative in writing before applying for revocation, provide valid identification documents and certificate revocation application documents,

accept the relevant terms of the certificate revocation application, and agree to bear the corresponding liability.

CMCA7\*24接受订户证书吊销申请，并处理订户证书吊销请求。

CMCA7\*24 accepts the subscriber certificate revocation application and process the subscriber certificate revocation request.

CMCA收到订户的吊销申请材料后，将查询订户需吊销的证书是否为CMCA所发放，证书是否在有效期内，吊销理由是否属实，若均通过则对证书进行吊销。

CMCA receiving the subscriber's revocation application materials, the subscriber will inquire whether the certificate to be revoked is issued by CMCA, whether the certificate is within the validity period, whether the reason for revocation is true, and if all pass, the certificate will be revoked.

#### 4.9.3.2被动吊销Passive revocation

当出现被动吊销的情形时，CMCA将以适当形式通知订户，告知拟吊销的证书内容、吊销原因、吊销操作时限等事项，在确认订户收到吊销通知且无异议后予以吊销。

In the case of passive revocation occurs, CMCA will notify the subscriber in an appropriate form, inform the contents of the certificate, the reason, the suspension time limit and other matters, and confirm that the subscriber receives the revocation notice with no objection.

CMCA在发现证书订户身份资料有问题或其对证书有非法使用情况下，可根据CA策略对终端客户的证书执行吊销操作，无需用户提出吊销申请。

- 证书的私钥泄漏；
- 客户未缴纳证书相关费用；
- 其他中国移动 CMCA 认为有必要吊销客户证书的原因
- 中国移动 CMCA 或授权的注册机构或受理点书面填写“证书吊销申请表”，并附上必须吊销证书的问题报告；
- 中国移动 CMCA 或授权的注册机构按照第三章的要求对等待吊销的证书申请进行审核；
- 中国移动 CMCA 吊销客户证书后，发证机构将通知客户证书被吊销以及

吊销原因;

- 吊销的客户证书在 24 小时内进入 CRL 或被直接签发 CRL, 向外界公布。

CMCA if it is found that there is a problem with the identity information of the certificate subscriber or its illegal use of the certificate, the certificate of the terminal customer can be revoked according to the CA strategy, without the need for the user to apply for revocation.

- Private key leak for the certificate;
- Customer has failed to pay the certificate - related fees;
- Any other reason why CMCA consider it necessary to revoke customer certificates;
- CMCA or authorized registration agencies or acceptance points to fill in the "certificate revocation application form" in writing, and attach the issue of the certificate must be revoked report;
- CMCA or authorized registration agencies in accordance with the requirements of Chapter 3 to review pending revocation of the certificate application;
- After CMCA revokes the customer certificate, the issuing authority will inform the customer of the revocation and the reason for the revocation;
- The revoked customer certificate enters CRL within 24 hours or is issued directly to CRL.

依赖方和其他第三方, 有责任和义务向 CMCA 报告可疑的私钥泄漏、证书误用或其他类型的欺诈、折衷、误用、不当行为或与证书相关的任何其他事项。

Dependent parties and other third parties have the responsibility and obligation to report to CMCA suspicious private key leaks, certificate misuse or other types of fraud, compromise, misuse, misconduct or any other matters relating to certificates.

## **4.9.4 吊销请求宽限期 Revocation Request Grace Period**

RA 强制吊销可以给予 24 小时的宽限期。订户申请吊销时，RA 应在收到吊销请求 24 小时内吊销证书，没有宽限期。

RA compulsory revocation can be given 24 hours of grace period. When the terminal customers apply for revocation, RA shall revoke the certificate within 24 hours after receiving the revocation request with no grace period.

## **4.9.5 电子认证服务机构处理吊销请求的时限 Time within which CA Must Process the Revocation Request**

在主动吊销的情形下，CMCA 收到吊销请求并审核完成后，24 小时内吊销证书。

If the revocation is active, CMCA shall revoke the certificate within 24 hours after receiving the revocation request and completing the audit.

在被动吊销的情形下，订户在收到吊销通知后的 3 个工作日内可向 CMCA 提出申辩理由，CMCA 将会对申辩理由进行评估，若确认其理由正当则不予以吊销；若订户在 3 个工作日内未回复或回复无异议，则 CMCA 将于 24 小时内予以吊销。

Under passive revocation, the subscriber may submit a defence to CMCA within 3 working days after receiving the notice of revocation, CMCA will evaluate the defence and not revoke it if the reason is confirmed to be valid; if the subscriber fails to reply or reply within 3 working days without objection, CMCA will be revoked within 24 hours.

a. 应向订户、依赖方、应用软件供应商和其他第三方提供明确指示，以报告可疑的私钥泄漏、证书误用或其他类型的欺诈、折衷、误用、不当行为或与证书相关的任何其他问题事项。

b. 应识别高优先级证书问题报告。

c.在收到证书问题报告后 24 小时内，应调查与证书问题报告有关的事实和情况，并向订户和提交证书问题报告的实体提供初步调查报告。

a. Clear instructions should be provided to subscribers, relying parties, application vendors and other third parties to report suspected private key leaks, certificate misuse or other types of fraud, compromise, misuse, misconduct or any other issue related to the certificate.

b. High priority certificate problem reports should be identified.

c. Within 24 hours of receiving the certificate issue report, the facts and circumstances related to the certificate issue report shall be investigated, and a preliminary investigation report shall be provided to the subscribers and the entities that submit the certificate issue report.

在审查事实和情况后，应与订户和报告证书问题报告或其他与撤销有关通知的任何实体一起确定是否要撤销证书，如果要撤销证书，应确定撤销证书的日期。从收到证书问题报告或与撤销有关的通知到公布撤销的时间不得超过第 4.9.1.1 条规定的期限。选择撤销日期时应考虑下列原则：

- 所指称问题的性质(范围、背景、严重程度、程度、损害的风险)；
- 撤销的后果(对订阅者和依赖方的直接和间接影响)；
- 收到的有关特定证书或用户的证书问题报告的数量；
- 提出投诉的实体(例如，执法人员对网站从事非法活动的投诉应比消费者对其未收到所订购商品的投诉更有分量)；
- 相关法律法规。

d.应保持连续的 24x7 能力，对高优先级证书问题报告进行内部响应，并在适当情况下，将此类投诉提交给执法部门，并/或撤销此类投诉所涉及的证书。

After reviewing the facts and circumstances, a determination should be made with the subscriber and with any other entity reporting on the issue of certificates or related notices of revocation as to whether to revoke the certificate and, if so, the date of revocation. The period from the receipt of a report on the issue of certificates or notice relating to revocation to the publication of the revocation shall not exceed the period specified in Article

4.9.1.1. The following principles should be taken into account when selecting the date of revocation:

- The nature of the problem alleged (scope, context, severity, extent, risk of damage);

- Consequences of revocation (direct and indirect effects on subscribers and relying parties);

- Number of reports received on specific certificates or user-specific certificates;

- The submitting entity (e.g. law enforcement officials should have more weight in complaints about illegal activities on the website than consumers do about the goods they have not received);

- Relevant laws and regulations.

d. A continuous 24 x7 capacity should be maintained to respond internally to high-priority certificate issues reports and, where appropriate, submit such complaints to law enforcement and/or revoke the certificates involved in such complaints.

## **4.9.6 依赖方检查证书吊销的要求 Revocation Checking Requirement for Relying Parties**

依赖方在信任此证书前应检查证书的有效性，确认证书未被吊销。

The relying party shall check the validity of the certificate before trusting the certificate and confirm that the certificate has not been revoked.

## **4.9.7 CRL 发布频率 CRL issuance frequency**

订户证书的 CRL 在 24 小时内更新; 订户有特殊要求的, 将根据订户的需求, 适当更新 CRL 发布的频率。CMCA 签发的 CRL 信息, 根据需要, 也可以人工方式实时发布。



CMCA shall publish the revoked certificate within 24 hours through the certificate blacklist library CRL; If the subscriber has special requirements, the frequency of CRL release will be updated according to the subscriber's needs. CMCA issued CRL information, according to the need, can also be manually released in real time.

中级 CA 证书的 CRL 发布频率:CMCA 每 12 个月更新和补发 CRLs 一次(i), 在撤销中级 CA 证书后的 24 小时内更新和补发 CRLs 一次(ii).

CMCA 确保在证书有效期结束前, 证书的吊销状态可以在 CRL 中被查询。

The CRL release frequency of the subordinate CA certificate:

CMCA update and reissue CRLs every 12 months (i) and within 24 hours after revocation of subordinate CA certificate (ii).

CMCA ensures that the revocation status of the certificate can be queried in the CRL before the certificate validity period expires.

#### **4.9.8 CRL 发布的最大滞后时间 Maximum Latency for CRLs**

CMCA 的 CRL 发布的最大滞后时间为 24 小时。

The maximum lag time for CMCA CRL release is 24 hours.

#### **4.9.9 在线状态查询的可用性 On-line Revocation/Status Checking Availability**

OCSP 服务网址:

<http://mpus.cmca.net:8083/ocsp>

<https://mpus.cmca.net:8080/ocsp>

CMCA 提供 OCSP 查询服务, 服务 7\*24 小时可用。CMCA 的 OCSP 响应符合 RFC6960 标准。CMCA 确保在证书有效期结束前, 证书的吊销状态可以在 OCSP 中被查询。

信赖方是否进行在线状态查询完全取决于信赖方的安全要求。对于安全保障

要求高并且完全依赖证书进行身份鉴别与授权的应用，信赖方在信赖一个证书前可通过证书状态在线查询系统检查该证书的状态。

OCSP Services Website:

<http://mpus.cmca.net:8083/ocsp>

<https://mpus.cmca.net:8080/ocsp>

CMCA provide OCSP query service, service 7/24 hours available. CMCA OCSP response meets RFC6960 standards. CMCA ensure that the revocation status of the certificate can be queried in the OCSP before the expiry date of the certificate.

Whether the trust party carries out online status query depends entirely on the trust party's security requirements. For the application of high security requirement and complete dependence on certificate for identity identification and authorization, the trust party can check the status of the certificate through the certificate status online query system before trusting a certificate.

客户通过 http 协议访问 CMCA 的 OCSP 服务，CMCA 会对查询请求进行检查，检查的内容包括：

- ◆验证是否强制请求签名
- ◆用 CA 证书验证签名是否通过
- ◆验证证书是否生效或者已经过期
- ◆验证证书颁发者是否在信任证书列表内

The client visits CMCA OCSP services through a http protocol and checks the query request, including:

- ◆ verify that signature is mandatory
- ◆ verify the signature with CA certificate
- ◆ verification certificate is valid or expired
- ◆ whether the certificate issuer is in the trust certificate list

OCSP 响应包含下表所属的基本域和内容

域	值或者值的限制
状态	响应状态，包括成功、请求格式错误、内部错误、稍候重试、请求没有签名和请求签名证书无授权，当状态为成功时必须包

	括以下各项
版本	V1
签名算法签发	OCSP 的算法。Sha1RSA 算法签名
颁发者	签发 OCSP 的实体。签发者公钥的数据摘要值和证书甄别名
产生时间	OCSP 响应的产生时间
证书状态列表	包括请求中所查询的证书状态列表。每个证书状态包括证书标识、证书状态以及证书废止信息
证书标识	包括数据摘要算法、证书甄别名数据摘要值、证书公钥数据摘要值和证书序列号。
证书状态	证书的最新状态，包括有效、吊销和未知。
证书废止信息	当返回证书状态为废止时包含废止时间和废止原因

OCSP 的扩展信息与RFC6960一致。

OCSP response contains the basic domains and contents of the following table

field	Limit of value or value
Status	Response status, including success, request format error, internal error, retry later, Request without signature and request for signature certificate without authorization, When the state is successful, it must be wrapped Include the following
version	V1
Signing algorithm	OCSP algorithm. Sha1RSA algorithm signature
Presenter	The entity issuing the OCSP .Data summary value and certificate screening name of the issuer public key
Generation time	OCSP response
Certificate Status List	includes the list of certificate status queried in the request. Each certificate status includes certificate identification, certificate status and revocation information
Certificate ID	Including data summary algorithm, certificate screening name data summary value, certificate public key data summary value and certificate serial number.
Certificate status	The latest status of the certificate, including validity, revocation and unknown.
Certificate Abolition Information	When returning to the status of the certificate of revocation contains the time of revocation and the reasons for its revocation

OCSP extended information is consistent with RFC6960.

## **4.9.10 在线状态查询要求 On-line Revocation Checking Requirements**

CMCA 能够提供在线状态查询，证书订户和依赖方可通过 OCSP 服务进行证书状态的实时查询。

CMCA can provide online status query so that certificate subscribers and dependent parties can perform nowcast query of certificate status through OCSP service.

OCSP 所有返回的信息均已电子签名，并包括所有所需的数据。

All information returned by OCSP has been electronically signed and shall cover all required data.

中国移动CMCA提供的OCSP服务支持GET方式。

OCSP service provided by CMCA supports GET method.

对于中级证书及订户证书而言 CMCA 的 OCSP 信息的更新频率为 10 小时；OCSP 服务响应最大时间为 10 秒；OCSP 服务响应信息最大有效期为 10 小时。

For subordinate ca certificates and subscriber certificates, update frequency of CMCA's OCSP information is 10 hours; maximum response time of OCSP service is 10 seconds; maximum validity period of OCSP service response information is 10 hours.

## **4.9.11 吊销信息的其他发布形式 Other Forms of Revocation Advertisements Available**

证书吊销信息可以通过CRL或者OCSP服务获得。订户可通过证书扩展域中的CRL地址获得CRL信息。

Certificate revocation information can be obtained through the CRL or OCSP service. Subscribers can obtain CRL information from the CRL address in the certificate extension domain.

## **4.9.12 密钥损害的特别要求 Special Requirements Related to Key Compromise**

无论是订户还是 CMCA，发现或者怀疑密钥安全被损害时，应该立即吊销证书，并发布到 CRL。吊销后如需继续申请证书，按照证书申请流程进行操作。Whether a subscriber or CMCA, discovers or suspects that key security is compromised, the certificate should be revoked immediately and posted to CRL. If you need to continue to apply for a certificate after the revocation, operate according to the certificate application process.

## **4.9.13 证书挂起的情形 Circumstances for Suspension**

CMCA 不提供全球信任证书的证书挂起服务。  
CMCA does not provide a certificate hang service for global trust certificates.

## **4.9.14 请求证书挂起的实体 Who Can Request Suspension**

CMCA 不提供全球信任证书的证书挂起服务。  
CMCA does not provide a certificate hang service for global trust certificates.

## **4.9.15 挂起请求的流程 Procedure for Suspension Request**

CMCA 不提供全球信任证书的证书挂起服务。  
CMCA does not provide a certificate hang service for global trust certificates.

## **4.9.16 挂起的期限限制 Limits on Suspension Period**

CMCA 不提供全球信任证书的证书挂起服务。  
CMCA does not provide a certificate hang service for global trust certificates.

## 4.10 证书状态服务 Certificate status services

### 4.10.1 操作特性 Operational characteristic

证书状态可以通过CMCA提供的OCSP 以及CRL 获取（在证书到期之前）上述方式的证书状态服务应该对查询请求有合理的响应时间和并发处理能力。证书吊销信息的保留期限至证书有效期后。

The certificate status service which can be obtained by the OCSP provided by CMCA and the certificate status service (before the certificate expires) should have reasonable response time and concurrent processing ability to the query request. The retention period of certificate revocation information is after the validity of the certificate.

### 4.10.2 服务可用性 Service availability

中国移动CMCA提供7\*24小时不间断OCSP（在线证书状态查询）服务，在网络允许的情况下，订户能够实时获得证书状态查询服务，响应时间小于10秒。

The CMCA provides 724 hours uninterrupted OCSP (online certificate status protocol) service. When the network allows, the subscriber can obtain the certificate status query service in real time, and the response time is less than 10 seconds.

### 4.10.3 可选特征 Optional Features

无。

None.

## 4.11 订购结束 End Of Subscription

订购结束是指证书订户终止与中国移动 CMCA 的服务，包含以下情况：

1. 当证书到期时，证书订户不再延长证书使用期或者不再重新申请证书时，服务终止自动产生。
2. 在证书的有效期内，由于证书订户的原因而单方面要求终止证书服务，如用户申请吊销该证书。中国移动 CMCA 将根据证书订户的要求吊销证书。证书订户与中国移动 CMCA 的服务终止。

End of order means that the certificate subscriber terminates the service CMCA, including the following:

1. When the certificate expires, the certificate subscriber does not extend the certificate service period or reapply for the certificate, the service termination automatically arises.
2. During the validity period of the certificate, the unilaterally requests the termination of the certificate service due to the reason of the certificate subscriber, such as the user applying for the revocation of the certificate. CMCA will revoke the certificate according to the requirements of the certificate subscriber. Certificate Subscriber and CMCA Service Termination.

## 4.12 密钥托管与恢复 Key Escrow And Recovery

### 4.12.1 密钥恢复的策略与行为 Key escrow and recovery policy and practices

不适用。CMCA不托管任何SSL证书订户的私钥，因此也不提供密钥恢复服务。

Not applicable. CMCA does not host the private key of any SSL certificate subscriber and therefore does not provide a key recovery service.



#### **4.12.2 会话密钥的封装与恢复的策略与行为 Session key encapsulation and recovery policy and practices**

不适用。

Not applicable.

### **5. 认证机构设施、管理和操作安全控制 Facility, management and operational security controls of certification body**

本章描述物理环境、操作过程和人员的安全控制。

This chapter describe physical environment, operation process and personnel security controls.

#### **5.1 物理安全控制 Physical security controls**

##### **5.1.1 物理场地位置与建筑 Physical location and architecture**

CMCA的运营机房位于广东省广州市天河区高唐路333号中国移动南方基地数据中心B座5楼，进入机房须经过三道审核，机房电磁屏蔽效能满足GJBz20219-94标准“C”级要求。机房具备抗震、防火、防水、恒湿温控、独立供电、备用发电、门禁控制、视频监控等功能，可保证认证服务的连续性和可靠性。

The operating computer room of CMCA is located on the 5th floor of B data Center of China Mobile South Base, 333 Gaotang Road, Tianhe District, Guangzhou City, Guangdong Province. The electromagnetic shielding efficiency of the computer room meets the "C" level requirement" of the GJBz20219-94 standard. The machine room has the functions of earthquake

resistance, fire prevention, waterproof, constant humidity and temperature control, independent power supply, standby power generation, access control, video surveillance and so on, which can ensure the continuity and reliability of the certification service.

