广东数字证书认证中心有限公司

证书策略

版本：V1.0 **生效日期：2010 年 1 月 1 日**

目 录

一、 引言 1

1.1 本项说明 1

1.2 概述 1

1.2.1 GDCA 架构 2

1.2.2 GDCA 证书层次架构 2

1.3 文档名称与标识 2

1.4 PKI 参与者 2

1.4.1 电子认证服务机构 2

1.4.2 注册机构 3

1.4.3 订户 3

1.4.4 依赖方 3

1.4.5 其他参与者 3

1.5 证书应用 4

1.5.1 适合的应用 4

1.5.1.1 个人类证书 4

1.5.1.2 机构类证书 4

1.5.1.3 设备类证书 5

1.5.2 限制的证书应用 5

1.6 策略管理 5

1.6.1 策略文档管理机构 5

1.6.2 联系人 5

1.6.3 决定 CP 符合策略的机构 5

1.6.4 CP 批准程序 6

1.7 定义和缩写 6

1.7.1 术语定义一览表 6

1.7.2 缩略语及其含义一览表 7

二、 发布与信息库责任 8

2.1 信息库 8

2.2 认证信息的发布 8

2.3 发布的时间和频率 8

2.4 信息库访问控制 8

三、 身份标识与鉴别 9

3.1 命名 9

3.1.1 命名类型 9
3.1.2 对命名有意义的要求 9
3.1.3 订户的匿名或伪名 9
3.1.4 解释不同命名的规则 9
3.1.5 命名的唯一性 9
3.1.6 商标的识别、鉴别与角色 9
3.2 初始身份确认 9
3.2.1 证明拥有私钥的方法 9
3.2.2 机构身份的鉴别 10
3.2.3 个人身份的鉴别 10
3.2.4 设备身份的鉴别 10
3.2.5 没有验证的订户信息 11
3.2.6 授权确认 11
3.2.7 互操作准则 11
3.3 密钥更新请求的标识与鉴别 11
3.3.1 常规密钥更新的标识与鉴别 11
3.3.2 吊销后密钥更新的标识与鉴别 11
3.4 吊销请求的标识与鉴别 12
四、 证书生命周期操作要求 13
4.1 证书申请 13
4.1.1 证书申请实体 13
4.1.2 注册过程与责任 13
4.2 证书申请处理 14
4.2.1 执行识别与鉴别 14
4.2.2 证书申请批准和拒绝 14
4.2.2.1 证书申请的批准 14
4.2.2.2 证书申请的拒绝 14
4.2.3 处理证书申请的时间 15
4.3 证书签发 15
4.3.1 证书签发中 RA 和 CA 的行为 15
4.3.2 CA 和 RA 通知订户证书的签发 15
4.4 证书接受 15
4.4.1 构成接受证书的行为 15
4.4.2 CA 对证书的发布 15
4.4.3 CA 通知其他实体证书的签发 15
4.5 密钥对和证书的使用 16
4.5.1 订户私钥和证书的使用 16
4.5.2 依赖方公钥和证书的使用 16
4.6 证书更新 16

4.6.1 证书更新的情形.....16
4.6.2 请求证书更新的实体.....16
4.6.3 处理证书更新请求.....16
4.6.4 通知订户新证书的签发.....17
4.6.5 构成接受更新证书的行为.....17
4.6.6 CA 对更新证书的发布.....17
4.6.7 CA 通知其他实体证书的签发.....17
4.7 证书密钥更新.....17
4.7.1 证书密钥更新的情形.....17
4.7.2 请求证书密钥更新的实体.....18
4.7.3 处理证书密钥更新请求.....18
4.7.4 通知订户新证书的签发.....18
4.7.5 构成接受密钥更新证书的行为.....18
4.7.6 CA 对密钥更新证书的发布.....18
4.7.7 CA 通知其他实体证书的签发.....18
4.8 证书变更.....18
4.8.1 证书变更的情形.....18
4.8.2 请求证书变更的实体.....18
4.8.3 处理证书变更请求.....19
4.8.4 通知订户新证书的签发.....19
4.8.5 构成接受变更证书的行为.....19
4.8.6 CA 对变更证书的发布.....19
4.8.7 CA 通知其他实体证书的签发.....19
4.9 证书吊销和挂起.....19
4.9.1 证书吊销的情形.....19
4.9.2 请求证书吊销的实体.....19
4.9.3 证书吊销请求的处理程序.....20
4.9.3.1 订户请求吊销证书.....20
4.9.3.2 订户被强制吊销证书.....20
4.9.4 吊销请求的宽限期.....20
4.9.5 CA 处理吊销请求的时限.....20
4.9.6 依赖方检查证书吊销的要求.....20
4.9.7 CRL 发布频率.....20
4.9.8 CRL 发布的最大滞后时间.....21
4.9.9 在线状态查询的可用性.....21
4.9.10 在线状态查询要求.....21
4.9.11 吊销信息的其他发布形式.....21
4.9.12 密钥损害的特别要求.....21
4.9.13 证书挂起的情形.....21
4.9.14 请求证书挂起的实体.....22
4.9.15 挂起请求的程序.....22
4.9.16 挂起的期限限制.....22
4.10 证书状态服务.....22

4.10.1 操作特征 22
4.10.2 服务可用性 22
4.10.3 可选特征 22
4.11 订购结束 23
4.12 密钥托管与恢复 23
4.12.1 密钥托管与恢复的策略与行为 23
4.12.2 会话密钥的封装与恢复的策略与行为 23
五、 认证机构设施、管理和操作控制 24
5.1 物理控制 24
5.1.1 场地位置与建筑 24
5.1.2 物理访问控制 24
5.1.3 电力与空调 24
5.1.4 防水 24
5.1.5 火灾防护 24
5.1.6 介质存放 25
5.1.7 废物处理 25
5.1.8 异地备份 25
5.2 程序控制 25
5.2.1 可信角色 25
5.2.2 每项任务需要的人数 25
5.2.3 每个角色的识别与鉴别 26
5.2.4 需要职责分割的角色 26
5.3 人员控制 26
5.3.1 资格、经历和清白要求 26
5.3.2 背景调查程序 26
5.3.3 培训要求 27
5.3.4 再培训的频度和要求 27
5.3.5 工作岗位轮换的频度和次序 28
5.3.6 未授权行为的处罚 28
5.3.7 独立合约人的要求 28
5.3.8 提供给人员的文件 28
5.4 审计记录程序 28
5.4.1 记录事件的类型 28
5.4.2 处理日志的频度 29
5.4.3 审计日志的保留期限 29
5.4.4 审计日志的保护 29
5.4.5 审计日志的备份程序 29
5.4.6 审计收集系统 29
5.4.7 对导致事件主体的通知 29
5.4.8 脆弱性评估 29

5.5 记录归档 30
5.5.1 归档记录的类型 30
5.5.2 归档记录的保留期限 30
5.5.3 归档文件的保护 30
5.5.4 归档文件的备份程序 30
5.5.5 记录时间戳要求 30
5.5.6 归档收集系统 30
5.5.7 获得和检验归档信息的程序 30
5.6 密钥变更 31
5.7 损害与灾难恢复 31
5.7.1 事故和损害处理程序 31
5.7.2 计算机资源、软件和/或数据的损坏 31
5.7.3 实体私钥损害处理程序 31
5.7.4 灾难后的业务存续能力 32
5.8 CA 或 RA 的终止 32
六、 认证系统技术安全控制 34
6.1 密钥对的生成与安装 34
6.1.1 密钥对的生成 34
6.1.1.1 CA 密钥对生成 34
6.1.1.2 订户签名密钥对生成 34
6.1.1.3 订户加密密钥对生成 34
6.1.2 加密私钥传送给订户 34
6.1.3 公钥传送给证书签发机构 35
6.1.4 CA 公钥传送给依赖方 35
6.1.5 密钥的长度 35
6.1.6 公钥参数的生成和质量检查 35
6.1.7 密钥使用目的 35
6.2 私钥保护和密码模块工程控制 36
6.2.1 密码模块的标准和控制 36
6.2.2 私钥多人控制（m 选 n） 36
6.2.3 私钥备份 36
6.2.4 私钥归档 36
6.2.5 私钥导出、导入密码模块 37
6.2.6 私钥在密码模块的存储 37
6.2.7 激活私钥的方法 37
6.2.8 冻结私钥的方法 37
6.2.9 销毁私钥的方法 37
6.2.10 密码模块的评估 38
6.3 密钥对管理的其他方面 38
6.3.1 公钥归档 38

6.3.2 证书操作期和密钥对使用期限.....38
6.4 激活数据.....39
6.4.1 激活数据的产生和安装.....39
6.4.2 激活数据的保护.....39
6.4.3 激活数据的其他方面.....39
6.5 计算机安全控制.....39
6.5.1 特别的计算机安全技术要求.....39
6.5.2 计算机安全评估.....40
6.6 生命周期技术控制.....40
6.6.1 系统开发控制.....40
6.6.2 安全管理控制.....40
6.6.3 生命周期的安全控制.....41
6.7 网络的安全控制.....41
七、 证书、证书吊销列表和在线证书状态协议.....42
7.1 证书描述.....42
7.1.1 版本号.....42
7.1.2 证书扩展项.....42
7.1.2.1 标准扩展项.....42
7.1.2.2 自定义扩展项.....43
7.1.3 算法对象标识符.....44
7.1.4 名称形式.....44
7.1.5 名称限制.....45
7.1.6 证书策略对象标识符.....45
7.1.7 策略限制扩展项的用法.....45
7.1.8 策略限定符的语法和语义.....45
7.1.9 关键证书策略扩展项的处理语义.....45
7.2 证书吊销列表.....45
7.2.1 版本.....46
7.2.2 CRL 和 CRL 条目扩展项.....46
7.3 OCSP 描述.....46
7.3.1 版本号.....46
7.3.2 OCSP 扩展项.....46
八、 认证机构审计和其他评估.....47
8.1 评估的频度和情形.....47
8.2 评估者的身份/资格.....47
8.3 评估者与被评估者之间的关系.....47
8.4 评估的内容.....47

8.5 对问题与不足采取的行动 47
8.6 评估结果的传达与发布 48
8.7 其他评估 48
九、 法律责任和其他业务条款 49
9.1 费用 49
9.2 财务责任 49
9.2.1 保险范围 49
9.2.2 其他财产 49
9.2.3 对最终实体的保险或担保范围 49
9.3 业务信息保密 49
9.3.1 保密信息范围 49
9.3.2 不属于保密的信息 50
9.3.3 保护保密信息的责任 50
9.4 个人隐私保密 50
9.4.1 隐私保密计划 50
9.4.2 作为隐私处理的信息 50
9.4.3 不被认为隐私的信息 51
9.4.4 保护隐私的责任 51
9.4.5 使用隐私信息的告知与同意 51
9.4.6 依法律或行政程序的信息披露 51
9.4.7 其他信息披露情形 52
9.5 知识产权 52
9.6 陈述与担保 52
9.6.1 CA 的陈述与担保 52
9.6.2 RA 的陈述与担保 53
9.6.3 订户的陈述与担保 53
9.6.4 依赖方的陈述与担保 53
9.6.5 其他参与者的陈述与担保 53
9.7 担保免责 54
9.8 有限责任 54
9.9 赔偿 54
9.9.1 认证机构的赔偿责任 54
9.9.2 订户的赔偿责任 55
9.9.3 依赖方的赔偿责任 55
9.10 有效期与终止 55
9.10.1 有效期 55
9.10.2 终止 55