### 5.1.2 物理访问 Physical access

外来人员进入CMCA机房，需经过中国移动南方基地、CMCA两道审核，进入CMCA机房需要有CMCA工作人员陪同进入。

操作人员进入CMCA综合机房，须经过指纹认证加门禁授权卡身份认证，并有24小时视频监控设备进行监控。

操作人员进入CA核心区需要双人指纹加门禁卡认证，其他区域为单人指纹加门禁卡认证，并且所有门禁的进出信息都会在监控室的安保系统中记录。

Non-CMCA staff entering CMCA machine room need to go through the audit of China Mobile South Base and CMCA Road. CMCA staff are required to enter CMCA machine room.

If the operators enter CMCA comprehensive machine room, they must pass the fingerprint authentication and access control authorization card identity authentication, and have the 24 - hour video monitoring equipment for monitoring.

Operators entering the CA core area require dual fingerprint and access card authentication, while other areas require single fingerprint and access card authentication. All access information will be recorded in the security system of the monitoring room.

### 5.1.3 电力与空调 Power and air conditioning

- 为了确保计算机设备安全可靠连续运行，本工程引入三路电源，两路由大楼总配电室 UPS 接至屏蔽机房配电柜再分别供给各计算机设备，门禁监控等使用；一路市电工机房照明和专用空调使用。全部电气系统均为

三相五线制。本工程所装配的动力配电柜采用常州正泰 XL-21 产品。大量的动力布线按安装规范均穿金属管槽保护。安全可靠，经检验整个系统运行正常。

- In order to ensure safe, reliable and continuous operation of computer equipment, the engineering has introduced three power supplies, of which two power supplies are connected from total distribution room UPS of the building to shielding room power distribution cabinet, and then supply to each computer equipment and access monitoring, etc. respectively for usage; One power supply is used for electric supply machine room and special-purpose air conditioning. All electrical systems are three-phase five-wire systems. Power distribution cabinet assembled in the engineering shall adopt Changzhou CHINT XL-21 Products. A large number of power wiring shall pass through metal tube seat for protection in accordance with installation specification. It is security and reliable, and the overall system can run normally after inspection.
- 机房采用两台机房专用空调机，活动地板下送风，顶部侧回风，温度控制范围在 18℃~28℃，湿度控制范围在 30%~75%RH，能够满足机房高热湿比、长时间运行、高可靠性、安全性的要求。经检测达到设计要求。
- The machine room adopts two special-purpose air conditioning machines for machine room, which supplies air below raised floor and returns air from top side. The temperature range is controlled within 18℃~28℃ and humidity range is controlled within 30%~75%RH, which can meet the requirements of high heat humidity ratio, long time operation, high reliability and security in the machine room. Reach the design requirements after detection.

### 5.1.4 水患防治 Water protection

中国移动 CMCA 在机房建设时已采取相应措施，防止水侵蚀，充分保障系统安全。

CMCA has taken corresponding measures during the construction of machine room, to prevent water erosion and fully ensure the system security.

### 5.1.5 火灾防护 Fire prevention and protection

中国移动 CMCA 通过与专业防火部门协调，实施消防灭火等应急响应措施，避免火灾的威胁，充分保障系统安全。敏感区（三层）、安全区域（四、五层），其建筑物的耐火等级按照 GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级。

CMCA can implement the corresponding emergency response measures such as fire extinguishment, etc. through the coordination with Specialized Fire Protection Department, to avoid the threatening of fire disaster and fully ensure the system security. Sensitive area (Floor 3), security area (Floor 4 and 5), fire resistance rating of its building shall be performed in accordance with secondary fire resistance rating stipulated in GBJ45 Fire Protection Design of Tall Buildings.

### 5.1.6 介质存储 Media storage

CMCA 保管的介质是指光盘、硬盘、软盘、U 盘、存储卡、磁带等，由专人管理，存储介质必须得到安全可靠的保护，避免诸如温度、湿度和磁力等环境变化可能产生的危害和破坏。

Medias refer to storage media such as light disc, hard disc, floppy disc, U-disk, memory card and tape, etc., and media storage must get safe and reliable protection, to avoid the possible harm and destruction caused due to environmental change such as temperature, humidity and magnetic force, etc.

### 5.1.7 废物处理 Waste disposal

当 CA 机构保存的相关数据已不再需要或存档的期限已满时，中国移动 CMCA 将完全销毁这些数据。所有处理行为将记录在案，以供审查的需要，销毁行为遵守我国的法律。

敏感的文件资料（包括纸介质、光盘或软盘废物等）抛弃前要进行粉碎处理；对于存储或传输信息的介质，在抛弃前要做不可读取处理；涉密介质在抛弃前要根据生产商的指导做归零处理。加密机等重要设备废弃根据加密机管理办法销毁。When relevant data saved by CA institution is no longer needed or filing period has expired, CMCA will destroy these data completely. All disposal behavior shall be recorded for the review, and the destruction behavior shall conform to our country's law.

Sensitive documents (including paper media, CD or floppy disk waste, etc.) should be crushed before abandonment; for media that store or transmit information, it should be unreadable before abandonment; and confidential media should be treated according to the manufacturer's guidance before abandonment. Encryption machine and other important equipment abandoned according to encryption machine management methods to destroy.

### 5.1.8 异地备份 Off-site backup

CMCA建立了异地备份机制。设置异地备份机房，并配置相关设备，当CA系统出现灾难时，可以通过异地备份中心的备份数据恢复CA系统。

CMCA established a remote backup mechanism. Set up remote backup computer room and configure related equipment. When the CA system is in disaster, the CA system can be restored through the backup data of the remote backup center.

## 5.1.9 时间戳服务器证书物理控制 Physical control of timestamp server certificates

CMCA独立控制并运营时间戳服务器，其密钥保存在加密机中，CMCA确保时间戳服务使用的私钥被保存在符合FIPS-140-2级别或者更高级别的加密机中，CMCA时间戳服务提供的时间源为北斗时，溯源自中国科学院国家授时中心协调时间时UTC。

CMCA independently controls and operates the time stamp server, whose key is stored in the crypt machine, CMCA ensures that the private key used by the time stamp service is saved in the FIPS-140-2 level or higher, the time source provided by CMCA time stamp service is Beidou, UTC. from the National Time Grant Coordination Center of Chinese Academy of Sciences.

## 5.2 流程安全控制 Process security controls

### 5.2.1 可信角色 Trusted roles

中国移动 CMCA 明确规定了以下关键职能职位为可信角色：

- 1) 系统管理人员：指对数字证书系统进行日常管理、运维、监控等日常处理的人员，并可根据需要签发服务器证书和系统角色证书的人员。
- 2) 安全管理人员：安全管理人员对 CA 中心物理安全和系统安全负责，负责拟定安全管理制度和操作流程，以及日常安全工作的执行督导管理。
- 3) 密钥管理人员：密钥管理员负责管理密钥设施，对密钥进行操作，如密钥生成、备份、恢复、销毁等操作。
- 4) 证书业务管理员：对业务操作员进行管理。
- 5) 核心技术人员：指 CA 系统的专业开发、测试人员或证书服务技术支持专业人员。

CMCA clearly stipulated that the following key functional positions are trusted roles:

- 1) System management personnel: refers to personnel who carry out daily

management, operation, monitoring, and other daily processing of digital certificate systems, and can issue server certificates and system role certificates as needed.

2) Security management personnel: Security management personnel are responsible for the physical security and system security of the CA center, responsible for formulating security management systems and operational procedures, as well as supervising and managing the execution of daily security work.

3) Key management personnel: Key administrators are responsible for managing key facilities and operating keys, such as key generation, backup, recovery, destruction, etc.

4) Certificate business administrator: manages business operators.

5) Core technical personnel: Refers to professional developers, testers, or certificate service technical support professionals of the CA system.

### **5.2.2 每项任务需要的人数 Number of people required per task**

CMCA 对与运行和操作相关的职能有明确的分工，对于敏感操作，贯彻互相牵制的安全机制。

对于密钥和加密设备的操作，需要 5 个可信人员中的 3 个共同完成；

对于证书审核、签发至少需要 2 个证书业务管理员。

CMCA have a clear division of functions related to running and operation, and carry out the security mechanism of mutual containment for sensitive operations.

For the operation of keys and encryption devices, 3 out of 5 trusted personnel are required to complete it together;

For certificate review and issuance, at least 2 certificate business administrators are required.



### 5.2.3 每个角色的识别与鉴别 Identification and identification of each role

所有中国移动 CMCA 的在职人员的识别与鉴别都是通过各种安全令牌标示的，所有人员必须通过认证后，根据作业性质和职位权限的需要，发放系统操作卡、门禁卡、登录密码、操作证书、作业帐号等安全令牌。对于使用安全令牌的员工，中国移动 CMCA 系统将独立完整地记录其所有的操作行为。

All the on-the-job personnel of CMCA are identified and authenticated through various security tokens. All personnel must pass the authentication and issue security tokens such as system operation card, access card, login password, operation certificate, job account number and so on according to the nature of the operation and the need of the position authority. For employees who use security tokens, the CMCA system will record all its operations independently and completely.

所有中国移动 CMCA 在职人员必须确保：

- 发放的安全令牌只直接属于个人或组织所有
- 发放的安全令牌不允许共享

中国移动 CMCA 的系统 and 程序通过识别不同的令牌，对操作者进行权限控制。

All mobile CMCA employees must ensure that:

- Security tokens issued belong directly to individuals or organizations
- Security tokens issued do not allow sharing

CMCA system and program by identifying different tokens to the operator authority control.

### 5.2.4 职责分割原则 Responsibility division principle

中国移动 CMCA 的运营员工和负责 CA 中心系统设计、开发、维护的员工承担不同的职责，双方的岗位互相分离。此外，证书发放关键环节中，信息录入与

审核签发人员应由不同的人员担任。

Operating employees and employees who take charge of design, development and maintenance of CMCA system of CMCA shall assume different responsibilities, and post of each party is separated with each other. Besides, in the key link of certificate issuance, different persons serve as the information entry personnel and the review signer.

当 CA 中心员工被怀疑，或者已进行了未授权的操作，例如未经授权滥用权利或超出权限使用 CA 中心系统或进行越权操作，CA 中心在得到信息后立即中止该员工进入 CA 中心证书服务体系。根据情节严重程度，实施包括提交司法机关处理等措施。

一旦发现上述情况，CA 中心立即作废或终止该人员的工作。

When a CMCA employee is suspected or has performed unauthorized operations, such as unauthorized abuse of rights or using the CMCA system beyond authority or performing unauthorized operations, the CMCA immediately suspends the employee's access to the CMCA certificate service system after receiving the information. According to the seriousness of the circumstances, measures including submitting to judicial authorities for handling are implemented.

Once the above condition is found, CMCA immediately cancels or terminates the work of such personnel.

## 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

人事管理制度用以 CA 中心确定其人员和岗位设置，保障 CA 中心的安全运营。人事管理制度包括人员的可信度审查、岗位设置等。

The personnel management system confirms the personnel and post setting with CMCA to ensure the safe operation of CA center. Personnel management system includes the credibility review of personnel, post setting, etc.

中国移动 CMCA 对员工在资格、经历方面有着严格的要求，而且所聘任的员工要求没有法律方面的过失，具备高可信度。

CMCA has strict requirement to staff in qualification and experience, and the staff appointed shall have no law fault with high reliability.

CA 中心应制定可信人员策略并据此进行人员的可信度审查和聘用。可信人员必须接受并通过广泛的背景调查，才能证明他们有能力进行那些关键操作所必须的信任级别。

CMCA shall formulate the trusted personnel strategy and conduct the reliability review and employment of personnel based on this. The trusted personnel shall receive and conduct wide background survey to certify that they have the ability to conduct the key operation with necessary trust level.

CA 中心对人员的教育水平、从业经历、信用情况等方面进行调查，来评估人员的可信度。进行可信人员背景调查必须遵循国家的有关法律、法规和政策。对任何参与证书管理过程的人员，无论是作为 CA 的雇员、代理或独立合约人，CA 中心都应核实该人员的身份和可信度。

CMCA should investigate the educational level, working experience and credit standing of employees to assess their credibility. Background investigation of credible personnel must be consistent with relevant laws, regulations and policies of the country.

For people participating in the certificate management process as an employee, agent or independent contractor of the CA, the CMCA shall verify their identity and credibility.

### **5.3.2 背景审查程序 Background review procedures**

CA 中心员工的录取经过严格的审查，根据岗位需要增加相应可信任的员工。

员工需要有 2 个月的考察期，根据考察的结果安排相应的工作或者辞退并且剥离岗位。CA 中心根据需要对员工进行职责、岗位、技术、政策、法律、安全等方面的培训。

CMCA staff shall be enrolled with strict review, and the corresponding trusty staff is added according to the post need. The staff shall experience 2-month survey period, and corresponding work is arranged, or the staff is refused and leave the post according to the survey result. CMCA conducts the training in responsibility, post, technology, policy, laws, safety and other aspects according to the demand.

CA 中心会对其关键的 CA 职员进行严格的背景调查。受理点操作员的审查可以参照 CA 中心对可信任员工的考察方式。受理点责任单位可以在此基础上，增加考察和培训条款，但不得违背 CA 中心证书受理的规程和 CA 中心证书业务声明。

CMCA would conduct the strict background survey to its key staff. The operator at the LRA could be reviewed by reference of the survey method made by the CMCA to the trusted staff. The responsible unit at the LRA could add survey and training terms on such basis, but shall not violate the certificate acceptance rule of CMCA and the certificate business statement of CA center.

CA 中心确立流程管理规则，据此 CA 员工受到合同和章程的约束，不许泄露 CA 中心证书服务体系的敏感信息。所有的员工与 CA 中心签定保密协议。

CMCA confirms the process management rules, and CA staff shall not give away the sensitive information of certificate service system in CMCA due to constraint from contract and Articles of Association. All staff shall sign the confidentiality agreement with CA center.

### 5.3.3 培训要求 Training requirements

CA 中心对 CA 中心员工进行以下内容的综合性培训：

◇ 公司统一新员工培训

- ✧ CA 中心技术系统介绍
- ✧ CA 中心运营体系介绍
- ✧ 岗位职责及业务流程
- ✧ 相关法律、管理办法等

CMCA conducts the comprehensive training of the following contents to its staff:

- ✧ Uniform new staff training of company
- ✧ Introduction to technical system of CMCA
- ✧ Introduction to operation system of CA center
- ✧ Post responsibility and business process
- ✧ Relevant laws and management method, etc.

中国移动 CMCA 对录用人员按照其岗位和角色安排培训。培训内容有：PKI 的相关知识、岗位职责、内部规章制度、认证系统软件、相关应用软件、操作系统与网络、ISO9000 质量控制体系、ISO27001 信息安全管理体系统、CP/CPS 等。

CMCA arranges training for recruiters according to their positions and roles. The training contents include: PKI related knowledge, job responsibilities, internal rules and regulations, certification system software, related application software, operating system and network, ISO9000 quality control system, ISO27001 information security management system, CP/CPS and so on.

处理证书业务相关的员工必须接受下列培训：

- 1) 向所有负责信息身份验证的职员（“验证专家”）提供技能培训。培训内容包括基础 PKI 知识、审核与验证制度和流程、对验证过程的主要威胁因素（如，网络钓鱼及其他社会工程学策略）；
- 2) 保留人员培训记录，并且确保“验证专家”能够胜任身份信息验证工作的 技术要求；
- 3) 验证专家必须按其不同的技术水平等级被授予不同的签发证书权限，技术水平分级标准应与培训内容以及业绩考核标准一致；
- 4) 确保为验证专家分配签发证书权限前，不同技术水平等级的验证专家都具有足够的胜任能力；

5) 要求所有的验证专家通过关于证书标准中身份验证要求的 CA 内部考试。

Employees involved in the certification business must receive the following training:

- 1) Provide skills training to all staff responsible for information authentication ("Verification experts"). The training includes basic PKI knowledge , audit and verification systems and processes, major threat factors to the verification process (For example, phishing and other social engineering strategies) ;
- 2) Maintain personnel training records and ensure that "certification experts" are up to the technical requirements of authentication;
- 3) Validation experts must be granted different certification authority according to their different technical level, and the technical level classification standard should be consistent with the training content and performance appraisal standard;
- 4) Ensure that certification experts at different levels of technology have sufficient competence before assigning certification authority to certification experts;
- 5) All certification experts are required to pass CA internal examinations on authentication requirements in certification standards.

### **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 CMCA 组织的培训一次。

根据行业法律法规、CA 中心策略调整、系统更新等情况，CA 中心可能要求员工进行继续培训，以适应新的变化。

中国移动 CMCA 所有受信任角色的人员应保持与 CA 的培训和绩效计划一致的技能水平。

For those who act as credible or other important roles, they are trained at least once a year by CMCA organizations.

Depending on industry laws and regulations, CMCA strategy adjustment, system updates, etc., the CMCA may require employees to continue their training to accommodate new changes.

Personnel of all trusted roles in CMCA should maintain skills consistent with CA's training and performance plan.

### **5.3.5 工作岗位轮换周期和顺序 Job rotation cycle and sequence**

CA 中心运营服务员工和负责 CA 中心开发、维护的员工承担不同的职责，双方的岗位互相分离，即开发员工和运营员工分离的原则。

CMCA 根据具体工作情况安排并制定员工工作岗位的轮换周期与顺序。

The CMCA Operations Service staff and those responsible for the development and maintenance of the CMCA assume different responsibilities, with their positions separated from each other, namely the principle of separation between development and operating employees.

CMCA according to the specific work situation to arrange and formulate the employee job rotation cycle and order.

### **5.3.6 未授权行为的处罚 Sanctions for unauthorized actions**

当 CA 中心员工被怀疑，或者已进行了未授权的操作，例如未经授权滥用权利或超出权限使用 CA 中心系统或进行越权操作，CA 中心在得到信息后立即中止该员工进入 CA 中心证书服务体系。根据情节严重程度，实施包括提交司法机关处理等措施。一旦发现上述情况，CA 中心立即作废或终止该人员的工作。

When the personnel in CMCA is doubted or operates without authorization, for



example, the right is abused without authorization or the CMCA system is used beyond the permission or the operation is conducted beyond the power, CMCA shall immediately suspend the staff entering the CMCA certificate service system after knowing the information. Implement the measures, including submitting to judiciary authorities for handling according to the case seriousness. Once the above condition is found, CMCA immediately cancels or terminates the work of such personnel.

### **5.3.7 独立合约人的要求 Requirements of Independent Contractors**

CA 应验证授权的第三方人员在证书颁发过程中是否符合第 5.3.3 节的培训和技能要求，以及第 5.4.1 节的文件保存和事件记录要求。

对不属于 CMCA 内部的工作人员，但从事 CMCA 有关业务的人员等独立签约者，CMCA 的统一要求如下：

1. 人员档案进行备案管理；
2. 具有相关业务的工作经验；
3. 符合本 CP/CPS 5.3.3 的要求。

如承担可信角色则需与内部人员管理要求一致。

CA shall verify that authorized third party personnel comply with the training and skills requirements of Section 5.3.3, as well as the event recording requirements of Section 5.4.1 during the certificate issuance process.

For independent contractors who do not belong within CMCA, but those engaged in CMCA business, the unified requirements of CMCA are as follows:

1. Personnel files for record management;
2. Experience in related business;
3. Meet the requirements of this CP/CPS 5.3.3.

If you assume a credible role, you need to be consistent with internal

personnel management requirements.

### 5.3.8 提供给员工的文档 Supplements for personnel

文档包括《中国移动 CMCA 认证业务规则》、《中国移动 CMCA 运营管理规范》、《中国移动 CMCA 鉴证管理规范》、《中国移动 CMCA 服务管理规范》、相关法律、政策、制度说明以及相关管理制度等。

The document includes the Certification Business Rules of CMCA, Operations Management Specification of CMCA, Authentication Management Specification of CMCA, Service Management Specification of CMCA, the relevant laws, policies, system introduction and the relevant management system, etc.

## 5.4 审计日志程序 Audit log procedures

### 5.4.1 记录事件的类型 Types of event records

CMCA记录的日志信息包括但不限于以下类型：

- 1、CA密钥生命周期内的管理事件，包括密钥生成、备份、恢复、归档和销毁；
- 2、RA系统记录的证书订户身份信息；
- 3、证书生命周期中的各项操作，包括证书申请、证书密钥更新、证书吊销等事件；
- 4、系统、网络安全记录，包括入侵检测系统的记录、系统日常运行产生的日志文件、系统故障处理工单、系统变更工单等；
- 5、人员访问控制记录；

上述日志信息包括记录时间、序列号、记录的实体身份、日志种类等。

Log information logged by CMCA includes, but is not limited to, the following types:

- 1、Management event within CA key life cycle, including Key generation, backup, storage, recovery, archival and destruction;
- 2、Certificate subscriber identity information recorded by the RA system;

3、Actions in the certificate life cycle , including Certificate application, approval, renewal and revocation;

4、System and network security records, including records of intrusion detection system, log files generated by daily operation, system fault processing orders , system change list , etc;

5、Personnel access control records;

The above log information includes record time, serial number, recorded entity identity, log type, etc.

### 5.4.2 处理日志的周期 Frequency of processing log

CMCA 对上条中 1 类日志由密钥管理员收集并管理；2、3 类日志由数据库保存，并每天进行一次增量备份，每周进行一次全备份；4 类日志每天自动保存在备份设备上。5 类日志每季度进行一次审计。

CMCA the first class log in the above article is collected and managed by the key administrator; the 2 and 3 kinds of logs are saved by the database, and the incremental backup is carried out once a day, and the full backup is carried out once a week; the 4 kinds of logs are automatically saved on the backup device every day. Class 5 logs are audited quarterly.

### 5.4.3 审计日志的保存期限 Retention period for audit log

中国移动 CMCA 在数据库保存审查记录至少三个月，离线存档至少七年。  
CMCA shall preserve the review record in database for three months at least, and keep in the archives off line for 7 years at least.

#### 5.4.4 审计日志的保护 Protection of audit log

中国移动 CMCA 执行严格的访问控制管理，确保只有中国移动 CMCA 授权的人员才能接近这些审查记录。这些记录处于严格的保护状态，严格禁止访问、阅读、修改和删除等操作。

CMCA implements the strict visit control management to ensure only the personnel with the authorization of CMCA could access these review record. These records are in strict protection status, no visit, reading, amendment, deletion and other operations are allowed.

#### 5.4.5 审计日志备份程序 Back procedures of audit log

中国移动 CMCA 保证所有的审查记录和审查总结都按照中国移动 CMCA 备份标准和程序进行。根据记录的性质和要求，采用在线和离线的各种备份工具，有实时、每天、每周、每月和每年等各种形式的备份。

CMCA ensures all review records and review summary are conducted according to the backup standard and procedure of CMCA. Based on the record nature and requirement, various online and offline backup tools are adopted with the real-time, daily, weekly, monthly, yearly, and other various backup.

#### 5.4.6 审计收集系统 Audit collection system

应用程序、网络和操作系统等都会自动生成审计数据和记录信息。

Applications, networks, and operating systems will automatically generate audit data and record information.

### 5.4.7 对导致事件实体的处理 Processing to event-causing subject

中国移动 CMCA 对审查中发现的攻击现象将做详细记录，在法律许可的范围内追溯攻击者，并保留采取相应对策措施的权利，如：切断对攻击者已经开放的服务、递交司法部门处理等措施。

CMCA 有权决定是否对导致事件的实体进行通告。

CMCA should take a detailed record of the attacks found in the review, ascend the attackers within the law, and reserve the right to take appropriate countermeasures, such as: Cutting off the open service to attacker, submitting the judicial department for treatment, and other measures.

CMCA has the right to decide whether to notify the entity that caused the event.

### 5.4.8 脆弱性评估 Vulnerability assessments

CMCA 每年进行一次风险评估，内容如下：

- 1、识别可预见的内部和外部威胁，可能导致未经授权的访问、披露、误用、更改或破坏任何证书数据或证书管理过程；
- 2、评估这些威胁的可能性和潜在损害，同时考虑证书数据和证书管理过程的敏感性；和
- 3、评估 CA 为对付这些威胁而采取的政策、程序、信息系统、技术和其他安排的充分性。

CMCA conducts an annual risk assessment as follows:

- 1) Identify foreseeable internal and external threats that may lead to unauthorized access, disclosure , misuse , change or destruction of any certificate data or certificate management process ;
- 2) Assess the likelihood and potential harm of these threats, taking into account the sensitivity of certificate data and the certificate

management process; and

- 3) Assess the adequacy of the policies, procedures, information systems, technologies, and other arrangements taken by the CA to address these threats.

对在审查过程中发现的系统的脆弱性，中国移动 CMCA 的相关关键人员，包括审计管理员、安全管理员、系统超级管理员等，或者聘请专业的系统安全评估单位，共同进行相应的脆弱性评估，出具评估报告，并在 96 小时内对系统脆弱性进行修补。

For the system vulnerability found in the review process, the relevant key personnel of CMCA, including audit administrator, safety administrator, system super administrator or the employed professional system safety evaluation unit, jointly conduct the corresponding vulnerability evaluation, issue the evaluation report, and repair the system vulnerability within 96 hours.

对在审查过程中发现的物理安全、制度安全、人员安全等方面问题，要及时进行相应的处理和解决。

The problems in physical security, system security and personnel security found in the review process should be handled and solved accordingly.

## 5.5 记录归档 Records archival

### 5.5.1 归档记录的类型 Types of records archived

中国移动 CMCA 会对 CA 的数据库定期存档，间隔时间由中国移动 CMCA 自行决定，存档的内容包括中国移动 CMCA 发行的证书和 CRL、审查数据记录、证书申请审批资料等。（签名私钥由实体本身保存，有关私钥的责任由实体本身承担）。

CMCA would regularly file the CA database, and the internal time is voluntarily decided by CMCA, and the filing content includes the certificate and CRL released by CMCA, review data record, certificate application approval data,

etc. (The signature private key is saved by the entity, and the responsibility related to the private key is undertaken by the entity).

### **5.5.2 归档记录的保存期限 Retention period for archived records**

中国移动 CMCA 应保留所有与证书请求及其验证有关的文件，以及所有证书及其撤销，在基于该文件的任何证书失效后至少七年。

CMCA shall retain all documents relating to the certificate request and its verification, as well as all certificates and their revocation, at least seven years after the expiry of any certificate based on the document.

### **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，如物理场地安全管理，存档信息异地存储，也有密码技术的保证，如存储区域密码设置，存储柜钥匙权限设置。

只有经过授权的工作人员按照特定的安全方式才能接近它们。

中国移动 CMCA 保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力的破坏。

中国移动 CMCA 每年会验证存档信息的完整性。

The filing contents have both the physical security measures and password technology guarantee.

Only the working personnel with authorization could access them in the specific safety method.

Relevant archives should be protected from threat of adverse environment, such as destruction of temperature, humidity, and magnetic forces by CMCA.

CMCA would verify the integrity of filing information every year.

### **5.5.4 归档文件的备份 Backup of archived records**

所有存档文件的数据库除了保存在中国移动 CMCA 的主要存储库，还将在



异地保存其备份。

存档的数据库采取物理或逻辑隔离的方式，与外界不发生信息交互。

只有授权的工作人员才能在监督的情况下，对档案进行读取操作。

中国移动 CMCA 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。

All filing document databases are stored in the main storage library of CMCA, besides their backups would be kept in another place.

The filing database has no information interaction with the outside world in the method of physical separation or logic separation.

Only the authorized personnel could read the file under the supervision condition.

CMCA ensures no deletion, amendment and other operations to its files and backup are allowed in safety mechanism.

### **5.5.5 记录时间戳要求 Requirements for time-stamping of records**

所有存档内容都要加时间标识。

All archived content should be identified with time.

### **5.5.6 归档收集系统 Archives collection system**

中国移动 CMCA 中的档案收集系统由人工操作和自动操作两部分组成。

Document collection system in CMCA consists of manual operation and automatic operation.

### **5.5.7 获得和检验归档信息的程序 Procedures for obtaining and inspecting archived information**

由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，

需要对这两个拷贝进行比较。CMCA 每年会验证归档信息的完整性。

Two copies of the archived data are kept separately and are compared to ensure the accuracy of the archival information. CMCA verifies the integrity of the archived information each year.

## 5.6 电子认证服务机构密钥更替 Key replacement

### 5.6.1 密钥更替操作 Key replacement operation

在这里密钥更替是指当中国移动 CMCA 根证书到期而需要更换根密钥对时所采取的措施。有效期详见 6.3.2。

The key replacement refers to the measures taken when CMCA root certificate expires and needs to replace root key pair. Valid date is seen in 6.3.2.

在中国移动 CMCA 证书到期之前，中国移动 CMCA 将对根私钥进行更换。密钥转换程序在旧密钥对向新密钥对的转换起着过渡的作用。中国移动 CMCA 密钥转换采用以下方式：

- 一个上级 CA 将在其私钥到期时间小于下级 CA 的生命期之前停止签发新的下级 CA 证书（“停止签发日期”）。
- 产生新的密钥对，签发新的上级 CA 证书。
- 在“停止签发证书的日期”之后，对于批准的下级 CA 或最终客户证书请求，将采用新的 CA 密钥签发证书。

The CMCA will replace the root private key before the expiration of the CMCA certificate. The key conversion program plays a transition role in the conversion of the old key pair to the new key pair. CMCA Key Converter:

- A superior CA will stop issuing a new lower CA certificate (Stop Issue Date) before its private key expires less than the life of the lower CA.
- Generate new key pairs and issue new superior CA certificates.

- The certificate will be issued with a new CA key for the approved subordinate CA or final customer certificate request after the date of stopping issuing the certificate.

中国移动 CMCA 将继续使用旧的 CA 私钥签发的 CRL，直到由旧的 CA 私钥签发的证书到期为止。

CMCA shall continue to use CRL issued by the former CA private key until the certificate issued by the former CA private key expires.

### 5.6.2 密钥更替操作管理 Key replacement operation management

CMCA 建立严格的密钥更替的管理要求：

- 1、 密钥管理员提前提交密钥更替审批，经策略委员会批准后明确操作；
- 2、 密钥更替过程将全称进行记录、录像，并由第三方审计机构见证；
- 3、 密钥更替将提前 30 天通知相关方。

CMCA establish strict key turnover management requirements:

1. The key administrator shall submit key replacement approval in advance, and operation is granted with consent by the policy committee;
2. The key-replacement process will be recorded and recorded in full and witnessed by a third-party audit institution;
3. Key replacement will be notified 30 days in advance.

## 5.7 损害与灾难恢复 Damage and Disaster Recovery (DR)

CA 系统的灾难恢复，指的是为保证在发生灾害（水灾、风灾、地震等自然灾害，或电力中断、火灾、爆炸等结构型破坏以及人为失误、网络黑客攻击、病毒等操作问题）或战争等攻击而导致 CA 彻底损毁时，能够恢复 CA 的密钥和客户资料。

The Disaster Recovery (DR) of CA system refers to the key and customer data which could recover CA when the disaster (flood, wind disaster, earthquake and other natural disasters, or electricity interruption, fire hazard, explosion and other structural damage, and human error, network hacker attack, virus and other operation problems) or war and other attacks happen and CA is completely damaged.

通过在异地设立灾难备份中心可以实现灾难恢复，灾难备份中心存放了备份的私钥和客户数据。中国移动 CMCA 定期将系统备份服务器中的数据通过磁带备份，以人工方式送到异地容灾备份中心。

The DR could be achieved by setting up a disaster backup center at another place, and the disaster backup center stores the backup private key and customer data. CMCA regularly backups the data of the system backup server by magnetic tape, and sends it to the disaster backup center in another place by manpower.

当公钥基础设施（PKI）发生灾难性故障时，中国移动 CMCA 拥有恢复运营的能力。对于一般故障，CMCA 将在 2 小时内解决；对于紧急事件，CMCA 在 24 小时内解决；对于灾难性事件，在主运营场地出现灾难事故或不可抗力事故而不能正常运营时，CMCA 将在 48 小时内，利用备份数据和设备在数据备份中心恢复电子认证服务。

When the public key infrastructure (PKI) catastrophic failure, CMCA has the ability to resume operations. CMCA will solve the general failure within 2 hours; for emergencies, CMCA within 24 hours; for catastrophic events, in the event of a disaster or force majeure accident at the main operation site and cannot operate normally, CMCA will restore electronic authentication services in the data backup center using backup data and equipment within 48 hours.

CA 应具有事件响应计划和灾难恢复计划。

The CA should have event response plans and disaster recovery plans.

CA 应编制业务连续性和灾难恢复程序，用于在发生灾难、安全损害或业务失败时通知并合理保护应用程序软件供应商、订阅者和依赖方。

CA shall prepare business continuity and disaster recovery procedures to inform and reasonably protect application software suppliers, subscribers and dependencies in case of disaster, security damage or business failure.

CA 不需要公开披露其业务连续性计划，但应根据要求向 CA 的审计师提供其业务连续性计划和安全计划。

CA do not need to publicly disclose their business continuity plans, but should provide their business continuity plans and security plans to CA auditors as required.

CA 应每年对这些程序进行测试、审查和更新。

These procedures shall be tested, reviewed and updated annually.

业务连续性计划必须包含如下内容：

1. 启动计划的条件
2. 紧急程序
3. 回退过程
4. 恢复程序
5. 计划的维护计划
6. 认知和教育要求
7. 个人的责任
8. 恢复时间目标(RTO)
9. 定期测试应变计划
10. 关键业务流程中断或失败后，CA 计划及时维护或恢复 CA 的业务操作
11. 在灾难发生后的一段时间内，以及在恢复原基地或偏远地点的安全环境之前，尽可能保护其设施的程序。

The business continuity plan must include the following:

1. Conditions for starting a plan
2. emergency procedure
3. Retreat process
4. Recovery program

5. Planned maintenance Plan
6. Cognitive and educational requirements
7. Personal responsibility
8. Recovery time target (RTO)
9. Regular test of the strain plan
10. CA plan to maintain or resume CA operations in a timely manner after critical business processes are interrupted or failed
11. Procedures to protect their facilities as far as possible during the period following the disaster and before restoring a safe environment in the original base or remote location.

灾难恢复的具体工作包括：

- 制定灾难恢复计划；
- 数据的备份和存储；
- 辅助设备准备；
- 启动灾难恢复计划；
- 灾难恢复所需时间评估。

Specific disaster recovery efforts include:

- Development of disaster recovery plans;
- Backup and storage of data;
- Auxiliary equipment preparation;
- Start up the disaster recovery plan;
- Time assessment for disaster recovery.

灾难恢复计划实施：

1. 所有的口令经安全部门主管以及相关的安全管理员、政策审批部门变更。
2. 根据灾难的性质，部分或全部证书需要吊销或以后重新认证。
3. 如果目录无法使用或者目录有不纯的嫌疑，目录数据，加密证书和 CRL 需要进行恢复，一旦目录管理员从备份中恢复了目录，安全部门和政策审批部门、授权运营部门可从中国移动 CMCA 系统的目录服务器恢复中国移动 CMCA 数据。

Disaster Recovery Plan implementation:

- 1) All passwords are changed by the head of the security department and the relevant security administrator, policy approval department.
- 2) Depending on the nature of the disaster, some or all of the certificates need to be revoked or re-certified later.
- 3) Where the directory cannot be used or the directory is suspected of being impure, directory data, encryption certificates and CRL need to be restored. Once the directory administrator recovers the directory from the backup, the security department and the policy approval department, the authorized operation department can restore the CMCA data from the directory server of the CMCA system.

### **5.7.1 事故和损害处理程序 Processing procedure of accident and damage**

事故和损害处理流程为:

1. 保证现有的对外提供的所有设备能够正常提供服务，并且针对每个环节设置紧急预案。
2. 所有的 CA 应用服务都具备基本的监控。
3. 出现故障时，应以尽快正常对外提供服务为目标，记录故障现场，对于影响面大的故障，发现问题 5 分钟内不能快速解决问题的，应考虑启动紧急预案。
4. 严重影响对外服务的故障，应该及时上报主管领导。

The process is as follows::

- 1) Ensure all equipment provided outsides could normally provide service, and set the emergency plan aiming at each link.
- 2) All CA application services own basic monitoring.
- 3) When the fault occurs, record the fault site as soon as possible aiming at normally providing service outsides. For the fault with large influence area,



in case the problems couldn't be solved rapidly within 5 minutes after the problems are found, the emergency plan shall be started.