9.10.3 终止的效果与存续.....55
9.11 对参与者的个别通告及信息交互.....56
9.12 修订.....56
9.12.1 修订程序.....56
9.12.2 通知机制和期限.....56
9.12.3 必须修订的情形.....56
9.13 争议解决条款.....56
9.14 管辖法律.....57
9.15 符合适用法律.....57
9.16 一般条款.....57
9.16.1 完整协议.....57
9.16.2 让渡.....57
9.16.3 分割性.....57
9.16.4 强制执行.....57
9.16.5 不可抗力.....58
9.17 其他条款.....58

一、 引言

1.1 本项说明

广东数字证书认证中心有限公司（GUANG DONG CERTIFICATE AUTHORITY CO., LTD），是广东省数字证书认证中心暨广东省电子政务认证中心的企业化运作实体，简称 GDCA。GDCA 经广东省信息产业厅批准于 2002 年开始从事电子认证服务，公司注册成立于 2003 年，2005 年 9 月 6 日依法通过了信息产业部的资质审查，成为全国首批八家获得《电子认证服务许可证》的电子认证服务机构之一。

本文件描述 GDCA 的证书策略（CP），是 GDCA 数字证书服务的策略声明，适用于所有由 GDCA 签发和管理的数字证书及相关参与主体。为批准、签发、管理、使用、吊销和更新证书和相关的可信服务制定业务、法律和技术上的要求和规范。这些规范保护 GDCA 证书服务的安全性和完整性，包含一整套在 GDCA 范围内一致适用的单一规则集，因此在整个 GDCA 架构内能够提供同样的信任担保。本 CP 并不是 GDCA 和各参与方之间的法律性协议，GDCA 和各参与方之间的权利义务依靠他们之间签署的各类协议构成。

本 CP 满足“互联网 X.509 公开密钥基础设施证书策略和证书业务框架”（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework），即由互联网标准组织“互联网工程工作组”（Internet Engineering Task Force）制定的 RFC3647 标准的结构和内容要求，并根据中国的法律法规和 GDCA 的运营要求进行适当的改变。

1.2 概述

本 CP 作为最高策略，为整个 GDCA 内的证书提供管理、操作和规范的依据，以及为 GDCA 各参与方的权利义务关系确定一个限制范围和基本条款。本 CP 制定了 GDCA 所有证书和相关服务的操作流程框架，以及为安全、完整地实施这些流程所应该采取的业务、技术和法律方面的要求。

GDCA 作为一个证书服务机构（CA），在本 CP 的约束下生成根证书和 CA 证书，签发订户证书。基于不同的类型和应用范围，作为证书持有人的订户可以使用证书进行网络站点安全保护、代码签名、邮件签名、文档签名、身份认证等不同的应用。依

赖方依照本 CP 中关于依赖方的义务要求，决定是否信任一张证书。GDCA 的电子认证业务规则（CPS）接受本 CP 的约束，详细阐述了 GDCA 作为电子认证服务机构提供的证书、如何提供证书以及相应的管理、操作和保障措施。所有 GDCA 证书的订户及依赖方必须参照本 CP 及相关 CPS 的规定，决定对证书的使用和信任。

1.2.1 GDCA 架构

本 CP 是 GDCA 最高的策略，GDCA 的证书服务机构（CA）按照 CP 制定 CPS，RA 按照本 CP 及相关 CPS 进行证书服务申请鉴别，订户、依赖方及其他相关实体按照本 CP 及相关 CPS 决定对证书的使用、信任并履行相关的义务。GDCA 包含了根 CA、子 CA，各相关注册机构，分中心，这些实体都是 GDCA 认证体系内不同层次的服务主体。

1.2.2 GDCA 证书层次架构

GDCA 目前有 2 个根证书，分别为 1024-bit 密钥长度和 2048-bit 密钥长度，均为自签名根证书，由 GDCA 管理和运营。每个根 CA 下设子 CA，以签发用户证书。

1.3 文档名称与标识

本文档称作《广东数字证书认证中心有限公司证书策略》（简称《GDCA CP》）。GDCA 为其注册分配了对象标识符为：1.2.156.112559.1.1.1.1。

1.4 PKI 参与者

1.4.1 电子认证服务机构

电子认证服务机构（Certification Authority，简称 CA）是颁发证书的实体。GDCA 是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，依法设立的第三方电子认证服务机构。GDCA 通过给从事电子交易活动的各方主体颁发数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。CA 是向最终订户或其下 CA 签发证书的实体的术语，它的一个特例是根 CA，一个根 CA 是一类证书体系的最高层。

1.4.2 注册机构

注册机构（Registration Authority，简称 RA）代表 CA 建立起注册过程，确认证书申请者的身份，批准或拒绝证书申请者。在订户获得证书前，它必须以申请者的身份来注册证书。证书申请者必须从 CA 或 RA 建立的注册过程来完成注册，并将注册信息提交给 CA 或 RA。CA 或 RA 将对申请者的身份及其它属性进行确认，然后决定是签发还是拒绝该请求。如果签发证书，则证书将被发送给申请者。RA 还可以根据订户需要吊销证书，尽管是 CA 完成最终的吊销工作，并将证书加入到证书吊销列表(CRL)中。

1.4.3 订户

订户，即从 CA 接收证书的实体，包括所有接受 GDCA 证书的个人、单位。订户和申请人很多时候并不一致，如果订户和申请人不一致，则需要申请人保证获得明确、适当的授权。个人又分为自然人和从属于某一个单位的个人；单位包括各类政府组织、企事业单位和其它社会团体，一般而言，单位应该具有法人资格或者组织机构代码证号码；对于设备类证书，由于证书中包含主体的特殊性，订户通常应被理解为拥有该设备的单位或者个人，并由拥有该设备的单位或者个人承担相应的义务。

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

1.4.4 依赖方

依赖方是指信任证书、使用证书的个人和单位。依赖方可以是证书订户，也可以不是证书订户。

要信任或者使用一张证书，依赖方必须验证证书的吊销信息，包括证书吊销列表（CRL），使用 OCSP 方式查询证书状态。依赖方必须经过合理的审核后才能够信任一张证书。

1.4.5 其他参与者

其他参与者是指为 GDCA 的电子认证活动提供相关服务的其他实体。

1.5 证书应用

1.5.1 适合的应用

GDCA 的订户证书是通用证书，按照证书类型的不同，都有适用的应用。例如个人证书用来发送签名加密邮件、登陆办公 OA 系统等，机构证书用来进行网上申报税等，设备证书用来标识设备身份、进行信息通道加密等。除了因为证书标识的主体身份的不同而导致证书应用差异外，GDCA 订户证书可以广泛应用在电子政务、电子商务及其他应用，以实现身份认证、电子签名、关键数据加密等目的。

GDCA 订户证书，从功能上可以满足下列安全需要：

- 身份认证，保证采用 GDCA 信任服务的证书持有者身份的合法性。
- 验证信息完整性，保证采用 GDCA 数字证书和数字签名时，可以验证信息在传递过程中是否被篡改，发送和接收的信息是否一致。
- 信息的机密性，机密性保证传送方和接收方信息的机密，不会泄露给其它未合法授权方。
- 验证数字签名，对信任体交易不可抵赖性的依据即数字签名进行验证。

订户可以根据实际需要，自主判断和决定采用相应合适的证书类型，不同的证书具有不同的应用范围。

1.5.1.1 个人类证书

颁发给个人的数字证书，个人包括自然人或特定身份的人员，如公务员、企业员工等。此类证书通常用于数字签名、加解密、安全电子邮件以及网上身份认证；

1.5.1.2 机构类证书

颁发给机构的数字证书，机构包括企事业单位、政府机关、社会团体等。此类证书又分为组织机构证书和机构业务证书。

- 组织机构证书：适用于各类应用，包括但不限于代表机构签订文件、合同、协议、网上交易等，提供高等担保级别的保证。还适用于客户端的鉴别，可以提供诸如网站的访问控制，以及提供电子邮件的签名加密。
- 机构业务证书：适用于特定的应用，为机构在特定应用系统中提供数字签名、加解密、安全电子邮件以及网上身份认证。

1.5.1.3 设备类证书

即颁发给设备的数字证书，设备包括服务器、防火墙、路由器等，此类证书通常用于网上设备的身份认证，设备之间安全信息的传递。例如，给服务器颁发的证书使浏览器可以鉴别网站服务器的身份，并创建 SSL 加密通道以使双方进行加密会话。

1.5.2 限制的证书应用

一般而言，GDCA 证书是一般性目的的证书，可以和不同的依赖方之间相互操作。尽管如此，GDCA 证书在功能上是受到限制的，如个人证书只能用于个人用户的应用，而不能作为服务器或组织机构证书使用。

证书不设计用于、不打算用于、也不授权用于危险环境中的控制设备，或用于要求防失败的场合，如核设备的操作、航天飞机的导航或通讯系统、空中交通控制系统或武器控制系统中，因为它的任何故障都可能导致死亡、人员伤害或严重的环境破坏。

证书禁止在任何违反国家法律、法规或破坏国家安全的情形下使用，否则由此造成的法律后果由用户自己承担。

1.6 策略管理

1.6.1 策略文档管理机构

策略文档管理机构为 GDCA 行政管理部门。

1.6.2 联系人

联系人：GDCA 行政管理部门

邮件地址：GDCA@gdca.com.cn

联系电话：020-83487228

传真：020-83486610

1.6.3 决定 CP 符合策略的机构

本 CP 由 GDCA 技术与运营策略委员会批准，包括本 CP 的修订和版本变更。

GDCA 技术与运营策略委员会负责评估 GDCA 的 CPS 是否符合本 CP，是批准和

决定 GDCA 的 CPS 是否与本 CP 相适应的机构。

1.6.4 CP 批准程序

本 CP 由 GDCA 技术与运营策略委员会主任及委员会常务秘书组织相关人员拟定文档，提交 GDCA 技术与运营策略委员会批准审核。经该委员会批准后，GDCA 根据《电子认证服务管理办法》中规定，在自公布之日起的三十日之内向工业和信息化部备案。