- 4) For the fault which severely influences the foreign service, promptly report to the competent leader.

### **5.7.2 计算资源、软件和/或数据的损坏 Damage of computing resource, software and/or data**

当计算资源、软件和/或数据受到破坏时，进行以下操作：

1. 恢复环境、CA 系统和备份数据并上线；
2. 为客户恢复证书，重新进行认证；
3. 尽快启动原系统。

When the computing resource, software and/or data is damaged, the following operations shall be conducted:

1. Recover the environment, CA system and backup data, and on line;
2. Conduct the certification again to recover the certificate for the customer;
3. Start the original system as early as possible.

### **5.7.3 实体私钥损害处理程序 Damage treatment procedure of entity private key**

对于实体证书私钥的损害，中国移动 CMCA 有如下处理要求和程序：

- 1) 当客户发现实体证书私钥损害时，必须立即停止使用其私钥，并立即访问中国移动 CMCA 或相应的注册机构的证书服务网站吊销其证书，或者立即通过电话、电子邮件的方式通知中国移动 CMCA 或注册机构吊销其证书。中国移动 CMCA 按 4.9 节发布证书吊销信息。
- 2) 当中国移动 CMCA 或注册机构发现证书订户的实体证书私钥受到损害

时，中国移动 CMCA 或注册机构将立即吊销证书，并通知证书订户，订户必须立即停止使用其私钥。中国移动 CMCA 按 4.9 节发布证书吊销信息。

- 3) 当中国移动 CMCA 的 CA 证书出现私钥损害时，中国移动 CMCA 将立即吊销该 CA 证书并及时通过广达的途径通知依赖方，然后生成新的 CA 密钥对、签发新的 CA 证书。

For the damage of entity certificate private key, CMCA has the following treatment requirements and procedures:

- 1) When finding the entity certificate private key is damaged, the customer shall immediately stop using the private key, and immediately visit the certificate services website of CMCA or the corresponding RA to revoke its certificates, or immediately notify CMCA or the RA to revoke his certificate by phone and e-mail. CMCA releases the revocation information of certificate according to 4.9.
- 2) When finding the entity certificate private key of certificate subscriber is damaged, CMCA or RA would immediately revoke the certificate, and notify the certificate subscriber, then the subscriber shall immediately stop using his private key. CMCA releases the revocation information of certificate according to 4.9.
- 3) When the private key of CA certificate of CMCA is damaged, CMCA would immediately revoke such CA certificate and promptly notify the relying party by wide approaches, then generate new CA key pair and sign new CA certificate.

#### **5.7.4 灾难后的业务连续性能力 Business continuity ability after disaster**

灾难发生后中国移动 CMCA 立即从备份系统或异地备份中心恢复系统和数

据，系统上线并对客户提供服务，保持业务持续性。

After the disaster happens, CMCA immediately recovers the system and data from the backup system or off-site backup center, then the system is online and provides the service for the customer to keep the business continuity.

## **5.8 电子认证服务机构或注册机构的业务终止 CA or RA termination**

### **5.8.1 CA 终止原因 Termination reason of CA**

CA 终止服务的原因可以分为密钥受损原因和非密钥受损原因。

The service termination reason of CA could be divided into key damage reason and non-key damage reason.

### **5.8.2 终止通知 Termination notice**

当中国移动 CMCA 打算终止经营时，会在终止经营前九十天向给中国移动 CMCA 受理点和证书订户书面通知，并在终止服务六十日前向国务院信息产业主管部门报告，按照相关法律法规规定的步骤进行操作。

In event CMCA intends to terminate its operations, it shall notify the acceptance point and certificate subscribers authorized by CMCA in writing 90 days prior to termination of operations, and shall report to the State Council's information industry department 60 days in advance. All procedures are in compliance with related laws and regulations.

### **5.8.3 终止归档 Termination filing**

中国移动 CMCA 会按照相关法律法规的规定来安排好档案和证书的存档工作。CMCA would arrange the storage of file and certificate according to the relevant law regulations.

## 5.8.4 终止措施 Termination measures

在 CA 中止期间，采用以下措施终止业务：

- 起草 CA 终止声明；
- 通知与 CA 相关的实体；
- 关闭从目录服务器；
- 证书注销；
- 处理存档文件记录；
- 停止认证中心的服务；
- 存档主目录服务器；
- 关闭主目录服务器；
- 管理中国移动 CMCA 系统管理员和中国移动 CMCA 安全管理员；
- 处理加密密钥；
- 处理和存储敏感文档；
- 清除 CA 主机硬件。

During the termination period of CA, the following measures are adopted to terminate the business.:

- Draw up the CA termination statement;
- Notify the entity related to CA;
- Close the secondary LDAP server;
- Certificate cancellation;
- Handle the filing document record;
- Stop the service of certification center;
- File the main LDAP server;
- Close the main LDAP server;
- Manage the system administrator and safety administrator of CMCA;
- Handle the encryption key;
- Handle and store the sensitive documents;

- Eliminate the host hardware of CA.

### 5.8.5 RA 的终止 Termination of RA

不涉及。

Not involved.

## 6. 认证系统技术安全控制 Technical safety control of certification system

### 6.1 密钥对的生成和安装 Generation and installation of key pair

由于密钥对是安全机制的关键，所以在 CP/CPS 中制定了相应的规定，确保密钥对的产生、传送、安装等具备保密性、完整性和不可否认性。

Since the key pair is the key of security mechanism, so the corresponding regulations are formulated in CP/CPS to ensure that the generation, convey, installation of key pair own the confidentiality, integrity and non-repudiation.

#### 6.1.1 密钥对的生成 Generation of CA key pair

CA 密钥对由中华人民共和国密码主管部门批准和许可的设备生成的。由于中华人民共和国对于密码产品和认证系统有严格的管理要求，因此，CMCA 在密钥的生成、管理、储存、备份和恢复时应遵循中华人民共和国相关规定进行，在此基础上，遵循 CNS 15135、ISO 19790 或 FIPS140-2 标准的相关规定，使用符合其标准的硬件设备生成和管理 CA 密钥。CA 密钥生成过程需要在独立第三方公正方见证下进行，并由其出具见证报告。CA 密钥生成日志记录在加密机设备中，将永久保存。

订户密钥对由订户自身的服务器或其它设备内置的密钥生成机制生成，中国移动 CMCA 有义务指导订户按照正确的流程生产密钥，中国移动 CMCA 拒绝弱密钥申请数字证书，并可在订户需要时提供相应的技术支持人员帮助订户生成正确的密钥。

The CA key pair is generated by a device approved and licensed by the cryptography authority of the People's Republic of China. Since the People's Republic of China has strict management requirements for cryptographic

products and authentication systems, CMCA should follow the relevant provisions of the People's Republic of China in key generation, management, storage, backup and recovery. On this basis, CMCA should follow the relevant provisions of CNS 15135, ISO 19790 or fips140-2 standards, The CA key is generated and managed by hardware devices that meet its standards. The CA key generation process needs to be witnessed by an independent third party, who will issue a witness report. The CA key generation log is recorded in the encrypt or device and will be saved permanently.

The subscriber key pair is generated by the built-in key generation mechanism of the subscriber's own server or other devices. CMCA has the obligation to guide the subscriber to produce the key according to the correct process. CMCA refuses the weak key application for digital certificate, and can provide the corresponding technical support personnel to help the subscriber generate the correct key.

### **6.1.2 私钥传送给订户 Public key transfer**

私钥由订户自行生成，不需要将私钥传递给订户。

The private key is generated by the subscriber itself, and it is not necessary to pass the private key to the subscriber.

### **6.1.3 公钥传送给证书签发机构 Public key transmission of CA**

证书订户公钥以 PKCS #10 格式提交证书请求给 CA，应通过安全可靠的方式进行传输。

The certificate subscriber's public key submits the certificate request to CA in PKCs # 10 format, which should be transmitted in a safe and reliable way.



### **6.1.4 CMCA 电子认证服务机构公钥传送给依赖方 CMCA e-certification service agency public key is transmitted to the depending party**

中国移动 CMCA 的根公钥包含在中国移动 CMCA 根证书中。证书订户可以从中国移动 CMCA 的网站上下载中国移动 CMCA 根证书。

Root public key of CMCA is contained in root certificate of CMCA. Certificate subscribers can download the CMCA root certificate from the website of CMCA.

### **6.1.5 密钥的长度 Length of key**

中国移动 CMCA 遵从国家法律法规、政府主管机构等对密钥长度的明确规定和要求，目前：

ROOT CA---RSA-4096/SHA-256

EV SSL CA---RSA-4096/SHA-256

SSL CA---RSA-4096/SHA-256

订户密钥的长度均为 RSA-2048

CMCA complies with the clear regulations and requirements of national laws and regulations and government authorities on key length

ROOT CA---RSA-4096/SHA-256

EV SSL CA---RSA-4096/SHA-256

SSL CA---RSA-4096/SHA-256

The length of subscriber key is rsa-2048

## 6.1.6 公钥参数的生成和质量检查 **Generation and quality check of public key**

公钥参数由国家密码管理局许可的、中国移动 CMCA 数字证书签发系统支持的硬件产生。

The public key parameter is generated by the hardware which is permitted by State Cryptography Administration and supported by digital certificate issuing system of CMCA.

CMCA 在采购这些设备时要求其必须具有国家密码主管部门的相应资质，并遵从国家密码主管部门发布的《证书认证系统密码及相关安全技术规范》以及其他相关规范和标准要求，如对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均已达到足够的安全等级要求等。

When purchasing these devices, CMCA requires that they must have the corresponding qualification of the national cryptography authority, and comply with the "technical specification for password and related security of certificate authentication system" issued by the national cryptography authority, as well as other relevant specifications and standards, such as the quality inspection standard for generated public key parameters, the built-in protocols of these devices The algorithm has reached enough security level requirements.

## 6.1.7 密钥使用目的 **Purpose of key use**

CMCA 的根密钥仅用于签发以下证书：

- 为根 CA 自己签发的根 CA 自签名证书；
- 中级 CA 证书；
- OCSP 响应验证证书。

The root key of CMCA is only used to issue the following certificates:

- The root CA self-signed certificate issued by the root CA itself;
- Intermediate CA certificate;

## ■ OCSP response validation certificate.

订户的密钥用于提高安全服务，例如身份认证、信息加密和解密、不可抵赖性和信息的完整性。

The subscriber's key is used to enhance security services, such as identity authentication, information encryption and decryption, non-repudiation, and information integrity.

## **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**

中国移动 CMCA 使用国家密码管理局许可的产品，密码模块的标准符合国家规定的要求。

CMCA uses the products permitted by the State Cryptography Administration, and the standards of cryptographic module meet the requirements stipulated by the state.

### **6.2.2 私钥多人控制 Private key multi-person control**

中国移动 CMCA 采用 M 选 N 多人控制策略激活、使用、停止中国移动 CMCA 的签名密钥。M $\geq$ N，M 为 5，N 为 3。

CMCA adopts the N-out-of-M multi-person control policy to activate, use and stop the signature key of CMCA. M $\geq$ N (M is 5 and N is 3).

### **6.2.3 私钥托管 Private key trusteeship**

对于 CA 私钥,CMCA 无托管业务。

For CA private key, CMCA has no managed service.

## 6.2.4 私钥备份 Private key backup

CA 的私钥由加密机产生，被分割保存在 5 个 UKEY 中，由经过授权的安全管理人员掌握，并保存在屏蔽机房中保险箱中。

The private key of CA is generated by the encryptor and divided into 5 UKEYs, controlled by authorized security administrators, and stored in a safe in the shielded machine room.

订户的私钥由订户产生，建议订户自行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改或泄漏。

The private key of the subscriber is generated by the subscriber. It is suggested that the subscriber backup the private key by himself, and protect the backup private key by password or other access control mechanism to prevent unauthorized modification or disclosure

## 6.2.5 私钥归档 Private key archival

当 CMCA 的 CA 密钥对到期后，这些密钥对将被归档保存至少 10 年。归档的 CA 密钥对保存在本 CP/CPS 6.2.1 所述的硬件密码模块中，并且 CMCA 的密钥管理策略和流程都确保了归档后的 CA 密钥对不会再被用于生产系统中。当归档 CA 密钥对达到归档保存期限之后，CMCA 将按照本 CPS6.2.10 所述的方法进行安全地销毁。

When the CA key pairs of CMCA expire, these key pairs will be archived for at least 10 years. The archived CA key pair is stored in the hardware password module described in CP/CPS 6.2.1. The key management strategy and process of CMCA ensure that the archived CA key pair will not be used in the production system. When the backup CA key pair reaches the archive retention period, CMCA will be destroyed safely in accordance with the method described in CP/CPS 6.2.10.

CMCA 不对订户证书的私钥进行归档。

CMCA does not archive the private key of the subscriber certificate.

### **6.2.6 私钥导入、导出密码模块 Private key transfer into or from a cryptographic module**

CMCA 通过加密机生成 CA 密钥对, 需要备份或迁移 CA 私钥时, 从加密机中导出的私钥采用密文形式并由多人控制。

CMCA generates CA key pairs through an encryption machine. When it is necessary to backup or migrate the CA private key, the private key exported from the encryption machine is in ciphertext form and controlled by multiple people.

通过硬件产生的订户私钥不能导出密码模块。其他方法产生的订户私钥在导出时应采取加密的方式进行。

The subscriber private key generated by hardware cannot be exported to cryptographic module. The private key generated by other methods should be encrypted when exporting.

### **6.2.7 私钥在密码模块的存储 Private key storage on cryptographic module**

私钥以密文的方式分段加密存放在通过国家密码管理部门产品鉴定的硬件加密模块中。

The private key is encrypted and stored in the hardware encryption module which has passed the product authentication of the national password management department.

订户私钥存储在文件证书或 USBKey 等安全介质中。

The subscriber's private key is stored in secure media such as file certificates or USBKey.

CA 系统采用符合与 FIPS140-2 Level 3 安全规格相当的密码模块。

The CA system adopts a password module that meets the security specifications equivalent to FIPS140-2 Level 3 security specification.

### 6.2.8 激活私钥 Private key activation

CA 私钥存放在硬件密码模块中，并且其激活数据按第 6.2.2 节使用加密设备的管理员权限实现，具有激活私钥权限的管理员使用 USBKey 登录，启动密钥管理程序，进行激活私钥的操作，需要三名管理员以上同时到场。

The CA private key is stored in the hardware password module, and its activation data is implemented using the administrator privileges of the encryption device according to Section 6.2.2. Administrators with the authorization to activate the private key log in using USBKey, start the key management program, and perform the operation of activating the private key. Three or more managers are required to be present at the same time.

订户的私钥保存在密码模块中，订户使用密码模块口令（或 PIN 码）保护私钥。订户的私钥需要验证口令（或 PIN 码）或才能被激活、使用。

The subscriber's private key is stored in the password module, and the subscriber uses the password module password (or PIN code) to protect the private key. The private key of the subscriber needs to verify the password (or PIN code) or be activated and used.

### 6.2.9 解除私钥激活状态 Private key deactivation

对于服务器证书，当服务程序关闭、系统注销或系统断电后私钥即进入非激活状态。

For the server certificate, the private key immediately enters in the non-activation status after service procedure is closed; the system is cancelled or the system is powered off.

对于中国移动 CMCA 及其注册机构的运营服务器证书的私钥，当 CA 或 RA 系统向密码模块发出登出 (logout) 或密码管理软件向密码模块发出关闭 (close)

指令，或存放私钥的密码模块断电，私钥进入非激活状态。

For the private key of operation server certificate of CMCA and its RA, when CA or RA system sends the logout instruction to the cryptographic module or the password management software sends the close instruction to the cryptographic module, or the cryptographic module which is used to store the private key is powered off, the private key enters in the non-activation state.

对于中国移动 CMCA 私钥，当 CA 系统向密码模块发出登出（logout）或密码管理软件向密码模块发出关闭（close）指令，或存放私钥的硬件密码模块断电，私钥进入非激活状态。

For the private key to CMCA, when CA system sends out logout to cryptographic module, or the password management software sends out the close command to cryptographic module, or the hardware cryptographic module storing private key loses power, the private key will enter in the inactivated state.

## 6.2.10 销毁私钥 Private key destruction

在 CA 私钥生命周期结束后，中国移动 CMCA 将 CA 私钥继续保存在一个备份硬件密码模块中，并进行归档，其他的 CA 私钥备份被安全销毁。归档的 CA 私钥在其归档期限结束后，需在多名可信人员参与的情况下安全销毁。CA 私钥的销毁将确保 CA 私钥从硬件密码模块中彻底删除，不留有任何残余信息。

After the CA private key life cycle ends, CMCA shall continue keeping the CA private key in a backup hardware cryptographic module, and conduct the archival. Other CA private key backup is safely destroyed. After the filing deadline of archiving CA private key ends, the private key shall be destroyed when many trusted persons participate in. CA private key shall be completely destroyed from the hardware cryptographic module without any residual information.



## **6.2.11 密码模块的评估 Evaluation of cryptographic module**

CMCA 使用国家密码主管部门鉴定并批准使用的具有自主知识产权的高速主机加密设备，接受其颁布的各类标准、规范、评估结果等各类要求。

CMCA uses the high-speed host encryption equipment with independent intellectual property rights identified and approved by the national encryption authority, and accepts various standards, specifications, evaluation results and other requirements issued by CMCA.

## **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**

中国移动 CMCA 对所有的公钥进行归档处理。

CMCA archives all public keys.

### **6.3.2 证书操作期和密钥对使用期 Certificate operational periods and key pair usage periods**

中国移动 CMCA 会在客户申请审核鉴定通过，5 个工作日内将证书颁发给客户，密钥对的使用期限与证书有效期相一致，设置期限如下：

CMCA will issue certificate to customers within 5 working days after customer application passes review. The key pair service life is consistent with the effective date in the certificate, The setting period is as follows:

- 根证书有效期应当最长为 25 年
- 中级 CA 证书有效期最长为 20 年
- 用户证书有效期不超过 397 天
- The root certificate should be valid for a maximum of 25 years

- The maximum validity period of subordinate CA certificate is 20 years
- The validity period of user certificate shall not exceed 397 days.