1.7 定义和缩写

1.7.1 术语定义一览表

术　　语	定　　义
电子认证服务机构（CA）	一个授权签发、管理、吊销和更新证书的权威机构。
证书策略（CP）	一套命名的规则集，用以指明证书对一个特定团体或者具有相同安全需求的应用类型的适用性。例如，一个特定的 CP 可以指明某类证书适用于鉴别从事企业到企业交易活动的参与方，针对给定价格范围内的产品和服务。
认证路径（Certification Path）	一个有序的证书序列（包含路径中起始对象的公钥），通过处理该序列可获得末端对象的公钥。
参与者（Participant）	在一个给定 PKI 中扮演某一角色的个人或组织，如订户、依赖方、CA、RA、证书制作机构、证书库服务提供者、或类似实体。
策略限定符（Policy qualifier）	依赖于策略的信息，可能与 CP 标识符共同出现在 X.509 证书中。该信息可能包含可用 CPS 或依赖方协议的 URL 地址，也可能包含证书使用条款的文字。
依赖方（Relying party）	证书的接收者，他依赖于该证书和该证书所验证的数字签名。
依赖方协议（Relying party agreement）	证书认证机构与依赖方说签署的协议，通常规定了在验证数字签名或其他使用证书的过程中有关方所拥有的权利和义务。
订户（subscriber）	被颁发给一张证书的证书主体。
订户协议（subscriber agreement）	CA 与订户之间签署的协议，规定了双方在颁发核管理证书的过程中所拥有的权利和义务。
激活数据（Activation Data）	用于操作密码模块所必需的、并且需要被保护的非密钥数据值（例如：PIN、

	口令或人工控制的密钥共享部分）
鉴别（authentication）	确定个人、组织或事物如其所声称的个人、组织或事物的过程。在 PKI 上下文中，鉴别指的是证实以某个特定名称申请或试图访问某事物的个人或组织确实为真实的个人或组织的过程。
认证业务声明（certification practice statement）	证书认证机构在签发、管理、撤销或更新证书、密钥过程中所采纳的业务实践的通告。

1.7.2 缩略语及其含义一览表

GDCA	Guang Dong Certificate Authority	广东省数字证书认证中心
CA	Certificate Authority	电子认证服务机构
KM	Key Management Center	密钥管理中心
RA	Registration Authority	注册审核服务机构
LRA	Local Registration Authority	本地注册受理点
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
CP	Certification Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
CRL	Certificate Rovoke List	证书撤消列表
OCSP	Online Certificate Status Protocol	在线证书状态协议
PIN	Personal Indentification Number	个人身份识别码
PKCS	Public KEY Cryptography Standards	公共密钥密码标准
PKI	Public Key Infrastructure	公共密钥基础设施
RFC	Request For Comments	请求评注标准(一种互联网建议标准)

二、 发布与信息库责任

2.1 信息库

GDCA 的电子认证信息库应包括以下内容：证书策略（CP）、电子认证业务规则（CPS）、证书和证书吊销列表（CRL）。

2.2 认证信息的发布

GDCA 通过网站 http://www.gdca.com.cn 公布《GDCA 证书策略》、《GDCA 电子认证业务规则》，供相关方查阅。

GDCA 通过目录服务器发布订户的证书和证书吊销列表（CRL），订户或依赖方可以通过访问 GDCA 的目录服务器获取证书的信息和证书吊销列表。同时，GDCA 提供 OCSP（在线证书状态查询），OCSP 作为 CRL 的有效补充，方便证书订户及时查询证书状态信息。

2.3 发布的时间和频率

《GDCA 证书策略》、《GDCA 电子认证业务规则》自公布之日起的 15 天之后正式生效。GDCA 签发证书后立即将该证书发布到目录服务器。GDCA 的 CRL 发布周期为 24 小时，即在 24 小时内发布最新 CRL。

2.4 信息库访问控制

GDCA 信息库中的信息是对外公开发布的，任何人都能够查阅，对这些信息的只读访问不受任何限制。

GDCA 采取措施限制对信息库进行任何未经授权的增加、删除、修改等操作。

三、 身份标识与鉴别

3.1 命名

3.1.1 命名类型

GDCA 签发的数字证书符合 X.509 标准，分配给证书持有者的主体甄别名，采用 X.500 命名方式。

3.1.2 对命名有意义的要求

订户证书所包含的命名应具有一定的代表性意义，可以确定证书主题中的个人、机构或者设备的身份。

3.1.3 订户的匿名或伪名

订户不能使用匿名、伪名申请证书，证书中也不能使用匿名、伪名。

3.1.4 解释不同命名的规则

依 X.500 甄别名命名规则解释。

3.1.5 命名的唯一性

GDCA 应保证签发给某个订户的证书，其主体甄别名，在 GDCA 信任域内是唯一的。

3.1.6 商标的识别、鉴别与角色

GDCA 签发的证书的主体甄别名中不包含商标名。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

GDCA 在证书签发时，根据证书申请信息中的信息，GDCA 首先利用数据摘要算法进行计算，再用申请信息中的公钥对申请信息中的签名解密，然后进行比较，如果相等则证明数字证书的申请者拥有与签名验证公钥对应的签名私钥。

3.2.2 机构身份的鉴别

机构类订户的证书申请表上有申请者本身或被授权的证书申请者代表的签字（公章）表示接受证书申请的有关条款，并承担相应的责任。GDCA必须对订户所在机构进行身份鉴证，包括如下内容：

1. 确认机构是确实存在的、合法的实体。确认的方式可以是：政府机构签发的有效文件，包括但不限于工商营业执照或组织机构代码证等，或通过签发有效文件的权威第三方数据库确认。
2. 核查证书申请关键信息与有效文件或第三方数据库的资料是否相符，避免信息填写有误，但注册信息最终以申请者确认为准。

3.2.3 个人身份的鉴别

个人类订户的证书申请表上有申请者本身或被充分授权的证书申请者代表的签字表示接受证书申请的有关条款，并承担相应的责任。GDCA必须对订户的身份进行鉴证，包括如下内容：

1. 鉴别证明包括但不限于个人身份证或军官证等由政府机构颁发的能够证明个人身份的有效文件，或通过签发有效文件的权威第三方数据库确认。
2. 核查证书申请关键信息与有效文件或第三方数据库的资料是否相符，避免信息填写有误，但注册信息最终以申请者确认为准。

3.2.4 设备身份的鉴别

设备身份的鉴别会根据其设备拥有者的不同而不同，GDCA 必须对订户进行身份鉴证，包括如下内容：

1. 设备拥有者的身份鉴别根据不同类型按照不同的身份鉴别方式执行，订户为机构的，按照本CP$3.2.2节描述执行；订户为个人的，身份鉴别按照本CP$3.2.3节描述执行。
2. 核查证书申请关键信息与有效文件或第三方数据库的资料是否相符，避免信息填写有误，但注册信息最终以申请者确认为准。

3.2.5 没有验证的订户信息

不作验证的订户信息列表如下：

个人订户信息	机构订户信息	设备信息
● 电话/移动电话 ● 地址/邮政编码 ● 传真	● 单位英文名称 ● 地址/邮政编码 ● 电话/移动电话 ● 联系人传真	● 不作验证的个人或机构订户信息 ● 设备类型 ● MAC 地址

3.2.6 授权确认

当机构订户授权经办人办理证书业务时，组织机构须在相关业务表格上加盖单位公章，作为本机构对经办人的授权确认。

3.2.7 互操作准则

无规定。

3.3 密钥更新请求的标识与鉴别

在进行 CP § 4.7 所述的证书密钥更新前，需对更新的密钥进行鉴别以确保密钥更新请求来自原证书密钥拥有者。

3.3.1 常规密钥更新的标识与鉴别

对于常规情况下的密钥更新，订户可访问 GDCA 证书服务网站进行密钥更新申请，系统自动获取订户原证书信息，如甄别名、证书序列号等，形成证书密钥更新申请；GDCA 的证书认证系统将对密钥更新申请进行身份验证。订户也可以到 GDCA 的注册机构申请密钥更新，GDCA 注册机构必须验证订户与经办人的有效文件。

密钥更新会造成使用原密钥对加密的文件或数据无法解密，因此，订户在申请密钥更新前，必须确认使用原密钥对加密的文件或者数据已经解密，由此造成的损失，GDCA 将不承担责任。

3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后不能进行密钥更新。

3.4 吊销请求的标识与鉴别

证书吊销请求可以来自订户，也可以来自 GDCA、注册机构。当 GDCA 或者注册机构有充分的理由吊销订户的证书时，有权依法吊销证书，这种情况无须进行鉴证。如果订户主动请求吊销证书，则按照本 CP$3.2 节所述进行身份鉴别。

四、 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

证书申请实体包括个人和具有独立法人资格的组织机构(包括行政机关、事业单位、社会团体和人民团体等)。

4.1.2 注册过程与责任

1. 证书的注册过程（离线）

- 订户填写证书申请表；
- 订户携带身份证明材料到注册机构进行证书申请；
- 注册机构审核通过后，录入申请资料，向 GDCA 提交证书请求；
- GDCA 根据注册机构的请求签发证书；
- 注册机构通过安全的方式（如面对面提交）将证书交付给订户。

2. 证书的注册过程（在线）

- 订户登录网站在线填写证书申请表；
- 注册机构通过证书注册服务审核系统对订户提交的证书申请表进行查验，并决定是否受理申请；
- 注册机构审核通过后，向 GDCA 提交证书请求；
- GDCA 根据注册机构的请求签发证书；
- 订户携带申请表以及身份证明材料领取证书，注册机构对申请表及证明材料进行一致性和完整性的检查，审核通过后，将证书交付给订户。

3. 责任

- GDCA 及注册机构有责任向订户告知数字证书和电子签名的使用条件；
- GDCA 及注册机构有责任向订户告知服务收费的项目和标准；
- GDCA 及注册机构有责任向订户告知保存和使用订户信息的权限和责任；
- GDCA 及注册机构有责任向订户告知 GDCA 的责任范围；
- GDCA 及注册机构有责任向订户告知订户的责任范围；

- 订户负有在其证书申请中提供准确信息的责任；
- 注册机构承担对订户提供的证书申请信息与身份证明材料的一致性检查工作，同时承担相应审核责任。

4.2 证书申请处理

4.2.1 执行识别与鉴别

当 GDCA、注册机构接受到订户的证书申请后，应按本 CP § 3.2 的要求，对订户进行身份识别与鉴别。

4.2.2 证书申请批准和拒绝

GDCA、注册机构应在鉴证的基础上，批准或拒绝申请。如果拒绝申请，则应该通过适当的方式、在合理的时间内通知证书申请者。

4.2.2.1 证书申请的批准

如果符合下述条件，RA 可以批准证书申请：

1. 该申请完全满足本 CP § 3.2 关于订户身份的标识和鉴别规定；
2. 申请者接受或者没有反对订户协议的内容和要求；
3. 申请者已经按照规定支付了相应的费用。

4.2.2.2 证书申请的拒绝

如果发生下列情形，RA 可以拒绝证书申请：

1. 该申请不符合本 CP § 3.2 关于订户身份的标识和鉴别规定；
2. 申请者不能提供所需要的身份证明材料；
3. 申请者反对或者不能接受订户协议的有关内容和要求；
4. 申请者没有或者不能够按照规定支付相应的费用；
5. GDCA 或者注册机构认为批准该申请将会对 GDCA 带来争议、法律纠纷或者损失。

4.2.3 处理证书申请的时间

GDCA 的电子认证业务规则（CPS）应规定合理的证书申请处理时间。GDCA 和注册机构应在 CPS 规定的时间内处理证书申请，无论是批准还是拒绝。

4.3 证书签发

4.3.1 证书签发中 RA 和 CA 的行为

在证书的签发过程中 RA 的管理员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 的证书签发系统。RA 发往 CA 的证书签发请求信息须有 RA 的身份鉴别与信息保密措施，并确保请求发到正确的 CA 证书签发系统。

CA 的证书签发系统在获得 RA 的证书签发请求后，对来自 RA 的信息进行鉴别与解密，对于有效的证书签发请求，证书签发系统签发订户证书。

4.3.2 CA 和 RA 通知订户证书的签发

GDCA 的证书签发系统签发证书后，将直接或者通过 RA 通知订户证书已被签发，并向订户提供可以获得证书的方式。

4.4 证书接受

4.4.1 构成接受证书的行为

1. 订户自行访问专门的 GDCA 证书服务网站将证书下载至数字证书载体中，证书下载完毕即代表订户接受了证书。
2. GDCA 注册机构代替订户下载证书，下载的证书将被保存在数字证书载体中，当订户接受了该数字证书载体即代表订户接受了证书。

4.4.2 CA 对证书的发布

订户接受证书后，GDCA 将该订户证书发布到可被公开访问的目录服务系统。

4.4.3 CA 通知其他实体证书的签发

除证书订户外，GDCA 及注册机构不需要通知其他实体证书的签发。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户只能在本 CP 规定的应用范围内使用私钥和证书，其私钥可用于对信息的签名，订户应知悉并确认签名的内容，另外，私钥可用于对采用对应公钥加密的信息进行解密。

4.5.2 依赖方公钥和证书的使用

当依赖方接收到加载数字签名的信息后，有义务进行以下确认操作：

1. 获得数字签名对应的证书及信任链；
2. 确认该签名对应的证书是由 GDCA 所签发；
3. 通过查询 CRL 或 OCSP 确认该签名对应的证书是否被吊销；
4. 证书的用途适用于对应的签名；
5. 使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方有责任拒绝签名信息。

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。依赖方应将加密证书连同加密信息一起发送给接受方。

4.6 证书更新

4.6.1 证书更新的情形

每个证书都有其有效期，在一个订户证书到期前 30 天内至到期后 30 天内，如果订户的注册信息没有改变，订户可访问 GDCA 证书服务网站或者到 GDCA 的注册机构申请证书更新。

4.6.2 请求证书更新的实体

请求证书更新的实体为证书订户。

4.6.3 处理证书更新请求

对于证书更新，其处理过程包括申请验证、鉴别、签发证书。对申请的验证和鉴

别须基于以下几个方面：

1. 订户的原证书存在并且由 GDCA 所签发；
2. 验证证书更新请求在许可期限内；
3. 基于原注册信息进行身份鉴别。

在以上验证和鉴别通过后 GDCA 才可批准签发证书。

4.6.4 通知订户新证书的签发

同本 CP 4.3.2。

4.6.5 构成接受更新证书的行为

1. 订户自行访问专门的 GDCA 证书服务网站将证书下载至数字证书载体中，证书下载完毕即代表订户接受了证书。
2. GDCA 注册机构代替订户更新证书，当订户接受了已更新证书的数字证书载体即代表订户接受了证书。

4.6.6 CA 对更新证书的发布

同本 CP 4.4.2。

4.6.7 CA 通知其他实体证书的签发

同本 CP 4.4.3。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

GDCA 的证书密钥更新包括但不限于以下情形：

1. 证书私钥泄露而吊销证书；
2. 证书到期；
3. 证书密钥到期；
4. 基于技术、政策安全原因，GDCA 要求证书密钥更新。

4.7.2 请求证书密钥更新的实体

请求证书密钥更新的实体为证书订户。

4.7.3 处理证书密钥更新请求

同本 CP 4.6.3。

4.7.4 通知订户新证书的签发

同本 CP 4.3.2。

4.7.5 构成接受密钥更新证书的行为

1. 订户自行访问专门的 GDCA 证书服务网站将证书下载至数字证书载体中，证书下载完毕即代表订户接受了证书。
2. GDCA 注册机构代替订户更新密钥，当订户接受了已更新密钥的数字证书载体即代表订户接受了证书。

4.7.6 CA 对密钥更新证书的发布

同本 CP 4.4.2。

4.7.7 CA 通知其他实体证书的签发

同本 CP 4.4.3。

4.8 证书变更

4.8.1 证书变更的情形

如果订户提供的注册信息发生改变，必须向 GDCA 提出证书变更。

4.8.2 请求证书变更的实体

请求证书更新的实体为证书订户。

4.8.3 处理证书变更请求

证书变更按照初次申请证书的注册过程进行处理。

4.8.4 通知订户新证书的签发

同本 CP 4.3.2。

4.8.5 构成接受变更证书的行为

同本 CP 4.4.1。

4.8.6 CA 对变更证书的发布

同本 CP 4.4.2。

4.8.7 CA 通知其他实体证书的签发

同本 CP 4.4.3。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

发生下列情形，订户证书必须被吊销：

1. 私钥失窃、篡改、未经授权的泄露和其它安全威胁；
2. 订户违反了本 CP 规定的重要职责；
3. 订户主动提出吊销请求；
4. GDCA 发现订户在申请时提供的证明材料不真实；
5. 订户未能履行订户协议中应尽的责任，如订户未按期缴纳证书服务费。

4.9.2 请求证书吊销的实体

以下实体可以请求吊销一个订户证书：

1. GDCA 或注册机构可以依据本 CP § 4.9.1 要求吊销一个订户证书；
2. 对于个人证书，证书订户可以请求吊销他们自己的个人证书；
3. 对于机构证书，只有机构授权的代表有资格请求吊销已经签发给该机构的证

书；

4. 对于设备证书，只有拥有设备的机构授权的代表有资格请求吊销已经签发的证书。

4.9.3 证书吊销请求的处理程序

4.9.3.1 订户请求吊销证书

1. 订户向注册机构提交吊销申请表和身份证明材料，同时说明吊销原因；
2. 注册机构核实申请吊销实体的身份和吊销理由的正当性；
3. 注册机构将吊销申请表提交给 GDCA，由 GDCA 完成吊销。

4.9.3.2 订户被强制吊销证书

1. 当 GDCA 或注册机构有充分的理由确信出现本 CP§4.9.1 中的情况时，可通过内部确定的流程吊销证书；
2. GDCA 吊销订户证书后，通过适当的方式，包括电子邮件、电话、传真等，告知订户证书已被吊销及吊销理由。

4.9.4 吊销请求的宽限期

如果出现密钥泄露或有泄露嫌疑等事件，吊销请求必须在发现泄密或有泄密嫌疑 8 小时内提出。其他吊销原因的吊销请求必须在变更的 48 小时内提出。

4.9.5 CA 处理吊销请求的时限

GDCA 自接到吊销请求到完成吊销之间的间隔期限，不得超过 24 个小时。

4.9.6 依赖方检查证书吊销的要求

依赖方在依赖一个证书前必须查询 GDCA 发布的 CRL 确认他们所信任的证书是否被吊销。

4.9.7 CRL 发布频率

GDCA 须定时发布最新的证书吊销列表。证书吊销列表更新的时间间隔不能超过

24 小时。

4.9.8 CRL 发布的最大滞后时间

一个证书从它被吊销到它被发布到 CRL 上的滞后时间不能超过 24 小时。

4.9.9 在线状态查询的可用性

GDCA 须提供证书状态的在线查询服务（OCSP），以供安全保障要求高的应用使用。

4.9.10 在线状态查询要求

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，依赖方在依赖一个证书前必须通过证书状态在线查询检查该证书的状态。

4.9.11 吊销信息的其他发布形式

除了 CRL、OCSP 外，GDCA 可以提供吊销信息的其他发布形式，但这不是必须的。

4.9.12 密钥损害的特别要求

除本 CP$4.9.1 规定的情形外，当订户或注册机构的证书密钥受到安全损害时，应立即向 GDCA 提出证书吊销请求。

4.9.13 证书挂起的情形

证书挂起的情形包括证书挂失和证书冻结 2 种，发生下列情形，GDCA 可以挂起订户证书：

1. 证书密钥受损；
2. 订户违反了本 CP 规定的重要职责；
3. 订户主动提出挂失请求。

4.9.14 请求证书挂起的实体

请求证书挂失的实体为订户，请求证书冻结的实体为 GDCA。

4.9.15 挂起请求的程序

证书挂失的处理程序：

1. 订户向注册机构提出证书挂失申请，并填写《证书挂失申请表》。注册机构核实申请挂失实体的身份和授权实体的身份，如果挂失原因是密钥受损，要根据 GDCA 的 CPS 和安全管理规范的相关规定验证订户身份。订户必须提供表单上所有的必须信息，同时确保填写在表单上的信息是真实和准确的；
2. 注册机构将《证书挂失申请表》提交给 GDCA，由 GDCA 完成挂失。

证书冻结的处理程序：

1. 当 GDCA 或注册机构有充分的理由相信需要冻结最终订户的证书时，GDCA 或注册机构的有关人员可以通过内部确定的流程冻结证书。
2. 在证书冻结后，GDCA 或注册机构将通过适当的方式，包括邮件、电话、传真等，通知最终订户证书已被冻结及被冻结的理由。

4.9.16 挂起的期限限制

证书挂起的最长时间为三十天。

4.10 证书状态服务

4.10.1 操作特征

订户可以通过 CRL、LDAP 目录服务、OCSP 查询证书状态，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。

4.10.2 服务可用性

证书状态服务必须保证 7X24 小时可用。

4.10.3 可选特征

无规定。

4.11 订购结束

订户证书出现下列情形时表明订户的订购行为正式结束：

1. 证书到期后没有进行更新；
2. 证书到期前被吊销。

4.12 密钥托管与恢复

4.12.1 密钥托管与恢复的策略与行为

GDCA 要求订户必须使用本订户的数字证书载体生成签名密钥对。订户可以委托 GDCA 代订户进行生成签名密钥对的有关操作。由于签名私钥遗失所造成的损失由订户自己承担，GDCA 对此不承担责任。

证书订户的加密密钥对由 GDCA 代订户向广东省电子密钥管理中心申请生成，并由广东省电子密钥管理中心进行管理。当证书订户需要恢复加密密钥时，按照广东省电子密钥管理中心的规范、流程，接受订户的申请，为订户恢复相应的加密密钥。