## 6.4 敏感数据 Sensitive data

### 6.4.1 敏感数据的产生 Sensitive data generation

敏感数据包括中国移动 CMCA 提供的口令、被加密的数据等。中国移动 CMCA 提供唯一的不可猜测的口令。这些口令由中国移动 CMCA 根据授权和操作的许可仅发放给授权客户。

Sensitive data includes password and encrypted data provided by CMCA. CMCA provides the only unpredictable password. These passwords are only given to authorized customers by CMCA according to authorization and operation permission.

### 6.4.2 敏感数据的保护 Sensitive data protection

中国移动 CMCA 采取加解密机制等多种方式保护敏感数据，以避免未授权使用。未授权客户企图使用敏感数据达到预定目的时，敏感数据会自动锁定。

CMCA adopts multiple ways, including encryption and decryption mechanism to protect sensitive data, to avoid unauthorized use. The unauthorized customer attempts to reach the predicted purpose with the sensitive data which shall be automatically locked. Mobile CMCA adopts encryption and decryption mechanism to protect sensitive data to avoid unauthorized use. When unauthorized customers attempt to use sensitive data to achieve the intended purpose, the sensitive data will be automatically locked.

### 6.4.3 敏感数据的其他方面 Other aspects of sensitive data

- **激活数据的传输 Activation of data transmission**

存有 CA 私钥的加密设备和相关 IC 卡,通常被保存在 CMCA 最安全区机房,不能携带离开 CMCA。如在某种特殊情况下需要进行传输时(如建设灾备系统时),其传送过程需要在 CMCA 安全管理人员和密钥管理人员共同监督的情况下进行。

Encryption devices and related IC cards with CA private key are usually stored in the most secure computer room of CMCA and cannot be carried away from CMCA. For example, in some special circumstances, the transmission process needs to be supervised by CMCA security manager and key manager.

对于证书订户,通过网络传输用于激活私钥的口令时,需要采取加密等保护措施,以防丢失。

For certificate subscribers, when the password used to activate the private key is transmitted over the network, encryption and other protection measures should be taken to prevent loss.

- **激活数据的销毁 Destruction of activation data**

CMCA 通过对设备初始化的方式来销毁 CA 私钥的激活数据。

订户私钥的激活数据在不需要时由订户自行销毁,订户应确保他人无法通过残余信息、存储介质直接或间接地恢复激活数据。

CMCA destroys the activation data of CA private key by initializing the device. The activation data of the subscriber's private key shall be destroyed by the subscriber when it is not needed. The subscriber shall ensure that the activation data cannot be recovered directly or indirectly by others through residual information or storage medium.

## 6.5 计算机安全控制 Computer Security Controls

### 6.5.1 具体的计算机安全技术要求 Computer security technical requirements

CMCA 数字证书签发系统的数据文件和设备由中国 CMCA 系统管理员维护，未经中国 CMCA 管理员授权，其它人员不能操作和控制 CMCA 系统。中国 CMCA 认证中心系统部署在多级不同厂家的防火墙之内，确保系统网络安全。The data document and equipment of CMCA digital certificate issuing system are maintained by CMCA system administrator. Without the authorization of CMCA administrator, anyone can't operate and control CMCA system; Other common customer has no system account and password. CMCA system is deployed in the firewall of multi-level different manufacturers to ensure the system network security.

中国 CMCA 中心系统内的计算机均采用了如防火墙、入侵检测、主机服务端口限制、操作系统安全补丁等防范措施，充分保证了计算机的安全可靠。The computers in CMCA system shall adopt the preventive measures such as firewall, intrusion detection, host service port restriction, operation system security patches, etc. to fully ensure the computer's safety and reliability.

对于设备有一套完整的保管和维护制度：

There is a complete system for the storage and maintenance of the equipment:

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。

Special personnel shall be responsible for the collection and storage of equipment, and the equipment collection, access to warehouse and scrap registration shall be made.

2. 对设备定期进行检查、清洁和保养维护。

Check, clean and maintain the equipment regularly.

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。

Make equipment maintenance plan and establish a vulnerable spare parts warehouse meeting the minimum requirements of normal operation.

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、维修

过程及与维修有关的情况等。

When repairing the equipment, the maintenance objects, causes of faults, troubleshooting methods and main points must be recorded

5. 设备维修时，必须有派专人在场监督

When the equipment is maintained, special personnel must be assigned to supervise on the spot.

6. 唯一的设备密码。

Unique device password.

并且每一个使用 CMCA 系统的人员必须使用唯一的数字证书，人员配置的访问限制为执行工作职责要求的最小权限，满足双因素认证。

And every person using CMCA system must use a unique digital certificate. The access limit of personnel configuration is the minimum permission required to perform the work responsibilities, and meet the double factor authentication.

CA 对所有能够直接导致证书颁发的账户实施多因素认证。

CA performs multi factor certification for all accounts that can directly lead to certificate issuance.

## 6.5.2 计算机安全评估 Computer security rating

中国移动 CMCA 使用的密码设备是通过国家密码管理局批准生产的密码设备。其他涉及安全的网络设备、主机、系统软件等都通过了国家相关部门的检测，属合格产品。

The cryptographic equipment used by CMCA is the cryptographic equipment manufactured through the approval of the State Cryptography Administration. The network equipment involving security, host, system software, etc. are the qualified products passing the inspection of the relevant state department.

## 6.6 系统生命周期控制 System life cycle controls

### 6.6.1 系统开发控制 System development controls

CMCA 的系统由符合国家相关安全标准和具有密码标准资质的可靠开发商开发，其开发过程符合 CMCA 系统管理的各项规定。

CMCA system is developed by a reliable developer which meets relevant national security standards and has the qualification for cryptography standards, and the developing process complies with all requirements of CMCA system management.

### 6.6.2 安全管理控制 Security management controls

CMCA 已制定了各种安全策略、管理制度与流程对 CA 运营系统进行安全管理。

CMCA has made various security policies, management systems and procedures to carry out security management to CA operation system.

### 6.6.3 生命周期的安全控制 Life cycle security control

CMCA 的证书认证系统在系统设计过程中充分进行了安全性考虑，在开发过程中有严格的流程进行代码安全管理，在开发完成后进行了严格的安全测试，在正式使用前通过了国家有关部门的系统安全性审查。

Security has been fully considered during the design of CMCA certificate authentication system. There are strict procedures for code security management in the development process, and strict security tests are conducted after the system is developed. The system passes system security review of relevant national department before being used formally.

## 6.7 网络的安全控制 Network security controls

中国移动 CMCA 有防火墙以及其他访问控制机制保护，其配置只允许已授权的机器访问。并且通过入侵检测、漏洞扫描等机制配合保证系统网络的安全。CMCA is protected by firewall and other access control mechanisms, and its configuration only accept the visit of authorized machine. Pass the intrusion detection, vulnerability scanning and other mechanisms to ensure the system network security.

只有经过授权的中国移动 CMCA 员工才能够进入中国移动 CMCA 签发系统、中国移动 CMCA 注册系统、中国移动 CMCA 目录服务器、中国移动 CMCA 证书发布系统等设备或系统。所有授权客户必须有合法的安全令牌，并且通过密码验证。

Only authorized employees of CMCA can enter the equipment or systems including CMCA issuing system, CMCA registration system, CMCA LDAP server, CMCA certificate issuing system. All authorized customers shall have the legal safety token which shall pass the password verification.

## 6.8 时间戳 Digital Time Stamp (DTS)

数字时间戳（DTS: Digital Time Stamp）是对时间信息的数字签名，主要用于实现确定在某一时间某个文件确实存在和确定多个文件在时间上的逻辑关系功能。

Digital Time Stamp (DTS) is the digital signature of time information, which is mainly used to confirm certain document really exists at certain time and confirm the logic relation function of many documents on the time.



## 7. 证书、证书吊销列表和在线证书状态协议 CERTIFICATE, CRL, AND OCSP PROFILES

### 7.1 证书 Certificate Profile

CMCA 签发的证书均符合 X.509 V3 证书格式。均按照 RFC5280 设置，符合 CA/Browser 的当前版本要求。证书的最基本字段与内容见下表。

All the certificates issued by CMCA conform to the format of X.509 V3 certificate. All of them are set according to rfc5280 and meet the requirements of the current version of CA / Browser. The most basic fields and contents of the certificate are shown in the table below.

CMCA GLOBAL TRUST ROOT CA

证书域	域值
版本	V3
序列号	包含 24 位的随机数
签名算法	SHA256RSA
颁发者	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN
有效期起止日	证书有效期起始时间
有效期终止日	证书有效期终止时间
主题	证书的主题 DN，见 CSP7.1.4
公钥	RSA（4096）
基本限制	Subject Type=CA Path Length Constraint=None
密钥用法	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

CMCA GLOBAL TRUST ROOT CA

<b>Certificate domain</b>	<b>Field value</b>
Edition	V3

Serial number	Random number containing 24 bits
Signature algorithm	SHA256RSA
Issuer	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN
Effective date	Certificate validity start time
Expiry date	Certificate expiry date
Subject	Subject DN of certificate, see csp7.1.4
Public key	RSA (4096)
Basic Constraints	Subject Type=CA Path Length Constraint=None
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

### CMCA SSL CA

证书域	域值
版本	V3
序列号	包含 24 位的随机数
签名算法	SHA256RSA
颁发者	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN
有效期起止日	证书有效期起始时间
有效期终止日	证书有效期终止时间
主题	证书的主题 DN, 见 CSP7.1.4
公钥	RSA (4096)
颁发机构访问信息	[1]Authority Info Access Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://mpus.cmca.net:8080/files/downloadcenter/CMCA GLOBALTRUSTROOTCA.cer [2]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://mpus.cmca.net:8083/ocsp

基本限制	Subject Type=CA Path Length Constraint=None
证书策略	[1]Certificate Policy: Policy Identifier=所有颁发策略 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://mpus.cmca.net:8083/files/downloadcenter/cps.doc
CRL 发布点	该发布点包含了一个 URL，用于获得 CRL 文件。
密钥用法	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

### CMCA SSL CA

Certificate domain	Field value
Edition	V3
Serial number	Random number containing 24 bits
Signature algorithm	SHA256RSA
Issuer	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN
Effective date	Certificate validity start time
Expiry date	Certificate expiry date
Subject	Subject DN of certificate, see csp7.1.4
Public key	RSA (4096)
Authority access information	[1]Authority Info Access Access Method=Certificate issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://mpus.cmca.net:8080/files/downloadcenter/CMCA GLOBALTRUSTROOTCA.cer [2]Authority Info Access Access Method=Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://mpus.cmca.net:8083/ocsp
Basic Constraints	Subject Type=CA Path Length Constraint=None
Certificate Policy	[1]Certificate Policy: Policy Identifier=All award strategies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://mpus.cmca.net:8083/files/downloadcenter/cps.doc
CRL	The publishing point contains a URL to get the CRL file.

Distributionpoint	
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

### CMCA EV SSL CA

证书域	域值
版本	V3
序列号	包含 24 位的随机数
签名算法	SHA256RSA
颁发者	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN
有效期起止日	证书有效期起始时间
有效期终止日	证书有效期终止时间
主题	证书的主题 DN, 见 CSP7.1.4
公钥	RSA (4096)
颁发机构访问信息	[1]Authority Info Access Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://mpus.cmca.net:8080/files/downloadcenter/CMCA GLOBALTRUSTROOTCA.cer [2]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://mpus.cmca.net:8083/ocsp
基本限制	Subject Type=CA Path Length Constraint=None
证书策略	[1]Certificate Policy: Policy Identifier=所有颁发策略 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://mpus.cmca.net:8083/files/downloadcenter/cps.doc
CRL 发布点	该发布点包含了一个 URL, 用于获得 CRL 文件。
密钥用法	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

### CMCA EV SSL CA

<b>Certificate domain</b>	<b>Field value</b>
---------------------------	--------------------

Edition	V3
Serial number	Random number containing 24 bits
Signature algorithm	SHA256RSA
Issuer	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN
Effective date	Certificate validity start time
Expiry date	Certificate expiry date
Subject	Subject DN of certificate, see csp7.1.4
Public key	RSA (4096)
Authority access information	[1]Authority Info Access Access Method=Certificate authority issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://mpus.cmca.net:8080/files/downloadcenter/CMCA GLOBALTRUSTROOTCA.cer [2]Authority Info Access Access Method=Online certificate status protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://mpus.cmca.net:8083/ocsp
Basic Constraints	Subject Type=CA Path Length Constraint=None
Certificate Policy	[1]Certificate Policy: Policy Identifier=All issuance strategies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://mpus.cmca.net:8083/files/downloadcenter/cps.doc
CRL Distributionpoint	The publishing point contains a URL to get the CRL file.
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

### 订户证书 (EV)

证书域	域值
版本	V3
序列号	包含 24 位的随机数
签名算法	SHA256RSA

颁发者	CN = CMCA EV SSL CA O = Aspire Technologies C = CN
有效期起止日	证书有效期起始时间
有效期终止日	证书有效期终止时间
主题	证书的主题 DN，见 CSP7.1.4
公钥	RSA（2048）
颁发机构访问信息	[1]Authority Info Access Access Method=证书颁发机构颁发者（1.3.6.1.5.5.7.48.2） Alternative Name: URL=http://mpus.cmca.net:8080/files/downloadcenter/CMCAEVSSLCA.cer [2]Authority Info Access Access Method=联机证书状态协议（1.3.6.1.5.5.7.48.1） Alternative Name: URL=http://mpus.cmca.net:8083/ocsp
证书策略	[1]Certificate Policy: Policy Identifier=2.23.140.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://mpus.cmca.net:8083/files/downloadcenter/cps.doc
CRL 发布点	该发布点包含了一个 URL，用于获得 CRL 文件。
密钥用法	Digital Signature, Key Encipherment (a0)
增强密钥用法	客户端身份验证（1.3.6.1.5.5.7.3.2） 服务器身份验证（1.3.6.1.5.5.7.3.1）
主题备用名	域名

#### Subscriber certificate（EV）

Certificate domain	Field value
Edition	V3
Serial number	Random number containing 24 bits
Signature algorithm	SHA256RSA
Issuer	CN = CMCA EV SSL CA O = Aspire Technologies C = CN
Effective date	Certificate validity start time

Expiry date	Certificate expiry date
Subject	Subject DN of certificate, see csp7.1.4
Public key	RSA (2048)
Authority access information	<p>[1]Authority Info Access            Access Method=Certificate authority issuer            (1.3.6.1.5.5.7.48.2)            Alternative Name:            URL=http://mpus.cmca.net:8080/files/downloadcenter/CMCAEVSSLCA.cer</p> <p>[2]Authority Info Access            Access Method=Online certificate status protocol            (1.3.6.1.5.5.7.48.1)            Alternative Name:            URL=http://mpus.cmca.net:8083/ocsp</p>
Certificate Policy	<p>[1]Certificate Policy:            Policy Identifier=2.23.140.1.1            [1,1]Policy Qualifier Info:            Policy Qualifier Id=CPS            Qualifier:            http://mpus.cmca.net:8083/files/downloadcenter/cps.doc</p>
CRL Distribution point	The publishing point contains a URL to get the CRL file.
Key Usage	Digital Signature, Key Encipherment (a0)
Extended Key Usage	Client authentication (1.3.6.1.5.5.7.3.2) Server authentication (1.3.6.1.5.5.7.3.1)
Subject Alternative name	Domain name

### 订户证书 (OV)

证书域	域值
版本	V3
序列号	包含 24 位的随机数
签名算法	SHA256RSA
颁发者	CN = CMCA SSL CA O = Aspire Technologies C = CN
有效期起止日	证书有效期起始时间
有效期终止日	证书有效期终止时间
主题	证书的主题 DN, 见 CSP7.1.4
公钥	RSA (2048)



颁发机构访问信息	[1]Authority Info Access Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name:  URL=http://mpus.cmca.net:8080/files/downloadcenter/CMCASSLCA.cer [2]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://mpus.cmca.net:8083/ocsp
证书策略	[1]Certificate Policy: Policy Identifier=2.23.140.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://mpus.cmca.net:8083/files/downloadcenter/cps.doc
CRL 发布点	该发布点包含了一个 URL，用于获得 CRL 文件。
密钥用法	Digital Signature, Key Encipherment (a0)
增强密钥用法	客户端身份验证 (1.3.6.1.5.5.7.3.2) 服务器身份验证 (1.3.6.1.5.5.7.3.1)
主题备用名	域名

### Subscriber Certificate (OV)

Certificate domain	Field value
Edition	V3
Serial number	Random number containing 24 bits
Signature algorithm	SHA256RSA
Issuer	CN = CMCA SSL CA O = Aspire Technologies C = CN
Effective date	Certificate validity start time
Expiry date	Certificate expiry date
Subject	Subject DN of certificate, see csp7.1.4
Public key	RSA (2048)

Authority access information	[1]Authority Info Access Access Method=Certificate authority issuer (1.3.6.1.5.5.7.48.2) Alternative Name:  URL=http://mpus.cmca.net:8080/files/downloadcenter/CMCASSLCA.cer [2]Authority Info Access Access Method=Online certificate status protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://mpus.cmca.net:8083/ocsp
Certificate Policy	[1]Certificate Policy: Policy Identifier=2.23.140.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://mpus.cmca.net:8083/files/downloadcenter/cps.doc
CRL Distributionpoint	The publishing point contains a URL to get the CRL file.
Key Usage	Digital Signature, Key Encipherment (a0)
Extended Key Usage	Client authentication (1.3.6.1.5.5.7.3.2) Server authentication (1.3.6.1.5.5.7.3.1)
Subject Alternative name	Domain name

### 订户证书（DV）

证书域	域值
版本	V3
序列号	包含 24 位的随机数
签名算法	SHA256RSA
颁发者	CN = CMCA SSL CA  O = Aspire Technologies  C = CN
有效期起止日	证书有效期起始时间
有效期终止日	证书有效期终止时间
主题	证书的主题 DN，见 CPS7.1.4
公钥	RSA（2048）

颁发机构访问信息	[1]Authority Info Access Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://mpus.cmca.net:8080/files/downloadcenter/CMCASLCA.cer [2]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://mpus.cmca.net:8083/ocsp
证书策略	[1]Certificate Policy: Policy Identifier=2.23.140.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://mpus.cmca.net:8083/files/downloadcenter/cps.doc
CRL 发布点	该发布点包含了一个 URL，用于获得 CRL 文件。
密钥用法	Digital Signature, Key Encipherment (a0)
增强密钥用法	客户端身份验证 (1.3.6.1.5.5.7.3.2) 服务器身份验证 (1.3.6.1.5.5.7.3.1)
主题备用名	域名

### Subscriber Certificate (DV)

Certificate domain	Field value
Edition	V3
Serial number	Random number containing 24 bits
Signature algorithm	SHA256RSA
Issuer	CN = CMCA SSL CA O = Aspire Technologies C = CN
Effective date	Certificate validity start time
Expiry date	Certificate expiry date
Subject	Subject DN of certificate, see csp7.1.4
Public key	RSA (2048)

Authority access information	<p>[1]Authority Info Access Access Method=Certificate authority issuer (1.3.6.1.5.5.7.48.2) Alternative Name:  URL=http://mpus.cmca.net:8080/files/downloadcenter/CMCASSLCA.cer</p> <p>[2]Authority Info Access Access Method=Online certificate status protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://mpus.cmca.net:8083/ocsp</p>
Certificate Policy	<p>[1]Certificate Policy: Policy Identifier=2.23.140.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://mpus.cmca.net:8083/files/downloadcenter/cps.doc</p>
CRL Distribution point	The publishing point contains a URL to get the CRL file.
Key Usage	Digital Signature, Key Encipherment (a0)
Extended Key Usage	Client authentication (1.3.6.1.5.5.7.3.2) Server authentication (1.3.6.1.5.5.7.3.1)
Subject Alternative name	Domain name

### 7.1.1 证书版本号 Version Number(s)

X.509 V3。

### 7.1.2 证书扩展项 Certificate Content and Extensions; Application of RFC 5280

CMCA 签发的证书，其证书扩展项遵循 IETF RFC 5280 标准要求。

The certificate extension of CMCA follows the requirements of IETF RFC 5280.