4.12.2 会话密钥的封装与恢复的策略与行为

无规定。

五、 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

GDCA 中心机房按照功能主要分为核心区、服务区、管理区、操作区、公共区五个区域。核心区是一个高性能电磁屏蔽室。其壳体是六面优质冷轧钢板，其中顶、墙板采用厚度为 2mm 的冷轧钢板，地板采用厚度为 3mm 的冷轧钢板。焊接工艺为 CO2 保护焊。玻璃是加厚的嵌有金属网的防弹玻璃。屏蔽门是手动锁紧屏蔽门。通风口是按屏蔽室规格配置蜂窝型通风波导窗。电源滤波器是单相高性能低泄漏滤波器。存放保密资料的密码柜必须放置在核心区。

5.1.2 物理访问控制

进出每一个物理安全层的行为都需要被记录、审计和控制，从而保证进出每一个物理安全层的人都是经过授权的。GDCA 的 CPS 必须对物理访问控制进行比较详细的规定。

5.1.3 电力与空调

GDCA 机房应有安全、可靠的电力供电系统及电力备用系统，以确保持续不间断的电力供应。另外，还应具有机房专用空调系统、新风系统控制运营设施中的温度和湿度。

5.1.4 防水

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

5.1.5 火灾防护

GDCA 机房应采取预防措施，并制定相应的程序来消除和防止火灾的发生，这

些火灾防护措施应符合当地消防管理部门的安全要求。

5.1.6 介质存放

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

5.1.7 废物处理

当 GDCA 存档的纸张文件和材料已不再需要或存档期限已满时，必须采取措施销毁，使信息无法恢复。密码设备和存放敏感信息的存储介质在作废处置前根据制造商提供的方法先将其初始化并进行物理销毁。

5.1.8 异地备份

GDCA 建立了异地数据备份中心，使用专门的软件对关键系统数据、审计日志数据和其他敏感信息进行异地实时备份。

5.2 程序控制

5.2.1 可信角色

在 GDCA 提供的电子认证服务过程中，能从本质上影响证书的颁发、使用、管理和吊销等涉及密钥操作的职位都被 GDCA 视为可信角色。这些角色应包括：

1. 密钥和密码设备的管理人员；
2. 系统管理人员；
3. 安全审计人员；
4. 业务管理人员及业务操作人员。

5.2.2 每项任务需要的人数

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

1. 密钥和密码设备的操作和存放：需要 5 个可信人员中的 3 个共同完成；

2. 证书签发系统的后台操作：需要 3 个系统管理人员中的 2 个可信人员共同完成；
3. 审核和签发证书：需要 2 个可信人员共同完成。

5.2.3 每个角色的识别与鉴别

对于所有承担可信角色的人员，必须进行严格的识别和鉴证，确保其能够满足所从事工作职责的要求。

5.2.4 需要职责分割的角色

所谓职责分割，是指如果一个人担任了某一职能的角色，就不能再担任另一特定职能的角色。需要职责分割的角色包括且不限于：

1. CA 系统管理员和 KM 系统管理员不能由同一人担任；
2. 系统管理和安全审计岗位不能由同一人担任；
3. RA 录入人员和审核人员不能由同一人担任。

5.3 人员控制

5.3.1 资格、经历和清白要求

GDCA 对承担可信角色的工作人员的资格要求如下：

1. 具备良好的社会和工作背景；
2. 遵守国家法律、法规，服从 GDCA 的统一安排及管理；
3. 遵守 GDCA 有关安全管理的规范、规定和制度；
4. 具有良好的个人素质、修养以及认真负责的工作态度；
5. 具备良好的团队合作精神。

5.3.2 背景调查程序

GDCA 对充当可信角色的人员应进行严格的背景调查。根据不同可信岗位的工作特点，背景审查应该包括但不限于以下内容：

1. 身份证明，如个人身份证、护照、户口本等；
2. 学历、学位及其他资格证书；

3. 个人简历，包括教育、培训经历，工作经历及相关的证明人；

4. 无犯罪证明材料。

为了防止信息有假造情形发生，背景调查中 GDCA 应通过合法手段，尽可能地通过相关组织、部门进行人员背景信息的核实。

背景调查需要核实的材料和程序包括但不限于以下方面：

1. 验证先前工作记录的真实性；

2. 验证身份证明的真实性；

3. 验证学历、学位及其他资格证书的真实性；

4. 通过可靠途径确认教育、培训经历；

5. 检验无犯罪证明材料并确认无犯罪记录。

在背景调查中，如果发现下列情形，可以拒绝其获得可信人员的资格或取消其可信人员的资格：

1. 使用非法的身份证明或者学历、任职资格证明；

2. 借助不可靠人员的证明；

3. 存在捏造事实或资料的行为；

4. 有某些犯罪记录或者事实。

5.3.3 培训要求

为了使员工能够胜任工作，需要对员工进行必要的岗前培训和工作中的再培训，以更好的满足工作岗位对人员的要求。培训应该包括但不限于以下内容：

1. GDCA 颁布的证书策略和电子认证业务规则；

2. PKI 基本知识；

3. 电子签名法和相关法律法规；

4. GDCA 运营体系、技术体系和安全管理制度；

5. 工作职责和岗位说明。

5.3.4 再培训的频度和要求

GDCA 应根据需要安排再培训，以保证重要岗位的员工更加符合岗位需求，顺利地完成其工作职责。

5.3.5 工作岗位轮换的频度和次序

GDCA 应依据安全管理策略制定在职人员的工作岗位轮换周期和顺序。

5.3.6 未授权行为的处罚

GDCA 应建立并维护一套管理办法，对未授权行为进行适当的处罚，包括解除或终止劳动合同、调离工作岗位、罚款、批评教育、提交司法机构处理等方式。这些处罚行为应当符合法律法规的要求。

5.3.7 独立合约人的要求

对于不属于 GDCA 机构内部工作人员，但从事 GDCA 业务有关工作的如业务分支机构的业务人员、管理人员等独立合约人，GDCA 的统一要求如下：

1. 人员档案的备案管理；
2. 具有 1 年以上相关业务工作经验；
3. GDCA 提供统一的岗前培训和工作中的再培训，培训内容包括但不限于 GDCA 证书受理规则和电子认证业务规则。

5.3.8 提供给人员的文件

GDCA 提供给内部员工的文件应包括培训材料和与员工工作相关文档。

5.4 审计记录程序

5.4.1 记录事件的类型

GDCA 应记录的事件包括但不限于：

1. 订户申请、注销、更新、挂失证书及 GDCA 吊销、冻结用户证书或用户申请恢复密钥等；
2. GDCA 成员的建立，变更，登陆，重新设置和变更口令，吊销特权，创建、更新和恢复密钥；
3. 连接失败；
4. 由 GDCA 进行读写操作；
5. 所有关联事件诸如证书吊销，安全政策修改以及有效使用，GDCA/Authority

软件起始与停止，使证书及证书链有效化，属性证书管理，更新订户，DN变更，数据库及审计跟踪管理，证书生命周期管理及其它事件。

5.4.2 处理日志的频度

GDCA 应定期检查审计日志，以便发现重要的安全和操作事件，对发现的安全事件采取相应的措施。

5.4.3 审计日志的保留期限

GDCA 必须妥善保存电子认证服务的审计日志，保存期限为电子签名认证失效后五年。

5.4.4 审计日志的保护

所有的审计日志，应当采取严格的物理和逻辑访问控制措施，防止未经授权的浏览、修改、删除等。

5.4.5 审计日志的备份程序

对审计日志的备份应该建立和执行可靠的制度，定期进行备份。

5.4.6 审计收集系统

无规定。

5.4.7 对导致事件主体的通知

审计记录报告一个事件时，应通知引起该事件的个人、组织机构。

5.4.8 脆弱性评估

根据审计记录，GDCA 应定期进行安全脆弱性评估，并根据评估报告采取补救措施。

5.5 记录归档

5.5.1 归档记录的类型

需要归档的记录，除了本 CP§5.4.1 规定的外，还需要对如下记录进行归档，包括：

1. 证书申请信息；
2. 证书签发过程中的支持文档；
3. 证书生命周期的相关信息。

5.5.2 归档记录的保留期限

GDCA 的电子认证业务规则（CPS）应规定合理的归档记录保留期限。

5.5.3 归档文件的保护

应通过适当的物理和逻辑的访问控制方法保护归档数据，只有授权的可信人员允许访问归档数据，防止未经授权的浏览、修改、删除或其它的篡改行为。

5.5.4 归档文件的备份程序

对于系统生成的电子归档记录，应当定期进行备份，备份文件进行异地存放。

对于书面的归档资料，不需要进行备份，但需要采取严格的措施保证其安全性。

5.5.5 记录时间戳要求

GDCA 的档案在创建的时候须加盖带有 GDCA 数字签名的时间戳。

5.5.6 归档收集系统

各自实体应在内部建设归档收集系统，包括 GDCA 和注册机构。

5.5.7 获得和检验归档信息的程序

GDCA 的安全审计员和业务管理员分别保留归档信息的 2 个拷贝。在获得完整档案信息时，须对这 2 个拷贝进行比较。

5.6 密钥变更

在 CA 证书到期时，GDCA 将对 CA 证书进行更新。只要 CA 密钥对的累计寿命没有超过本 CP§6.3.2 中规定的最大生命期，那么 CA 证书可以使用原密钥进行更新。否则需要产生新的密钥对，替换已经过期的 CA 密钥对。即使在密钥对生命期内，GDCA 也可以通过生成新密钥对的方式产生新的 CA 证书。在一个 CA 证书过期之前，密钥变更过程被启动，以保障这个 CA 体系中的实体从 CA 旧密钥对到新密钥对的平稳过渡。

在生成新的 CA 密钥对时，必须严格遵守 GDCA 关于密钥管理的规范。新的密钥对产生时，GDCA 将签发新的 CA 证书，并及时进行发布，让订户和依赖方能够及时获取新的 CA 证书。

CA 密钥更替时，必须保证整个证书链的顺利过渡。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

GDCA 应制订各种事故处理方案和应急处理预案，规定相应的事故和损害处理程序。

5.7.2 计算机资源、软件和/或数据的损坏

如果出现计算机资源、软件和/或数据损坏的事件，GDCA 立即启动事故处理程序，如有必要，可按照灾难恢复计划实施恢复。

5.7.3 实体私钥损害处理程序

当 GDCA 的根 CA 私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，GDCA 应采取下列步骤以恢复安全环境：

1. 向政府主管部门汇报；
2. 通过网站和其它公共媒体对订户、依赖方进行通告；
3. 吊销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供订户和依赖方查询；
4. 生成新的 CA 密钥对，签发新的 CA 证书。

5. 新的 CA 证书签发以后，按照本 CP 关于证书签发的规定，重新签发订户证书；
6. 新的证书签发以后，立即通过 GDCA 信息库、目录服务器、HTTP 等方式进行发布。