#### 7.1.2.1 根证书扩展项目 Root CA Certificate

##### 1、 密钥用法 Key usage

按照 RFC5280 进行填充，内容为 Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)，该项的 criticality 域设置为 true。

Fill in according to rfc5280, the contents are digital signature, certificate signing, off-line CRL signing, CRL signing (86), and the criticality field of this item is set to true.

## 2、基本约束 Basic constraints

Path Length Constraint=None, 该项的 criticality 域设置为 true。

Path length constraint = none, and the criticality field of the item is set to true.

## 3、颁发者机构密钥标识符 Authority Key Identifier

颁发者机构密钥标识符由根 CA 证书公钥的 256 位 SHA256 散列组成。该项的 criticality 域设置为 false。

The authority key identifier consists of a 256 bit SHA256 hash of the public key of the root CA certificate. The criticality field of the item is set to false.

## 4、主体密钥标识符 Subject key identifier

主体密钥标识符由根 CA 证书公钥的 256 位 SHA256 散列组成。该项的 criticality 域设置为 false。

The principal key identifier consists of 160 bit SHA1 hash of the root CA certificate public key. The criticality field of the item is set to false.

### 7.1.2.2 中级证书扩展项 Subordinate certificate extension

#### 1、密钥用法 (Key Usage) Key usage

按照 RFC5280 进行填充, 内容为 Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86), 该项的 criticality 域设置为 true。

Fill in according to rfc5280, the contents are digital signature, certificate signing, off-line CRL signing, CRL signing (86), and the criticality field of this item is set to true.

#### 2、证书策略 (Certificate Policies Extension) Certificate Policies extension

按照 RFC5280 进行填充。该项的 criticality 域设置为 false。

Fill according to rfc5280. The criticality field of the item is set to false.

#### 3、基本约束 (Basic Constraints) Basic constraints

Path Length Constraint=None, 该项的 criticality 域设置为 true。

Path length constraint = none, and the criticality field of the item is set to true.

#### 4、CRL 发布点 (CRL Distribution Points) CRL distribution points

该发布点包含了一个 URL，URL 地址为 https://mpus.cmca.net:8080/crl/crl1.crl 用于获得 CRL 文件，该项的 criticality 域设置为 false。

The publishing point contains a URL, the URL address is https://mpus.cmca.net : 8080 / CRL / crl1.crl is used to get the CRL file, and the criticality field of this item is set to false.

#### 5、颁发者机构密钥标识符 (Authority Key Identifier) Authority key identifier

颁发者机构密钥标识符由根 CA 证书公钥的 256 位 SHA256 散列组成。该项的 criticality 域设置为 false。

The authority key identifier consists of a 256 bit SHA256 hash of the public key of the root CA certificate. The criticality field of the item is set to false.

#### 6、主体密钥标识符 (Subject Key Identifier) Subject key identifier

主体密钥标识符由中级 CA 证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false。

The principal key identifier consists of a 160 bit SHA1 hash of the subordinate CA certificate public key. The criticality field of the item is set to false.

#### 7、颁发者机构访问 (Authority Info Access) Authority info access

颁发者机构访问为联机证书状态协议，该项的 criticality 域设置为 false。

The authority access is the online certificate status protocol, and the criticality field of the key is set to false.

### 7.1.2.3 订户证书扩展项 Subscriber Certificate

#### 1、密钥用法 (Key Usage) Key usage

按照 RFC5280 进行填充，内容为 Digital Signature, Key Encipherment (a0)，该项的 criticality 域设置为 true。

Fill in according to rfc5280, the content is digital signature, key encryption (A0), and the criticality field of the item is set to true.

## 2、证书策略 (Certificate Policies Extension) Certificate Policies extension

按照 RFC5280 进行填充。该项的 criticality 域设置为 false。

Fill according to rfc5280. The criticality field of the item is set to false.

## 3、扩展密钥用法 (Extended Key Usage) Extended key usage

如果有将按照RFC5280进行填，内容为客户端身份验证 (1.3.6.1.5.5.7.3.2)，服务器身份验证 (1.3.6.1.5.5.7.3.1)。该项的criticality域设置为false。

If yes, it will be filled in according to rfc5280, including client authentication (1.3.6.1.5.5.7.3.2) and server authentication (1.3.6.1.5.5.7.3.1). The criticality field of the item is set to false.

## 4、CRL 发布点 (CRL Distribution Points) CRL distribution points

该发布点包含了一个 URL，用于获得 CRL 文件，该项的 criticality 域设置为 false。

The publishing point contains a URL to get the CRL file, and the criticality field of the item is set to false.

## 5、颁发者机构密钥标识符 (Authority Key Identifier) Authority key identifier

颁发者机构密钥标识符由中级CA证书公钥的256位SHA256散列组成。该项的criticality域设置为false。

The issuer key identifier consists of a 256 bit SHA256 hash of the subordinate CA certificate public key. The criticality field of the item is set to false.

## 6、主题密钥标识符 (Subject Key Identifier) Subject key identifier

主题密钥标识符标识了被认证的公钥，可用于区分同一主体使用的不同密钥（如证书密钥更新时）。其值从公钥中或者生成唯一值的方法导出。该项的criticality域设置为false。

The subject key identifier identifies the authenticated public key, which can be used to distinguish different keys used by the same principal (such as when the certificate key is updated). Its value is derived from the public key or from a method that generates a unique value. The criticality field of the item is set to false.

## 7、颁发者机构访问 (Authority Info Access) Authority info access



颁发者机构访问为联机证书状态协议，该项的 **criticality** 域设置为 **false**。

The authority access is the online certificate status protocol, and the criticality field of the key is set to false.

8、使用者备用名称（Subject Alternative Name）Subject alternative name

按照 RFC5280 进行填充，该项的 **criticality** 域设置为 **false**。

Fill in according to rfc5280, and the criticality field of the item is set to false.

### 7.1.3 算法对象标识符 Algorithm object identifier

中国移动 CMCA 签发的证书按照 RFC 5280 标准，用 SHA256 算法签名。

The certificate issued by CMCA is signed with sha256 algorithm according to RFC 5280 standard.

### 7.1.4 名称形式 Name form

CMCA 签发的证书（包括根证书、中间证书以及订户证书）的 DN 都采用 X.500（Distinguished Name; DN）命名方式，遵循 RFC5280 相关规定。

The DN of certificates issued by CMCA (including root certificate, subordinate certificate and subscriber certificate) adopts X.500 (distinguished name; According to rfc5280.

#### 7.1.4.1 证书颁发者 Certificate issuer

➤ DV SSL 证书（certificate）

CN = CMCA SSL CA

O = Aspire Technologies

C = CN

➤ OV SSL 证书（certificate）

CN = CMCA SSL CA

O = Aspire Technologies

C = CN

➤ EV SSL 证书 (certificate)

CN = CMCA EV SSL CA

O = Aspire Technologies

C = CN

➤ CMCA EV SSL CA 中级证书 (Subordinate Certificate)

CN = CMCA GLOBAL TRUST ROOT CA

O = Aspire Technologies

C = CN

➤ CMCA SSL CA 中级证书 (Subordinate Certificate)

CN = CMCA GLOBAL TRUST ROOT CA

O = Aspire Technologies

C = CN

➤ CMCA GLOBAL TRUST ROOT CA 根证书 (Root certificate)

CN = CMCA GLOBAL TRUST ROOT CA

O = Aspire Technologies

C = CN

#### 7.1.4.2 证书主题 Subject Information – Subscriber Certificates

CMCA 签发证书的甄别名符合 X.500 关于甄别名的规定，同时符合 CA/Browser 论坛 Baseline Requirements 中 7.1.4 节的要求。

The distinguished name of the certificate issued by CMCA meets the requirements of X.500 on distinguished name, and comply with the requirements of Section 7.1.4 of the CA/Browser Forum Baseline Requirements.

### 7.1.5 名称限制 Name Constraints

CMCA 全球信任体系下签发的证书，其实体名称不允许为匿名或者伪名，必须是有明确含义的识别名称，使用英文名称时应能正确表达实体名称。

The physical name of the certificate issued under CMCA global trust system is

not allowed to be anonymous or pseudo name. It must be an identification name with clear meaning. When using English name, it should be able to correctly express the entity name.

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

CA 中级证书的证书策略扩展项中，certificatePolicies:policyIdentifier 设置为 anyPolicy。

订户证书策略对象标识符如下：

DV SSL 证书对应的证书策略对象标识号符（OID）为 2.23.140.1.2.1。

OV SSL 证书对应的证书策略对象标识号符（OID）为 2.23.140.1.2.2。

EV SSL 证书对应的证书策略对象标识号符（OID）为 2.23.140.1.1。

CMCA 签发的证书应包含策略标识符。证书策略标识符包含一个证书策略对象标识符 OID 和 URL 地址。订户证书的证书策略对象标识符见 1.2，中级证书的证书策略对象标识符是所有策略，根证书没有证书策略对象标识符。订户证书、中级证书策略表述 URL 为

<http://mpus.cmca.net:8083/files/downloadcenter/cps.doc>

In the Certificate Policy Extension of CA subordinate certificate, certificatePolicies:policyIdentifier set to anyPolicy;

The subscriber Certificate Policy object identifier is as follows:

The oid corresponding to DV SSL certificate is 2.23.140.1.2.1.

The oid corresponding to OV SSL certificate is 2.23.140.1.2.2.

The oid of EV SSL certificate is 2.23.140.1.1.

Certificate issued by CMCA should contain policy identifier. The certificate policy identifier contains a certificate policy object identifier oid and a URL address. For the Certificate Policy object identifier of subscriber certificate, see 1.2. The Certificate Policy object identifier of subordinate certificate is all policies, and the root certificate has no certificate policy object identifier. The

policy expression URL of subscriber certificate and subordinate certificate is  
<https://mpus.cmca.net:8080/files/downloadcenter/cps.doc>.

证书标识符符合CA/浏览器论坛（CA/Browser Forum）发布的Baseline Requirements 7.1.6部分要求。

The certificate identifier conforms to section 7.1.6 of the Baseline Requirements published by CA / Browser forum.

### **7.1.7 策略限制扩展项的用法 Usage of Policy Constraints Extension**

未使用本扩展域。

This extended domain is not used.

### **7.1.8 策略限定符的语法和语义 Policy Qualifiers Syntax and Semantics**

未使用本扩展域。

This extended domain is not used.

### **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**

未使用本扩展域。

This extended domain is not used.

## **7.2 证书吊销列表 CRL PROFILE**

CMCA 定期签发CRL(证书吊销列表),供订户查询使用。具体参见 SGP.22 。  
CMCA regularly issues CRL (Certificate Revocation List). It is for subscribers'

inquiries. See SGP.22 for details.

### 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

CRL 符合 RFC5280 要求。列表包含最基本的字段和内容中指定下面的表：

字段	内容
Version	参考 7.2.1 章节
Signature Algorithm	用于对 CRL 进行签名的算法。参考 RFC3279
Issuer	签发 CRL 的实体，CRL 的颁发者。
Effective Date	CRL 文件的发布时间
Next Update	CRL 的下一步发布时间。CRL 的发布频率参考 4.9.7.
Revoked Certificates	插销的证书清单。包括证书序列号以及撤销日期，撤销原因。

#### CRL 基本字段

CRL meets the requirements of rfc5280. The list contains the most basic fields and contents specified in the following table:

Field	Content
Version	Refer to section 7.2.1
Signature Algorithm	The algorithm used to sign CRL. Refer to rfc3279
Issuer	The entity that issues the CRL, the issuer of the CRL.
Effective Date	Release time of CRL file
Next Update	The next release time of CRL. Refer to 4.9.7 for release frequency of CRL
Revoked	List of certificates for the plug. Including certificate serial

Certificates	number, revocation date and revocation reason.
--------------	--

#### CRL basic fields

中国移动 CMCA 每隔 24 小时自动发布最新的 CRL。

CMCA automatically releases the latest CRL every 24 hours.

## 7.3 在线证书状态查询协议 OCSP Profile

CMCA 为证书用户提供 OCSP（在线证书状态查询）服务，OCSP 为 CRL 的有效补充，方便证书订户及时查询证书状态信息。

CMCA provides OCSP (Online Certificate Status Protocol) service for the certificate customer, and OCSP is the effective complement of CRL in order that the certificate subscriber promptly inquires the certificate status information.

### 7.3.1 版本号 Version number(s)

中国移动 CMCA 为证书客户提供 OCSP（在线证书状态查询）服务，OCSP 为 CRL 的有效补充，方便证书订户及时查询证书状态信息。

版本号为 RFC 6960 定义的 OCSPV1 版。

CMCA provides OCSP (Online Certificate Status Protocol) service for the certificate customer, and OCSP is the effective complement of CRL in order that the certificate subscriber promptly inquires the certificate status information.

The version number is OCSPV1 defined by RFC 6960.

### 7.3.2 OCSP 扩展项 OCSP extension

不适用。

Not applicable.

## 8 认证机构审计和其他评估 Audit and other assessments of certification body

### 8.1 审计的频率或情形 Frequency or circumstances of audit

CMCA在如下情形中进行评估：

1. 内部审计：CMCA自行组织内部审计，频率为根据相关内审部门要求定期组织，至少每季度一次；
2. 主管部门的评估和检查：通常为年度检查，具体以国家相关主管部门要求为主；
3. 第三方审计公司的WebTrust审计：每年进行WebTrust审计，且审计报告发布日期不得晚于审计期间结束后三个月。

CMCA evaluates in the following situations:

1. Internal audit: CMCA organizes internal audits on its own, with a frequency of regularly organizing them according to the requirements of relevant internal audit departments, at least once a quarter.
2. Evaluation and inspection by competent authorities: usually annual inspection, mainly based on the requirements of relevant national regulatory authorities.
3. WebTrust audit of the third party audit company: conduct an annual WebTrust audit, and the release date of the audit report shall not be later than three months after the end of the audit period.

### 8.2 审计者的资质 Qualification of auditor

1. 内部审计人员资质：一般为公司内部安全管理人员，或按照公司相关管理要求指定的审计人员；

Qualification of internal auditors: Internal security management personnel of the company, or auditors designated according to relevant management requirements of the company;



2. 主管部门评估审计：由主管部门确认资质要求并指派符合要求的审计人员；  
Evaluation and audit by the competent department: The competent department confirms the qualification requirements and assigns auditors who meet the requirements;

3. 第三方WebTrust审计资质：对外部审计机构和审计师要求如下：

- 熟悉公钥基础设施技术、信息安全、WebTrust审计相关的法律法规、标准规范要求。
- 具备WebTrust审计要求的服务资质和职业资格等
- 具备相关专业技术、工具与技能
- 具有独立审计精神，受法律法规和职业道德规范的约束，在业界享有良好声誉

Third party WebTrust audit qualifications: The requirements for external audit institutions and auditors are as follows:

- Familiar with public key infrastructure technology, information security, WebTrust auditing related laws, regulations, and standard specifications.
- Having service qualifications and professional qualifications required for WebTrust auditing
- Possess relevant professional skills, tools, and skills
- Having an independent auditing spirit, constrained by laws, regulations, and professional ethics, and enjoying a good reputation in the industry

## 8.3 审计者与中国移动 CMCA 的关系 Relationships between auditors and CMCA

### 8.3.1 审计者与中国移动 CMCA 的关系 Relationships between auditors and CMCA

审计者与 CMCA 应无任何业务、财务往来或其它足以影响评估客观性的利害关系。

The auditor and CMCA shall have no business, financial transactions or other

interests that may affect the objectivity of the assessment.

## 8.4 审计内容 Audit content

对中国移动 CMCA 的审计包括但不限于以下内容：

- 1、CA 物理环境和控制
- 2、密钥管理操作
- 3、基础 CA 控制
- 4、证书生命周期管理
- 5、CA 业务规则

The regulation audit to CMCA should include::

1. CA physical environment and control
2. Key management operations
3. Basic CA control
4. Certificate lifecycle management
5. CA business rules

## 8.5 对问题与不足采取的措施 Resolution for problems and deficiencies

如果在审计过程中发现执行规范有不足之处，中国移动 CMCA 将根据审计报告的内容准备一份整改方案，并尽快落实解决。

If finding the standard implemented has deficiencies during the audit, CMCA will prepare a rectification plan according to the audit report contents and solve the deficiencies as soon as possible.