当证书订户的私钥出现遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，订户应立即通知 GDCA 吊销其证书，并尽可能地通知依赖方。GDCA 应按本 CP 4.9 及时吊销订户证书并发布证书吊销信息。订户需要重新申请证书才能继续使用。

5.7.4 灾难后的业务存续能力

GDCA 在发生灾难后，应有如下几个方面的业务存续能力：

1. 在尽可能短的时间内恢复业务系统，最多不超过 48 小时；
2. 能够恢复客户信息；
3. 能够保证恢复后的运营场地符合安全要求；
4. 有足够的人员继续开展业务并且不违反职责分割的要求。

5.8 CA 或 RA 的终止

当 GDCA 及其注册机构需要停止其业务时，必须严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》及相关法规中对认证机构终止电子认证服务的规定要求进行有关工作。

在 GDCA 终止前，必须：

1. 委托业务承接单位；
2. 起草 GDCA 终止声明；
3. 通知与 GDCA 终止相关的实体；
4. 关闭从目录服务器；
5. 证书注销；
6. 处理存档文件记录；
7. 停止认证中心的服务；
8. 存档主目录服务器；

9. 关闭主目录服务器；

10. 处理 GDCA 业务管理员和 GDCA 业务操作员；

11. 处理加密密钥；

12. 处理和存储敏感文档；

13. 清除 GDCA 主机硬件。

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

六、 认证系统技术安全控制

6.1 密钥对的生成与安装

6.1.1 密钥对的生成

6.1.1.1 CA 密钥对生成

CA 密钥对由国家密码主管部门批准和许可的设备生成的。密钥的生成、管理、存储、备份和恢复都按照严格的密钥管理流程规定进行。用于此类密钥生成的密码模块须通过国家密码主管部门鉴定、认证。

6.1.1.2 订户签名密钥对生成

GDCA 订户必须使用国家密码主管部门批准许可的设备生成签名密钥对，例如由加密机、加密卡、USB Key、IC 卡等生成。订户在选择这些设备前，应事先向 GDCA 咨询有关系统兼容和接受事宜。GDCA 向订户提供符合国家密码管理相关规定的 USB Key 作为订户签名密钥对的生成和存储设备。

GDCA 一般不提供代为生成签名密钥对，如果用户书面申请并经 GDCA 批准，GDCA 可以为申请者代为生成密钥对，并且承诺不保留私钥的副本，采取足够的措施保证密钥对的安全性、可靠性和唯一性，但是由于此密钥对的遗失、泄露等原因造成的损失，GDCA 不承担任何责任与义务。

订户签名密钥对的产生，必须遵循国家的法律政策规定。GDCA 在技术、业务流程和管理上，已经实施了安全保密的措施。

6.1.1.3 订户加密密钥对生成

GDCA 订户的加密密钥对由 GDCA 代订户向广东省电子密钥管理中心申请生成，并由广东省电子密钥管理中心进行管理。

6.1.2 加密私钥传送给订户

由证书签发机构代替订户对密钥管理中心提出加密密钥申请请求，密钥管理中心对产生的加密私钥使用订户通讯密钥进行数字信封加密，以数据流的方式传送给证书

签发机构，通过证书签发机构下载到订户证书载体时，订户使用自己的证书载体解密该私钥并存储。

6.1.3 公钥传送给证书签发机构

为了获得数字证书，最终订户和 RA 通过 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包格式，以电子的方式将公钥提交给 GDCA 签发，这些请求或文件包的传送需要使用安全协议保护，比如安全套接层协议（SSL）。

6.1.4 CA 公钥传送给依赖方

GDCA 应该通过安全可靠的途径将 CA 公钥传给依赖方，包括从安全站点下载、面对面的提交等方式。

GDCA 也需要通过目录发布其 CA 证书。

6.1.5 密钥的长度

CA 和最终订户密钥对至少是 1024 位 RSA。

6.1.6 公钥参数的生成和质量检查

公钥参数必须使用国家密码主管部门批准许可的加密设备和硬件介质生成，例如加密机、加密卡、USB Key、IC 卡等生成和选取，并遵从这些设备的生成规范和标准。GDCA 认为这些设备和介质内置的协议、算法等已经具备了足够的安全等级要求。

对于参数质量的检查，同样由通过国家密码主管部门批准许可的加密设备和硬件介质进行，例如加密机、加密卡、USB Key、IC 卡等。

6.1.7 密钥使用目的

GDCA 签发的 X.509v3 证书包含了密钥用法扩展项，其用法与 RFC 3280 标准 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002) 相符。如果 GDCA 在其签发证书的密钥用法扩展项内指明了用途，证书订户必须按照该指明的用途使用密钥。

参见本 CP 7.1.2。

6.2 私钥保护和密码模块工程控制

认证机构必须通过物理、逻辑和过程控制的综合实现来确保 CA 私钥的安全。订户协议会要求证书订户采取必要的预防措施防止私钥的丢失、泄露、更改或未经授权的使用。

6.2.1 密码模块的标准和控制

GDCA 必须使用国家密码管理部门认可、批准的硬件密码模块生成根 CA、签发证书的 CA 和其他 CA 密钥对，并存储相关 CA 私钥。

6.2.2 私钥多人控制（m 选 n）

认证机构必须通过技术及过程上的控制机制来实现多名可信人员共同参与 CA 加密设备的操作。技术上的控制可使用“秘密分割”技术，即将使用一个 CA 私钥时所需的激活数据分成若干个部分，分别由多名可信人员持有。如果为一个硬件密码模块的秘密分割总数为 m，那么必须有超过 n 个的可信人员才能激活储存在密码模块中的 CA 私钥。在这里 m 不小于 5，n 不小于 3。

6.2.3 私钥备份

为了保证业务持续开展，GDCA 必须创建 CA 私钥的备份，以备灾难恢复使用。私钥备份以加密的形式保存在硬件密码模块中。存储 CA 私钥的密码模块应符合 CP$6.2.1 的要求并存放在保险柜中。CA 私钥复制到备份硬件密码模块中要符合 CP$6.2.5 的要求。

对于订户签名证书，如果其私钥存放在软件密码模块中，建议订户对私钥进行备份，备份的私钥需要采用口令保护等授权访问控制，防止非授权的修改或泄露。

对于订户加密证书，其加密私钥由广东省电子密钥管理中心进行备份，备份私钥以密文形式存在。

6.2.4 私钥归档

在 CA 私钥到期后，必须使用满足 CP$6.2.1 要求的硬件密码模块归档保存至少 5 年。归档期限结束后，对 CA 私钥的销毁应符合 CP$6.2.9 的规定。

6.2.5 私钥导出、导入密码模块

CA 的私钥，GDCA 应严格按照根密钥管理规范进行备份，除此之外的任何导入导出操作将不被允许。当 CA 密钥对备份到另外的硬件密码模块上时，以加密的形式在模块之间传送，并且在传递前要进行身份鉴别，以防止 CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

GDCA 不提供订户私钥从硬件密码模块中导出的方法，也不允许如此操作。

6.2.6 私钥在密码模块的存储

CA 私钥必须以密文的形式存放在国家密码主管部门批准和许可的硬件密码模块中。

订户的私钥存储在符合国家密码管理规定的 USB Key 介质中，所有在 USB Key 中存储的私钥，都以密文的形式保存。

6.2.7 激活私钥的方法

CA 的私钥存放于硬件密码模块中，其激活数据按照 CP § 6.2.2 进行分割，并且保存在 IC 卡等硬件介质中，必须由 m 选 n 的方式分别输入激活数据才能激活私钥。

对于存放在诸如 USB Key、加密卡、加密机或者其他形式的硬件密码模块中的订户私钥，订户可以通过口令、IC 卡等方式进一步保护。当订户计算机上安装了相应的驱动后，将 USB Key、IC 卡等插入相应设备中，输入保护口令，则私钥被激活。

6.2.8 冻结私钥的方法

对于 CA 私钥，当存放私钥的设备断电，私钥就被冻结。

订户冻结私钥由其自行决定，当每次操作后注销计算机，或者把硬件密码模块从读卡器中取出时，私钥成为非激活状态。

6.2.9 销毁私钥的方法

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

对于最终订户加密证书私钥，在其生命周期结束后，应该妥善保存一定期限，以便于解开加密信息。对于最终订户签名证书私钥，在其生命周期结束后，如果无需再保存，可以通过私钥的删除、系统或密码模块的初始化来销毁。

CA 私钥，在生命周期结束后，需将 CA 私钥的一个或多个备份进行归档，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时需在多名可信人员参与的情况下安全销毁。CA 私钥存放在硬件加密卡中，CA 私钥的销毁必须通过将 CA 私钥从加密卡中彻底删除或将加密卡初始化的方式销毁。

6.2.10 密码模块的评估

GDCA 使用国家密码主管部门批准和许可的密码产品，接受其颁发的各类标准、规范、评估结果、评价证书等各类要求，GDCA 可根据产品性能、工作效率、供应厂商的资质等方面的条件，选择所需要的模块。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

必须归档 CA 和最终订户证书，归档的证书可存放在数据库中。

6.3.2 证书操作期和密钥对使用期限

公钥和私钥的使用期限与证书的有效期相关但却有所不同。

对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

另外需注意的是无论是订户证书还是 CA 证书，证书到期后，在保证安全的情况下，允许使用原密钥对对证书进行更新。但是密钥对不能无限期使用。

6.4 激活数据

6.4.1 激活数据的产生和安装

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

订户私钥的激活数据，包括用于下载证书的口令（以密码信封的形式提供）、USB Key 的 PIN 码等，都必须在安全可靠的环境下随机产生。

6.4.2 激活数据的保护

对于 CA 私钥的激活数据，必须通过秘密分割将分割后的激活数据由不同的可信人员掌管，而且掌管人员必须符合职责分割的要求，签署协议确认他们知悉秘密分割掌管者责任。

如果证书订户使用口令或 PIN 码保护私钥，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。同时为了配合业务系统的安全需求，应该经常对激活数据进行修改。

6.4.3 激活数据的其他方面

当私钥的激活数据进行传送时，应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

当私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

GDCA 系统的信息安全管理，按照国家密码管理局公布的《证书认证系统密码及其相关安全技术规范》、工业和信息化部公布的《电子认证服务管理办法》，参照 ISO17799 信息安全标准规范以及其他相关的信息安全标准，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。主要的安全技术和控制措施包括：身份识别和验证、逻辑访问控制、物理访问控制、人员职责分权管理、网络访问

控制等。

通过严格的安全控制手段，确保 CA 软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。

核心系统必须与其他系统物理分离，生产系统与其他系统逻辑隔离。这种分离可以阻止除指定的应用程序外对网络的访问。使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动。只有 CA 系统操作与管理组中的、有必要工作需要、访问系统的可信人员可以通过口令访问 CA 数据库。

6.5.2 计算机安全评估

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

GDCA 的认证系统，通过了国家密码管理局的安全性审查。

6.6 生命周期技术控制

6.6.1 系统开发控制

GDCA 的软件设计和开发过程遵循以下原则：

第三方验证和审查；

安全风险分析和可靠性设计；

同时，GDCA 的软件开发操作规范，参考 ISO15408 的标准，执行相关的规划和开发控制。

6.6.2 安全管理控制

GDCA 认证系统的信息安全管理，严格遵循国家密码主管部门的有关运行管理规范进行操作。

GDCA 认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行安全和使用，任何修改和升级会记录在案并进行版本控制、功能测试和记录。GDCA 还对认证系统进行定期和不定期的检查和测试。

GDCA 采用一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。

硬件设备由采购到接收时，会进行安全性的检查，用来识别设备是否被入侵，是否存在安全漏洞等。加密设备的采购和安装必须在更加严格的安全控制机制下，进行设备的检验、安装和验收。

GDCA 认证系统所有的软硬件设备升级以后，废旧设备在进行处理时，首先必须确认其是否有影响安全的信息存在。

6.6.3 生命周期的安全控制

GDCA 认证系统的软硬件设备具备可持续性的升级计划，其中包括了对软、硬件生命周期的安排。

6.7 网络的安全控制

GDCA 认证系统采用多级防火墙和网络资源安全控制系统的保护，并且实施完善的访问控制技术。

为了确保网络安全，GDCA 认证系统安装部署了入侵检测、安全审计、防病毒和网管系统，并且及时更新防火墙、入侵检测、安全审计、防病毒和网管系统的版本，以尽可能的降低来自于网络的风险。

七、 证书、证书吊销列表和在线证书状态协议

7.1 证书描述

GDCA 证书遵循 ITU-T X.509v3（1997）：信息技术-开放系统互连-目录：认证框架（1997 年 6 月）标准和 RFC 3280：Internet X.509 公钥基础设施证书和 CRL 结构（1999 年 1 月）。

证书至少包含基本的 X.509 v1 域，其规定值或值的限制如下表所描述。

表-证书结构的基本域

域	值或值的限制
版本	指明 X.509 证书的格式版本，值为 V3
序列号	证书的唯一标识符
签名算法	签发证书时所使用的签名算法（见 CP$7.1.3）
签发者 DN	签发者的甄别名
有效起始日期	基于国际通用时间(UTC)，和北京时间同步，按 RFC 3280 要求编码
有效终止日期	基于国际通用时间(UTC)，和北京时间同步，按 RFC 3280 要求编码。有效期限的设置符合 CP$6.3.2 规定的限制。
主题 DN	证书持有者或实体的甄别名
公钥	根据 RFC 3280 编码，使用 CP$7.1.3 中指定的算法，密钥长度满足 CP$6.1.5 指定的要求

7.1.1 版本号

GDCA 订户证书符合 X.509 V3 证书格式，版本信息存放在证书版本信息栏内。

7.1.2 证书扩展项

GDCA 除了使用 X.509 V3 版证书标准扩展项以外，还使用了自定义扩展项。自定义扩展项的使用是允许的，但是除非由于特别应用而包含该项，不保证该扩展项的使用。

7.1.2.1 标准扩展项

- 密钥用法 (key usage)

指定证书密钥对的用法：电子签名，不可抵赖，密钥加密，数据加密，密钥协议，验证证书签名，验证 CRL 签名，只加密，只解密，只签名。

- 颁发机构密钥标识符（Issuer Unique Identifier）

最终订户证书及中级 CA 证书加入颁发机构密钥标识符扩展项，当证书签发者包含主题密钥标识扩展项时，颁发机构密钥标识符由 160 位的颁发证书机构的公钥进行 SHA-1 散列运算后的值构成。否则，它将包含颁发 CA 的主题 DN。这个扩展项的 criticality 域设置为 FALSE。

- 主题密钥标识符（Subject Unique Identifier）

证书的主题密钥标识符扩展项赋值时，证书主题的公钥的密钥标识符被产生。使用该扩展项时，其扩展项的 criticality 域设为 FALSE。

- CRL 发布点（cRLDistributionPoints）

证书中的 CRL 的分发点扩展项，它包含本地的一个链接，可以向依赖方提供 CRL 的信息以便其查询证书状态。此扩展项的 criticality 项应设为 FALSE。

- 证书策略扩展项（Certificate Policies）

证书策略扩展项中有本 CP 中对应证书类的 CP 对象标识符及策略限定符。这个扩展项的 criticality 域设置为 FALSE。

- 基本限制扩展项（BasicConstraints）

CA 证书的基本限制扩展项中的主题类型被设为 CA。最终订户证书的基本限制扩展项的主题类型设为最终实体 (End-Entity)。这个扩展项的 criticality 域设置为 FALSE。将来，对于其它的证书，这个扩展项的 criticality 域可以设置为 TRUE。

CA 证书的基本限制扩展项中的路径长度设定为在证书路径中该证书之后的 CA 级数。对于最终订户证书签发 CA，其 CA 证书“pathLenConstraint”域的值设为 0，表示证书路径中仅有一个最终订户证书可以跟在这个 CA 证书后面。

7.1.2.2 自定义扩展项

针对不同的证书应用服务需求，GDCA 灵活定义一些扩展项，包括但不限于如下扩展项：

- 社会保险号：用于表示订户的社会保险号码。
- 组织机构代码：用于表示企业组织机构代码。

- 工商注册号：用于表示企业工商注册号码
- 国税登记证号：用于表示企业国税号码
- 信任服务号：证书颁发机构产生用于标识订户的唯一编号。
- 地税登记证号：用于表示企业地税号码。
- 个人身份证号码：用于表示居民身份证的唯一编号。

7.1.3 算法对象标识符

GDCA 签发的证书中，密码算法的标识符为 sha1RSA。

GDCA 所使用的算法对象标识符，符合 ISO 对象标识符（OID）管理的规范。例如：

1. 签名算法：

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {
iso（1） member-body（2） us（840） rsadsi（113549） pkcs（1）
pkcs-1（1） 5 }

2. 摘要算法：

sha-1 OBJECT IDENTIFIER ::= {
iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}
md5 OBJECT IDENTIFIER ::={
iso(1) member-body(2) us(840) rsadsi(113549) digestAlgorithm(2) 5}

3. 非对称算法：

rsaEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 1}

4. 对称算法

本 CP 建议使用国家密码管理部门认可的对称算法。

7.1.4 名称形式

GDCA 签发的证书名称形式的格式和内容符合 X.501 Distinguished Name(DN)的甄别名格式。

7.1.5 名称限制

订户的命名一定要有意义，应具有通常能够被理解的语义，可以明确确定证书主题中的个人、单位或者设备的身份，订户证书不被允许为匿名或者伪名。

7.1.6 证书策略对象标识符

当使用证书策略扩展项时，证书中包含证书策略的对象标识符，该对象标识符与相应的证书类别对应。

7.1.7 策略限制扩展项的用法

无规定。

7.1.8 策略限定符的语法和语义

无规定。

7.1.9 关键证书策略扩展项的处理语义

与 X509 和 PKIX 规定一致。

7.2 证书吊销列表

GDCA 定期签发 CRL，供用户查询使用。

依本 CP 签发的 CRL 符合 RFC3280 标准。CRL 至少包含如下表所述基本域和内容。

域	值或者值的限制
版本	V2
颁发者	签发 CRL 的实体，颁发者甄别。
生效日期	CRL 的签发日期
下次更新	CRL 下次签发的日期。最终订户证书每隔 24 小时更新
签名算法	Sha1RSA,签发 CRL 所使用的签名算法
颁发机构密钥标识符	由 160 位的颁发证书机构公钥进行 SHA-1 散列运算后的值构成

吊销列表	列出吊销的证书，包括吊销证书的序列号和吊销日期

7.2.1 版本

GDCA 目前签发 X.509 V2 版本的 CRL，此版本号存放在 CRL 版本格式栏目中。

7.2.2 CRL 和 CRL 条目扩展项

无规定。

7.3 OCSP 描述

GDCA 为用户提供 OCSP（在线证书状态查询服务），OCSP 作为 CRL 的有效补充，方便证书用户及时查询证书状态信息。

7.3.1 版本号

RFC2560 定义的 OCSP V1 版本。

7.3.2 OCSP 扩展项

无规定。

八、 认证机构审计和其他评估

8.1 评估的频度和情形

GDCA 应每年对物理控制、密钥管理、操作控制、鉴证执行等情况执行一次审计，以确定实际发生情况是否与预定的标准、要求一致，并根据审查结果采取行动。

8.2 评估者的身份/资格

GDCA 的审计、评估均为内部审计，由 GDCA 技术与运营策略委员会负责组织跨部门的审计评估小组，由审计评估小组执行此项工作。

8.3 评估者与被评估者之间的关系

GDCA 审计员与本机构的系统管理员、业务管理员、业务操作员的工作岗位不能重叠。

8.4 评估的内容

GDCA 内部审计的内容包括：

1. 安全策略是否得到充分的实施；
2. 运营工作流程和制度是否得到严格遵守；
3. 是否严格按 CP、业务规范和安全要求开展认证业务；
4. 各种日志、记录是否完整，是否存在问题；
5. 是否存在其他可能存在的安全风险。

8.5 对问题与不足采取的行动

对于 GDCA 内部审计结果中的问题，由审计评估小组负责监督这些问题的责任职能部门进行业务改进和完善的情况。完成对审计结果的改进后，各职能部门必须向审计评估小组提交业务改进工作总结报告。

对于 GDCA 授权注册机构的审计结果，如该机构正在进行违反本 CP 及 GDCA

制定的其他业务规范的行为，GDCA 将予以制止，并有权责令其立即停止这些行为，同时根据 GDCA 的要求进行业务整改。业务违规行为情节严重的注册机构，GDCA 将终止对该机构的电子认证业务有关授权。

8.6 评估结果的传达与发布

GDCA 的内部审计结果应向本机构各职能部门以及审计涉及的注册机构进行正式通报，对可能造成订户安全隐患，GDCA 必须及时向订户通报。

8.7 其他评估

无规定。

九、 法律责任和其他业务条款

9.1 费用

GDCA 可根据提供的电子认证服务向本机构的证书订户收取费用，具体收费标准必须根据国家有关物价管理部门的批复文件执行，GDCA 不得擅自提高收费标准，扩大收费范围。

9.2 财务责任

9.2.1 保险范围

保险范围主要针对 CP § 9.9 中所规定的赔偿。

9.2.2 其他财产

无规定。

9.2.3 对最终实体的保险或担保范围

证书订户一旦接受 GDCA 的证书，那么就意味着该订户已经接受了本 CP 关于保险和担保的规定和约束。

9.3 业务信息保密

9.3.1 保密信息范围

在 GDCA 提供的电子认证服务中，以下信息视为保密信息：

1. GDCA 订户的数字签名及解密密钥；
2. 审计记录包括：本地日志、服务器日志、归档日志的信息，这些信息被 GDCA 视为保密信息，只有安全审计员和业务管理员可以查看。除法律要求，不可在公司外部发布；
3. 其他由 GDCA 和 RA 保存的个人和公司信息应视为保密，除法律要求，不可公布。