## 8.6 评估结果的传达与发布 Communications of results

当CMCA接受行业主管部门的检查或评估后，行业主管部门会向公众发布对CMCA的检查或评估结果。当CMCA接受外部审计机构的审计后，CMCA会在公司网站上公布外部审计结果。当CMCA进行内部审计后，审计结果将只在公司内

部进行传达。

When CMCA is inspected or evaluated by the industry authorities, the industry authorities will release the inspection or evaluation results of CMCA to the public.

When CMCA is audited by an external auditor, CMCA will publish the external audit results on the company's website.

When CMCA conducts internal audit, the audit results will only be communicated within the company.

## 8.7 其他 Other

CMCA 在证书签发期间为严格控制服务质量以及保证对 CP/CPS 及 BR 准则的符合性应至少每季度要进行一次内部审计，随机抽取百分之三（如小于一则抽取一份样本）的样本进行评估。

In order to strictly control the service quality and ensure the compliance with CP/CPS and BR standards, CMCA shall conduct self-audit at least once a quarter during the certificate issuing period, and randomly select 3% (or one sample if less than one) samples for evaluation.

## 9 法律责任和其他业务条款 Legal responsibility and other business terms

### 9.1 费用 Fees

#### 9.1.1 证书签发和更新费用 Certificate fees

根据市场和管理部门的规定，CMCA将收取合理的费用，并在订户向CMCA订购证书时，提前告知证书的签发与更新费用。

According to the regulations of the marketing and management departments, CMCA will charge a reasonable fee and inform the subscriber of the issuing and updating fee of the certificate in advance when ordering the certificate

from CMCA.

### 9.1.2 证书查询费用 Certificate inquiry fee

CMCA 暂不收取此项收费，但保留对此项服务收费的权利。

CMCA does not charge for this service, but reserves the right to charge for this service.

### 9.1.3 证书吊销或状态信息的查询费用 Query fee for certificate revocation or status information

CMCA 暂不收取此项收费，但保留对此项服务收费的权利。

CMCA does not charge for this service, but reserves the right to charge for this service.

### 9.1.4 其他服务费用 Other service charges

CMCA 保留收取其他服务费用的权利。

CMCA reserves the right to charge for other services.

### 9.1.5 退款策略 Refund policy

除非CMCA违背了本CP/CPS所规定的责任与义务，订户可以要求退款。否则，CMCA对订户收取的费用均不退还。

订户应当提供符合CMCA要求的完整、真实、准确的证书申请信息，否则CMCA对此造成的损失和后果不承担任何责任。

Unless CMCA is in breach of its responsibilities and obligations under this CP/CPS, subscriber may request a refund. Otherwise, the fees charged by CMCA to subscribers will not be refunded.

The subscriber shall provide complete, true and accurate certificate application

information that meets the requirements of CMCA, otherwise CMCA will not be responsible for the losses and consequences.

## 9.2 财务责任 Financial responsibility

中国移动 CMCA 及其授权的分支机构应该具有维持其运作和履行其责任的经济能力，应该有能力承担对订户、依赖方等造成的风险。

中国移动 CMCA 每年定期委托公正、客观的第三方进行财务审核。

中国移动 CMCA 对于证书运营服务产生的风险，为了保障客户的权益，将建立财务赔偿基金，用来支付由于证书业务产生的赔偿。

CMCA and its authorized branch shall own the economic ability to maintain its operation and perform its responsibility, and shall have the ability to undertake the risk incurred due to the subscriber, relying party, etc.

CMCA entrusts just and objective third party for financial audit regularly each year.

For the risks incurred for certificate operation service, in order to safeguard customer's rights and benefits, CMCA will establish financial indemnification fund to pay for indemnification incurred for certificate business.

### 9.2.1 保险范围 Insurance coverage

中国移动 CMCA 根据业务发展情况决定其投保策略，包括但不限于：

- 1、建筑物与硬件设施的火灾等意外险；
- 2、证书责任险，保险范围涵盖中国移动 CMCA 证书订户和证书依赖方；
- 3、保险时间为在证书的有效期内。

中国移动 CMCA 在保险范围内仅承担有限责任。

CMCA determines its insurance policies according to the business development condition, including but not limited to:

- 1、The fire hazard of building and hardware facility, and other accident

insurance;

2、Certificate liability insurance, with insurance covering the certificate subscribers of CMCA and certificate relying party;

3、The insurance time is within the effective date of certificate.

CMCA only bears limited liabilities within the insurance scope.

## 9.2.2 其他资产 Other assets

CMCA 确保具有足够的财务实力来维持其正常经营并保证相应义务的履行，并合理地承担对订户及对依赖方的责任。

此要求对证书订户同样适用。

CMCA ensures that it has sufficient financial strength to maintain its normal operation and ensure the performance of corresponding obligations, and reasonably assumes the responsibility to subscribers and relying parties.

The same applies to certificate subscribers.

## 9.2.3 对最终实体的保险或担保 Insurance or guarantee of end entity

如果CMCA根据本CP/CPS或任何法律规定，以及司法判定须承担赔偿责任和/或补偿责任的，CMCA将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

If CMCA is liable for compensation and / or compensation in accordance with this CP/CPS or any laws and judicial decisions, CMCA will be liable for compensation in accordance with relevant laws and regulations, arbitration institutions' decisions or court decisions.

## 9.3 业务信息保密 Business information confidentiality

### 9.3.1 保密信息范围 Confidential information scope

1、CMCA与订户之间的协议、资料中未公开的内容等属于保密信息。除非法律明文规定或政府、执法机关等的要求，CMCA承诺不对外公布或透露订户证书信息以外的任何其它隐私信息。

2、订户私钥属于机密信息，订户应当根据本CP/CPS的规定妥善保管，如因订户自己泄漏私钥造成的损失，订户应自行承担。

1. The agreements, letters and commercial treaties between CMCA and the certificate issuing authority authorized by CMCA, between CMCA and relying party/subscribers, and those between RAs authorized by CMCA and relying party/subscribers shall not be published arbitrarily by one party without the approval of the other party generally, unless expressly specified by laws.
2. The private key of certificate subscribers is confidential, which should be properly kept by certificate subscribers and can't be disclosed to unauthorized third party. The losses caused by disclosure of private key by certificate subscribers shall be borne by the subscribers.

### 9.3.2 不属于保密的信息 Information not within the scope of confidential information

- 1、CA系统签发的证书信息和CRL中的信息。
  - 2、在提供方披露数据和信息之前，已被接受方所持有的数据和信息。
  - 3、在提供方披露数据和信息时或在披露数据和信息之后，非由于接受方的原因而被披露的信息。
  - 4、经公开或通过其他途径成为公众领域的一部分数据和信息。
  - 5、有权披露的第三方披露给接受方的数据和信息。
  - 6、其他可以通过公共、公开渠道获得的信息。
1. Certificate information issued by CA system and information in CRL.
  2. Data and information held by the receiving party prior to the disclosure of



- data and information by the provider.
3. Information disclosed by the provider, or after the disclosure of the data and information, not for the reasons of the recipient.
  4. Become part of the data and information in the public domain, either publicly or through other means.
  5. Data and information disclosed to the receiving party by a third party entitled to disclose.
  6. Other information that can be obtained through public and public channels.

### 9.3.3 保护保密信息 的责任 Responsibility of business information confidentiality

CMCA 有各种严格的管理制度、流程和技术手段来保护机密信息，包括但不限于商业机密、客户信息等。CMCA 的每个员工都要接受信息保密方面的培训。

CMCA has a variety of strict management systems, processes and technical means to protect confidential information, including but not limited to business secrets, customer information, etc. Every employee of CMCA should receive training on information confidentiality.

## 9.4 个人隐私保密 Privacy of individual information

### 9.4.1 隐私保密方案 Privacy plan

客户的个人隐私信息存储于 CA、RA 数据库中，证书的密钥加密存储于数据库中，未经授权无法取得。

CMCA 尊重所有订户和他们的隐私，个人隐私信息保密方案遵守现行法律已经同意接受 CMCA 的隐私保护制度。

Customer's individual privacy information is stored in CA and RA databases, and the certificate private key is stored in database after being encrypted,

which can't be obtained without authorization.

CMCA respects all subscribers and their privacy, and the privacy information confidentiality scheme of individual privacy complies with the existing laws and states that it has agreed to accept the privacy protection system of CMCA.

### 9.4.2 作为隐私处理的信息 Information treated as private

CMCA 在管理和使用订户提供的相关信息时，除了证书中已经包括的信息以及证书状态信息外，该订户的基本信息将被视为隐私处理，这些信息将只能由 CMCA 使用，非经订户同意或有关法律法规、公共权力部门根据合法的程序要求，CMCA 不会任意公开。包括但不限于以下信息：

- 订户的有效身份证号码，如居民身份证号码
- 订户的联系电话
- 订户的通信地址和住址
- 订户的银行账号

When CMCA manages and uses the relevant information provided by the subscriber, in addition to the information already included in the certificate and the status information of the certificate, the basic information of the subscriber will be treated as privacy. This information can only be used by CMCA, and CMCA will not disclose it arbitrarily without the consent of the subscriber or according to the legal procedure requirements of the relevant laws and regulations and public authorities. Including but not limited to the following information:

- Subscriber's valid ID card number, such as resident ID card number
- The contact phone number of the subscriber
- Subscriber's mailing address and residential address
- The subscriber's bank account number

### 9.4.3 不被视为隐私的信息 Information not deemed private

证书内包括的信息以及该证书的状态信息等是可以公开的，将不被视为隐私信息。

The information included in the certificate and the status information of the certificate could be publicized, and wouldn't be regarded as the private information.

### 9.4.4 保护隐私的责任 Responsibility to protect private information

CMCA、注册机构、订户、依赖方等机构或个人都有义务按照本CP/CPS的规定，承担相应的隐私保护责任。在法律法规或公共权力部门通过合法程序要求下，CMCA可以向特定的对象公布隐私信息，CMCA无需承担由此造成的任何责任。

CMCA, registration agencies, subscribers, relying parties and other institutions or individuals are all obliged to undertake corresponding responsibilities on privacy protection in compliance with provisions of this CP/CPS. Under requirements of laws and regulations or public authorities through legal procedures, CMCA can pronounce private information to specific objects, and CMCA does not need to bear any incurring responsibility.

### 9.4.5 使用隐私信息的告知与同意 Notice and Consent to Use Private Information

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

2、订户同意，在任何法律法规或公共权力部门要求下，CMCA向特定对象

披露隐私信息时，CMCA均可以不用告知订户。

1. Subscriber agrees that CMCA may use any subscriber information obtained in the business scope and in accordance with the privacy protection policy stipulated in this CP/CPS, whether it involves privacy or not, CMCA may not inform subscribers.
2. Subscriber agrees that CMCA may not inform subscribers when disclosing privacy information to specific objects, as required by any law, regulation or public authority.

#### **9.4.6 依法律或行政程序的信息披露 Information disclosure in accordance with legal or administrative procedures**

除非符合下列条件，CMCA不会将订户的保密信息提供给其他个人或第三方机构：

- 1、司法、行政部门或其他法律法规授权的部门依据政府法律法规、规章、决定、命令等的规定通过合法授权提出的申请。
- 2、订户采用书面形式的信息披露授权。
- 3、本CP/CPS规定的其他可以披露的情形。

CMCA will not provide subscriber's confidential information to other individuals or third parties unless the following conditions are met:

1. The application filed by the judicial, administrative departments or other departments authorized by laws and regulations through legal authorization in accordance with the provisions of government laws and regulations, rules, decisions, orders, etc.
2. Subscriber's authorization for information disclosure is in writing.
3. Other circumstances that can be disclosed in this CP/CPS.

#### **9.4.7 其他信息披露情形 Other information disclosure**

CMCA、订户、注册机构、依赖方等机构或个人都有义务按照本CP/CPS的规定，承担相应的保护隐私责任。在法律法规或公共权力部门通过合法程序或订

户书面申请授权要求下，CMCA可以向特定的对象公布隐私信息，CMCA无需承担由此造成的任何责任。

CMCA, subscribers, registered institutions, relying parties and other institutions or individuals are obliged to bear the corresponding responsibility for privacy protection in accordance with the provisions of this CP/CPS. CMCA can publish private information to specific objects under the legal procedures or the written authorization requirements of subscribers by laws and regulations or public authority departments, and CMCA does not need to bear any responsibility.

## 9.5 知识产权 Intellectual property rights

CMCA享有并保留对证书以及CMCA提供的全部软件、资料、数据等的著作权、专利申请权等全部知识产权；CMCA制订并发布的CP/CPS、技术支持手册、发布的证书和CRL等的所有权和知识产权均归属于CMCA。

CMCA shall enjoy and retain all intellectual property rights such as copyright, patent application right and other intellectual property rights to certificate and all software, data, data, etc. provided by CMCA; The ownership and intellectual property rights of CP/CPS, technical support manual, issued certificate and CRL formulated and issued by CMCA are all attributed to CMCA.

## 9.6 陈述与担保 Representations and warranties

### 9.6.1 电子认证服务机构的陈述与担保 CA representations and warranties

#### 9.6.1.1 中国移动 CMCA 的责任和义务 Responsibilities and obligations of CMCA

中国移动 CMCA 应承担的唯一和绝对的责任和义务是：

- 保证中国移动 CMCA 机构本身使用和发放的公钥算法在现有通常技术条件下不会被攻破；
- 保证中国移动 CMCA 的签名私钥在中国移动 CMCACSF 内部得到安全的存放和保护；
- 中国移动 CMCA 建立和执行的安全机制符合国家政策的规定；
- 中国移动 CMCA 向证书受益人（订户、应用软件供应方、依赖方）声明及保证，在证书有效期内，CMCA 在签发及管理证书时，已遵守 BR 规定，以及 CMCA 的 CP/CPS。
- 中国移动 CMCA 证书担保在证书业务过程中，对以下信息 进行完整准确的验证，经过验证通过后，才对执行相关证书操作：
  - 1.使用域名或 IP 地址的权利
  - 2.证书授权
  - 3.信息的准确性
  - 4.没有误导信息
  - 5.申请人身份
  - 6.用户协议
  - 7.状态
  - 8.撤销

The sole and absolute responsibility and obligation that CMCA shall bear are:

- Ensure the public key algorithm used and issued by CMCA wouldn't be broken under the existing common technical conditions;
- To ensure secure storage and protection of the signature private key in CMCACSF;
- The security mechanism established and implemented by CMCA complies with the requirements of national policies;
- CMCA declares and warrants to the certificate beneficiary (subscriber, application software supplier and relying party) that during the validity of the certificate, CMCA has complied with BR regulations when

issuing and managing the certificate, as well as CP/CPS of CMCA.

- CMCA certificate guarantee, in the process of certificate business, conducts complete and accurate verification of the following information. After the verification is passed, relevant certificate operation can be performed:
  1. right to use domain name or IP address
  2. Certificate Authorization
  3. accuracy of information
  4. no misleading information
  5. applicant's identity
  6. user agreement
  7. status
  8. cancellation

除上述规定的职责条款，中国移动 CMCA、中国移动 CMCA 的服务机构、中国移动 CMCA 授权的注册机构、中国移动 CMCA 的雇员不承担其它任何义务。必须指出，本认证业务声明的内容，没有任何信息可以暗示或解释成中国移动 CMCA 必须承担其它的义务或中国移动 CMCA 必须对其行为作出其它的承诺。

Except for the above-mentioned terms of responsibility, CMCA, CMCA service organization, registered institution authorized by CMCA and employees of CMCA shall not bear any other obligations. It must be noted that the content of this certification business statement has no information that can imply or explain that CMCA must undertake other obligations or CMCA must make other commitments to its actions.

#### 9.6.1.2 客观意外和不可抗力 Objective accident and force majeure

中国移动 CMCA 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损失、损坏或赔偿责任。这些事件包括劳动纠纷、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。

CMCA doesn't undertake any loss, damage or indemnification responsibility to the operation failure or delay incurred due to objective accident or other force majeure. These events include the labor dispute, intentionally or unintentional behavior of one transaction party, strike, riot, turmoil, war, fire hazard, explosion, earthquake, flood or other catastrophes.

### 9.6.1.3 其他 Others

在第 9.6.1.2 条款所罗列的任何情况下，中国移动 CMCA 由于受到影响，可免除第 9.6.1.1 条款、本 CP/CPS 规定的责任和义务。

由于技术的进步与发展，为保证证书的安全性，中国移动 CMCA 会要求证书订户及时更换证书以保证中国移动 CMCA 能更好地履行 9.6.1.1 条款。

Under any circumstance listed in Article 9.6.1.2, due to being affected, CMCA can be exempted from the responsibilities and obligations specified in Article 9.6.1.1, the CP/CPS.

Due to the progress and development of technology, to ensure the certificate security, CMCA may require certificate subscribers to replace certificate timely, to ensure that CMCA can perform Article 9.6.1.1 in a better way.

## 9.6.2 注册机构的陈述与担保 RA representations and warranties

注册机构必须遵守本认证业务声明的条款，以及《中国移动 CMCA 运营规范》和《中国移动 CMCA RA 管理规范》等规范制度，

注册机构均须遵守并按照鉴证规范在证书签发前严格执行鉴证流程，确保证书签发的准确性和可靠性。

RAs must abide by the CPS terms, as well as the standardizing system of Operations Management Specification of CMCA and Management



Specification of CMCA RA.

RAs must follow and strictly implement the certificate authentication process according to the standard for certificate authentication before the certificate is issued, to ensure the accuracy and reliability of certificate issuing.

### 9.6.3 订户的陈述与担保 **Subscriber representations and warranties**

在签发证书之前，为了 CA 和证书受益人的明确利益，证书订户必须提交纸质的签字和盖章的《CMCA 数字证书申请表》。所有的证书订户一旦提交该项材料，即默认用户同意《中国移动 CMCA 数字证书订户协议》中的所有条款，用户一旦违反订户协议中的条款，将承担因违反条款所带来的后果与责任，包括相应的法律责任。

Before issuing the certificate, for the clear interests of CA and certificate beneficiary, the certificate subscriber must submit the paper signed and sealed CMCA digital certificate application form. Once all certificate subscribers submit this material, it means that the default user agrees to all the terms in CMCA digital certificate subscriber agreement. Once the user violates the terms in the subscriber agreement, he will bear the consequences and responsibilities caused by the violation of the terms, including the corresponding legal liabilities.