9.3.2 不属于保密的信息

1. 由 GDCA 发行的证书、证书中的公钥；
2. 证书中的订户信息；
3. 证书吊销列表；
4. 证书策略（CP）、电子认证业务规则（CPS）。

9.3.3 保护保密信息的责任

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

当保密信息的所有者出于某种原因，要求 GDCA 公开或披露他所拥有的保密信息时，GDCA 应满足其要求；同时，GDCA 将要求该保密信息的所有者对这种申请进行书面授权， 以表示其自身的公开或者披露的意愿。如果这种披露保密信息的行为涉及任何其他方的赔偿义务，GDCA 不应承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者应承担与此相关的或由于公开保密信息引起的所有赔偿责任。

当 GDCA 在任何法律、法规、法院以及其他公权力部门通过合法程序的要求下，必须提供本 CP 中规定的保密信息时，GDCA 应按照法律、法规以及法院判决的要求，向执法部门公布相关的保密信息，GDCA 无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4 个人隐私保密

9.4.1 隐私保密计划

GDCA 应制定隐私保密计划对订户的个人信息保密。

9.4.2 作为隐私处理的信息

作为隐私处理的信息包括：

1. 订户的有效证件号码如身份证号码、单位机构代码；
2. 订户的联系电话；

3. 订户的地址；

4. 订户的银行帐号。

9.4.3 不被认为隐私的信息

订户持有的证书内包括的信息，以及该证书的状态等，是可以公开的，不被视为隐私信息。

9.4.4 保护隐私的责任

GDCA、注册机构有妥善保管与保护本 CP§9.4.2 中规定的订户隐私信息的责任与义务。

9.4.5 使用隐私信息的告知与同意

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

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

GDCA、注册机构如果需要将订户隐私信息用于双方约定的用途以外的目的，事前必须告知订户并获得订户同意和授权，而且这种同意和授权要用可归档的方式（如传真、信函等）。

9.4.6 依法律或行政程序的信息披露

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

1. 政府法律法规的规定并且经相关部门通过合法程序提出申请；

2. 法院以及公权力部门处理因使用证书产生的纠纷时合法的提出申请；

3. 具有合法司法管辖权的仲裁机构的正式申请。

9.4.7 其他信息披露情形

如果订户要求 GDCA 提供某类特定客户支援服务如资料邮寄时，GDCA 则需要把订户的联系电话和地址等信息提供给第三者如邮寄公司。

9.5 知识产权

1. GDCA 享有并保留对证书以及 GDCA 提供的所有软件的全部知识产权；
2. GDCA 对数字证书系统软件具有所有权、名称权、利益分享权；
3. GDCA 网站上公布的一切信息均为 GDCA 财产，未经 GDCA 书面允许，他人不能转载用于商业行为；
4. GDCA 发行的证书和 CRL 均为受 GDCA 支配的财产；
5. 对外运营管理策略和规范为 GDCA 财产；
6. 用来表示目录中 GDCA 域中的实体的甄别名（以下简称 DN）以及该域中颁发给终端实体的证书，均为 GDCA 的财产。

9.6 陈述与担保

9.6.1 CA 的陈述与担保

GDCA 对证书订户必须做出如下担保：

1. GDCA 签发给订户的证书符合本 CP 的所有实质性要求；
2. 在签发证书时，不会因 CA 的失误而使证书中的信息与 CA 所收到的信息不一致；
3. GDCA 保证其私钥得到安全的存放和保护，GDCA 建立和执行的安全机制符合国家相关政策的规定；
4. GDCA 将按本 CP 的规定，及时吊销证书；
5. GDCA 将向证书订户通报任何已知的，将在本质上影响订户的证书的有效性和可靠性事件；

GDCA 对依赖方必须做出如下担保：

1. 除未经验证的订户信息外，证书中的其他订户信息都是准确的；
2. GDCA 完全遵照本 CP 及 CPS 的规定签发证书；
3. 在 GDCA 信息库中发布的证书已经签发给了订户，并且订户已经按照本 CP

中的规定接受了该证书。

9.6.2 RA 的陈述与担保

1. 提供给证书订户的注册过程完全符合本 CP 的所有实质性要求；
2. 在 GDCA 生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请者的信息不一致；
3. 注册机构将按本 CP 的规定，及时向 GDCA 提交证书申请、吊销、更新等服务申请。

9.6.3 订户的陈述与担保

订户一旦接受 GDCA 签发的证书，就被视为向 GDCA、注册机构及依赖方作出以下承诺：

1. 已知悉和接受本 CP 中的所有条款和条件；
2. 在证书的有效期内进行数字签名；
3. 订户在申请证书时向注册机构提供的信息都是真实、完整和准确的；
4. 证书的私钥为订户本身访问和使用；
5. 证书在本 CP 中规定使用范围内合法使用；
6. 采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件。

9.6.4 依赖方的陈述与担保

1. 遵守本 CP 的所有规定；
2. 在依赖证书前，确认证书在规定的范围和期限使用；
3. 在依赖证书前，对证书的信任链进行验证；
4. 在依赖证书前，通过查询 CRL 或 OCSP 确认证书是否被吊销。

9.6.5 其他参与者的陈述与担保

遵守本 CP 的所有规定。

9.7 担保免责

除本 CP 9.6.1 中的明确承诺外，GDCA 不承担其他任何形式的保证和义务：

1. 不保证证书订户、依赖方、其他参与者的陈述内容；
2. 不对电子认证活动中使用的任何软件做出保证；
3. 不对证书在超出规定目的以外的应用承担任何责任；
4. 对由于不可抗力，如战争、自然灾害等造成的服务中断并由此造成的客户损失承担责任；
5. 订户违反本 CP 9.6.3 之承诺时，或依赖方违反本 CP 9.6.4 之承诺时，得以免除 GDCA 之责任。

9.8 有限责任

证书订户、依赖方因 GDCA 提供的电子认证服务从事民事活动遭受损失，GDCA 只承担本 CP 9.9.1 规定的有限责任。

9.9 赔偿

9.9.1 认证机构的赔偿责任

如 GDCA 违反了本 CP§9.6.1 中的陈述，订户、依赖方等实体可申请 GDCA 承担赔偿责任（法定或约定免责除外），包括以下情形：

1. GDCA 将证书错误的签发给订户以外的第三方，导致订户或依赖方遭受损失的；
2. 在订户提交信息或资料准确、属实的情况下，GDCA 签发的证书出现了错误信息，导致订户或依赖方遭受损失的；
3. 在 GDCA 明知订户提交信息或资料存在虚假谎报的情况，但仍然向订户签发证书，导致依赖方遭受损失的；
4. 由于 GDCA 的原因导致证书私钥被破译、窃取，订户或依赖方遭受损失的；
5. GDCA 未能及时吊销证书，导致依赖方遭受损失的。

9.9.2 订户的赔偿责任

在如下情况，订户对自身原因造成的 GDCA、依赖方损失，应当承担赔偿责任：

1. 提供的资料或信息不真实、不完整或不准确；
2. 证书中的信息发生变更但未停止使用证书并及时通知 GDCA 和依赖方；
3. 没有对私钥采取有效的保护措施，导致私钥丢失或被损害、窃取、泄露等；
4. 在得知私钥丢失或存在危险时，未停止使用证书并及时通知 GDCA 和依赖方；
5. 证书到期但仍在使用证书；
6. 订户的证书信息侵犯了第三方的知识产权；
7. 在规定的应用范围外使用证书，如从事违法犯罪活动。

9.9.3 依赖方的赔偿责任

在如下情况，依赖方对自身原因造成的 GDCA、订户损失，应当承担赔偿责任：

1. 没有履行 GDCA 与依赖方的协议和本 CP 中规定的义务；
2. 在不合理的情形下依赖证书，如依赖方明知证书存在超范围、超期限使用的情形或证书已经或有可能被人窃取的情形，但仍然依赖证书；
3. 依赖方没有对证书的信任链进行验证；
4. 依赖方没有通过查询 CRL 或 OCSP 确认证书是否被吊销。

9.10 有效期与终止

9.10.1 有效期

本 CP 及其更新版本自公布之日起的 15 天之后正式生效，在 GDCA 终止电子认证服务时失效。

9.10.2 终止

GDCA 终止电子认证服务时，本 CP 终止。

9.10.3 终止的效果与存续

本 CP 的终止，意味着认证机构认证业务的终止，但认证业务的终止不意味着认证机构责任的终止。认证机构在业务终止后应采取合理的措施，将认证服务转到其他

认证机构，保证订户的利益。

9.11 对参与者的个别通告及信息交互

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

9.12 修订

9.12.1 修订程序

本 CP 的修订，由 GDCA 行政管理部提出修订报告，获得 GDCA 技术与运营策略委员会批准后，由 GDCA 行政管理部负责组织修订，修订后的 CP 经过 GDCA 技术与运营策略委员会批准后正式对外发布。

9.12.2 通知机制和期限

修订后的 CP 经批准后将立即在 GDCA 的网站 www.gdca.com.cn 上发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，GDCA 将在合理的时间内通知有关各方，合理的时间应保证有关方受到的影响最小。

9.12.3 必须修订的情形

如果出现下列情况，GDCA 必须对本 CP 进行修改：

1. 密码技术出现重大发展，足以影响现有 CP 的有效性；
2. 有关认证业务的相关标准进行更新；
3. 认证系统和有关管理规范发生重大升级或改变；
4. 法律法规和主管部门要求；
5. 现有 CP 出现重要缺陷。

9.13 争议解决条款

当 GDCA、订户和依赖方之间出现争议时，有关方面应依据协议通过协商解决，

协商解决不了的，可通过法律解决。

9.14 管辖法律

GDCA 的 CP 受国家已颁布的《中国人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》法律法规管辖。

9.15 符合适用法律

认证机构的所有业务、活动、合同、协议必须符合《中国人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》以及其它中华人民共和国法律法规的规定。

9.16 一般条款

9.16.1 完整协议

CP、CPS、订户协议、依赖方协议及其补充协议将构成 PKI 参入者之间的完整协议。

9.16.2 让渡

根据本 CP 中详述的认证实体各方的权利和义务，各方当事人可按照法律的相关规定进行权利和义务的转让。此转让行为发生时不影响到转让方对另一方的任何债务及责任的更新。

9.16.3 分割性

如果本 CP 的任何条款或其应用遭遇如当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，那么本 CP 其余的部分可独立于这一条款而继续执行。

9.16.4 强制执行

无规定。

9.16.5 不可抗力

依据本 CP 制定的 CPS 应包括不可抗力条款，以保护各方利益。

9.17 其他条款

GDCA 对本 CP 具有最终解释权。