证书申请人为 CA 和证书受益人作出承诺和保证。

- 所有的证书订户必须严格遵守关于证书申请以及私钥的所有权和安全保存相关的程序，严格保护证书的密钥；
- 证书订户在证书申请表上或在线填列的所有声明和信息必须是完整、准确和真实的，证书订户对其提交的所有证书申请材料真实性负责，供中国移动 CMCA 或受理点检查和核实；
- 证书签发后，证书订户通过证书申请表上的邮箱接受 CMCA 签发的证书；
- 证书订户保证所申请的证书在合理合法范围内使用，如违规使用，证书

订户承担因此带来的一切问题与责任。

- 证书订户必须严格遵守和服从认证业务声明规定的或者由中国移动 CMCA 推荐使用的安全措施；
- 证书订户需熟悉本认证业务声明的条例和与证书相关的证书政策，还需遵守证书订户证书使用方面的有关限制；
- 一旦发生任何可能导致安全性危机的情况，如证书订户遗失私钥、遗忘或泄密以及其他情况，证书订户应立刻通知中国移动 CMCA 或中国移动 CMCA 授权的注册机构，申请采取挂失、吊销等处理措施；
- 如证书订户需要终止使用证书，应及时向 CA 中心提出申请。

The applicant of the certificate undertakes and guarantees for the Ca and the beneficiary of the certificate.

- All certificate subscribers shall strictly abide by the procedures of ownership and safety savings about the certification application and private key;
- All statements and information filled in the certificate application form or filled online by certificate subscribers must be complete, accurate and true, which are for inspection and verification of CMCA or LRAs;
- After the certificate is issued, the certificate subscriber accepts the certificate issued by CMCA through the email box on the certificate application form;
- The certificate subscriber guarantees that the certificate applied for is used within a reasonable and legal range. If the certificate is used in violation of the regulations, the certificate Subscriber shall bear all the problems and responsibilities arising therefrom;
- Certificate subscribers must strictly follow and obey the security measures specified in the CP/CPS or recommended by CMC;
- Certificate subscribers should be familiar with the regulations of the CP/CPS and certificate policies related to the certificate, and shall follow related restrictions about use of subscriber's certificate;

- In case of any circumstance that may result in security crisis, such as certificate subscriber's losing, forgetting or disclosing private key or other circumstances, the certificate subscriber shall inform CMCA or RAs authorized by CMCA to apply for adopting the disposal measures for reporting the loss of the certificate or revoking the certificate;
- If the subscriber needs to terminate the use of the certificate, he should apply to the CMCA in time.

### 9.6.4 依赖方的陈述与担保 Representations and warranties of relying party

依赖方在信赖中国移动 CMCA 证书的时候, 必须保证遵守和实施以下条款:

- 依赖方熟悉相关的证书政策, 了解证书的使用目的。
- 依赖方在信赖任何 CA 证书前, 必须检查最新的 CRL 以检查证书的状态, 只有确认该证书没有被作废时, 该证书才有效。
- 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这里的有关条例。

The relying party shall promise to follow and implement the following terms when trusting the certificate of CMCA:

- The relying party gets familiar with the relevant certificate policy, and knows the use purpose of the certificate.
- The relying party shall check the latest CRL to inspect the certificate status before trusting any CA certificate. The certificate could be effective only if it isn't cancelled by confirmation.
- All relying parties shall promise their trusts to certificate indicate they promise they know the relevant regulations here.

## 9.6.5 其他参与者的陈述与担保 Representations and warranties of other participants

其他参与者如目录服务提供者、以及其他提供电子认证相关服务的实体需要遵守中国移动 CMCA 的 CP/CPS。

Other participants, such as LDAP serve providers and other entities providing services related to electronic authentication, shall follow the CP/CPS of CMCA.

## 9.7 担保免责 Disclaimers of warranties

如果证书申请人故意或无意地提供不完整、不可靠或已过期的信息，而他又根据正常的流程提供了必须的审核文件，由此得到了中国移动 CMCA 机构签发的数字证书。由此引起的经济纠纷应由申请人全部承担，中国移动 CMCA 不承担与证书内容相关的法律和经济责任，但可以根据受害者的请求提供协查帮助。

In case the certificate applicant intentionally or unintentionally provides the incomplete, unreliable and expired information, but he also provides the necessary review document according to the normal processes, thus obtains the digital certificate issued by CMCA. All economic disputes incurred due to this shall be undertaken by the applicant, and CMCA doesn't undertake legal and economic responsibility related to the certificate consent, but could provide the survey assistance and help according to the request of the victim.

中国移动 CMCA 不承担任何其他未经授权的人或组织以中国移动 CMCA 名义编撰、发表或散布不可信赖的信息所引起的法律责任。

CMCA shall not bear any legal responsibility caused by preparing, publishing or spreading unreliable information by any other unauthorized person or organization in the name of CMCA.

中国移动 CMCA 在法律许可的范围内，根据受害者或法律的要求如实提供电子交易和作业中“不可抵赖”的数字签名依据，但并不对此承担法律责任。

CMCA truthfully provides the "non-repudiation" digital signature basis in the

electronic transaction and operation according to the requirements of victim or laws within the permitted scope of laws, but it doesn't undertake legal responsibility.

中国移动 CMCA 不对任何一方在信赖证书或使用证书过程中引起的直接或间接的损失承担责任。

CMCA doesn't undertake the responsibility to the direct or indirect loss incurred by any party in the certificate trust or usage process.

## 9.8 有限责任 Limited liability

如果 CMCA 根据本 CP/CPS 或任何法律规定，以及司法判定须承担赔偿责任和/或补偿责任的，CMCA 将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

If CMCA is liable for compensation and / or compensation in accordance with this CP/CPS or any laws and judicial decisions, CMCA will be liable for compensation in accordance with relevant laws and regulations, arbitration institutions' decisions or court decisions.

## 9.9 赔偿 Indemnities

1、除非有另外的规定或约定，对于非因本CP/CPS项下的认证服务而导致的任何损失，CMCA不向订户和/或依赖方承担任何赔偿和/或补偿责任。

Unless otherwise specified or agreed, CMCA shall not be liable to the subscriber and / or the relying party for any loss not caused by the certification services under this CP/CPS

2、订户或依赖方进行的民事活动因CMCA提供的认证服务而遭受的损失，CMCA将依据本CP/CPS的相关条款给予相应的赔偿。但无论如何，如果CMCA能够证明其提供的服务是按照《电子签名法》、《电子认证服务管理办法》、CMCA向主管部门备案的CP/CPS实施的，则视为CMCA不具有任何过错，CMCA将不对订户或依赖方承担任何赔偿或补偿责任。

CMCA will make corresponding compensation in accordance with the relevant

provisions of this CP/CPS for the losses suffered by subscribers or relying parties in civil activities due to the certification services provided by CMCA. However, in any case, if CMCA can prove that the services provided by CMCA are implemented in accordance with the electronic signature law, the administrative measures for electronic authentication services and the CP/CPS filed by CMCA with the competent authorities, it shall be deemed that CMCA does not have any fault, and CMCA will not be liable for any compensation or compensation to the subscriber or the relying party.

3、无论本CP/CPS是否有相反或不同规定，就以下损失或损害，CMCA不承担任何赔偿和/或补偿责任：

（1）订户和或依赖方的任何间接损失、直接或间接的利润或收入损失、信誉或商誉损害、任何商机或契机损失、失去项目、以及失去或无法使用任何数据、无法使用任何设备、无法使用任何软件；

（2）由上述第（1）项所述的损失相应生成或附带引起的损失或损害；

（3）非CMCA的行为而导致的损失；

（4）因不可抗力而导致的损失，如罢工、战争、灾害、恶意代码病毒等。

Regardless of the contrary or different provisions of this CP/CPS, CMCA shall not be liable for any compensation and / or compensation for the following losses or damages:

(1) Any indirect loss, direct or indirect loss of profit or revenue, damage to reputation or goodwill, loss of business opportunities or opportunities, loss of project, loss or inability to use any data, equipment or software of subscriber and or relying party;

(2) Loss or damage arising from or incidental to the loss mentioned in (1) above;

(3) Losses caused by non CMCA actions;

(4) Losses caused by force majeure, such as strikes, wars, disasters, malicious code viruses, etc.

4、无论本CP/CPS是否有相反或不同规定，如果CMCA根据本CP/CPS或任何法律规定，以及司法判定须承担赔偿责任和/或补偿责任的，CMCA将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

If CMCA is subject to this CP/CPS or any law, whether or not this CP/CPS is otherwise or not specified CMCA will be liable for compensation in accordance

with the relevant laws and regulations, the arbitration agency's decision or the court judgment if the law stipulates that the judicial judgment shall bear the liability for compensation and / or compensation.

## 9.10 有效期限与终止 Term and termination

### 9.10.1 有效期限 Term of validity

本 CP/CPS 自发布之日起正式生效，上一版本的 CP/CPS 同时失效；本 CP/CPS 在下一版本 CP/CPS 生效之日或在 CMCA 终止电子认证服务时失效。This CP/CPS shall come into effect on the date of issue, and the CP/CPS of the previous version shall be invalid at the same time; This CP/CPS shall become invalid on the effective date of the next version of CP/CPS or when CMCA terminates the electronic authentication service.

### 9.10.2 终止 Termination

CMCA 终止电子认证服务时，本 CP/CPS 终止。  
When CMCA terminates the electronic authentication service, this CP/CPS will terminate.

### 9.10.3 效力的终止与保留 Termination and reservation of validity

本 CP/CPS 终止后，其效力将同时终止，CP/CPS 中的内容将视为无效使用，但对终止之日前发生的法律事实，本 CP/CPS 中对各方责任的规定及责任免除仍然适用。

After the termination of this CP/CPS, its effect will be terminated at the same time, and the contents in the CP/CPS will be regarded as invalid use. However, for the legal facts occurring before the date of termination, the provisions of



this CP/CPS on the liability of all parties and the exemption of liability still apply.

## 9.11 对参与者的个别通告与沟通 Individual notification and communication to participants

参与者如需要进一步了解任何本 CP/CPS 中提及的服务、规范、操作等信息，可以通过网站或者邮件联系 CMCA。

联系网站: [www.cmca.net](http://www.cmca.net)

联系邮箱: [cmca@aspirecn.com](mailto:cmca@aspirecn.com)

If participants need to know more about any service, specification, operation and other information mentioned in this CP/CPS, they can contact CMCA through website or email.

Contact website: [www.cmca.net](http://www.cmca.net)

Contact email: [cmca@aspirecn.com](mailto:cmca@aspirecn.com)

## 9.12 修订 Amendments

### 9.12.1 修订程序 Revision procedure

修订程序与本 CP/CPS1.5.4“CPS 批准程序”相同。

The revision procedure is the same as cps1.5.4 "CPS approval procedure".

### 9.12.2 通知机制和期限 Notification mechanism and time limit

修订后的 CP/CPS 经批准后将立即在 CMCA 的网站 [www.cmca.net](http://www.cmca.net) 上发布。

The revised CP/CPS will be published on CMCA's website ([www.cmca.net](http://www.cmca.net)) as



soon as it is approved.

### **9.12.3 必须修改业务规则的情形 Situations where business rules have to be modified**

CMCA 必须对本 CP/CPS 进行修改的情形包括：CP/CPS 中相关内容与管辖法律的不一致，国家监管部门对本机构认证业务有明确的更改或调整要求等。

The situations that CMCA must modify this CP/CPS include: the inconsistency between the relevant contents of CP/CPS and the governing laws, and the clear requirements of the national regulatory authorities for the change or adjustment of the certification business of CMCA.

### **9.13 争议处理 Dispute resolution**

若本证书策略及认证业务声明的规定与其他规定、指导方针相互抵触，客户必须接受本证书策略及认证业务声明的约束。

凡因本认证业务声明引起的或与本证书策略及认证业务声明有关的一切争议，当事人均同意由卓望数码技术（深圳）有限公司注册地所在人民法院管辖。

In case the provisions in this CP/ mutually contradict with other provisions and guideline, the customer shall receive the constraint stated in the CP/CPS.

For all disputes incurred by this CP/CPS or related to this CP/CPS, all parties consent the local People's Court of ASPIRE TECHNOLOGIES (SHENZHEN) LTD. to administer.

### **9.14 管辖法律 Governing laws**

本证书策略及认证业务声明在各方面服从中华人民共和国电子签名法的管制和解释。

This CP/CPS is subject to the control and explanation of Law of Electronic

Signature of the People's Republic of China in all aspects.

## 9.15 适用法律的符合性 Applicable laws

无论合同或其他法律条款的选择及无论是否在中国建立商业关系，中国移动 CMCA 认证业务声明的执行、解释、翻译和有效性均适用中华人民共和国的法律。

法律的选择是确保对所有客户有统一的程序和解释，而不管他们在何地居住以及在何处使用证书。

The implementation, interpretation, translation and validity of CMCA certification business statement shall be governed by the laws of the People's Republic of China regardless of the choice of contract or other legal terms and whether or not a business relationship is established in China.

The choice of law is to ensure that there is a uniform procedure and interpretation for all customers, regardless of where they live and where they use certificates.

## 9.16 一般条款 General terms

### 9.16.1 完整协议 Entire agreement

本协议和附件构成双方就所涉事项达成的全部理解和同意，并取代所有双方先前达成的暂行协议或谅解备忘录。

The agreement and appendixes shall constitute complete understanding and consent between both parties with respect to the matters concerned, and shall supersede all temporary agreements or memorandum of understanding between them prior to the effective date of the agreement.

## 9.16.2 转让 Assignment

无论是各方明示的或暗示的继任者、执行者、继承者、代表、管理者和受让人，中国移动 CMCA 的 CP/CPS 均保证其权益，并对其有约束力。各方可根据法律转让（包括合并或转让可控有价证券）中国移动 CMCA 的 CP/CPS 详述的权利和义务。

For any of successor, performer, heir, representative, manager or assignee expressed or implied by either party, the CP/CPS of CMCA will ensure their rights and benefits and bind on them. Either party may transfer (including merger or transferring controllable securities) the rights and obligations specifically described in the CP/CPS of CMCA according to laws.

## 9.16.3 分割性 Segmentation

中国移动 CMCA 的 CP/CPS 的任何条款或其应用，如果因为任何原因或在任何范围内发现无效或不能执行，那么 CP/CPS 其余的部分（以及对它方的无效或不能执行的条款的适用）将会做出合理的解释以反映当事人的原意。相关当事人了解并同意，中国移动 CMCA 的 CP/CPS 所规定的责任限制、保证或其它免责条款或限制、或损害赔偿的排除等，系可独立于其它条款的个别条款，并可加以执行。

In case any terms of CP/CPS or its applications of CMCA are invalid or couldn't be implemented due to any reason or within any scope, the residual part (and the serviceability of invalid or unexecutable terms of other parties) of CP/CPS would make reasonable explanation to reflect the original intention of the party. The relevant parties know and agree that the responsibility limitation as regulated in the CP/CPS of CMCA, guarantee, or other exceptions or limitation, or elimination of damages is the individual term which could be independent of other terms and could be implemented.

## 9.16.4 强制执行 Enforcement

CMCA 声明，证书订户、依赖方等必须执行 CMCA 的 CP/CPS 中的所有

规定。若证书订户、依赖方等实体未执行 CMCA 的 CP/CPS 中某项规定，不被认为该实体将来不执行该项或其他规定。

CMCA states that certificate subscribers, relying parties, etc. must implement all the provisions in CP/CPS of CMCA. If the certificate subscriber, relying party and other entities do not implement a provision of CP/CPS of CMCA, it is not considered that the entity will not implement this or other provisions in the future.

### 9.16.5 不可抗力 Force majeure

中国移动 CMCA 和发证机构将不对以下超越它们控制能力的事件所造成中国移动 CMCA 的 CP/CPS 规定的担保责任违反、延误或无法履行负责。不可抗力一般包括劳动纠纷、交易一方故意或无意的行为、罢工、暴动、瘟疫、骚动、战争、断电、火灾、爆炸、地震、水灾或其他大灾难等。

CMCA and certifying authority shall not be responsible for the violation, delay or failure of fulfillment of guarantee liability specified in the CP/CPS of CMCA caused by the following force majeure events. The force majeure generally includes the labor dispute, intentionally or unintentional behavior of one transaction party, strike, riot, pestilence, turmoil, war, outage, fire hazard, explosion, earthquake, flood or other catastrophes.

### 9.17 其他条款 Other terms

中国移动 CMCA 与具体客户协商后另行确定其他条款，包括未在上述说明的其他相关内容条款。

CMCA could separately confirm other terms after negotiation with the specific customers, including other relevant content terms instructed in the above.

## 附录：证书信息

**Appendix: Certificate information**

Root/CA Certificate	Information
CMCA GLOBAL TRUST ROOT CA	Country=CN Organization= Aspire Technologies Common Name= CMCA GLOBAL TRUST ROOT CA Serial Number= 00 bf 7a bd c8 e5 f6 95 94 f4 13 b1 9d Validity= October 16, 2020 to October 16, 2045 SHA1digest= 4d fb 89 9c 98 4f 20 ac b1 63 29 7e b9 16 0d 8b 3b 53 3a ba
CMCA EV SSL CA	Country=CN Organization= Aspire Technologies Common Name= CMCA EV SSL CA Serial Number= 00 d5 71 ab 1b 6a c6 99 ae fd 36 0d b3 Validity= October 16, 2020 to October 16, 2040 SHA1digest= f3 71 64 b9 70 2f 60 ff 0f f7 ee 4d ea 1d 7d 3d 73 5d 75 bf
CMCA SSL CA	Country=CN Organization= Aspire Technologies Common Name= CMCA SSL CA Serial Number= 00 ad 4e 06 ab 7f 62 44 26 c1 47 46 2d Validity= October 16, 2020 to October 16, 2040 SHA1digest= 63 0a 44 b1 7c cc 4a 1d 63 36 d5 61 a4 a5 af 00 0b f7 d8 5d