数安时代科技股份有限公司

电子政务电子认证

证书策略和业务规则

版本：V2.1 **生效日期：2025 年 1 月 13 日**

目　　录

1 概括性描述

1.1 概述

1.1.1 公司简介

数安时代科技股份有限公司（Global Digital Cybersecurity Authority Co., Ltd.，简称 GDCA 或“数安时代”），原为“广东数字证书认证中心有限公司”，成立于 2003 年 3 月 6 日。2005 年 9 月，GDCA 依法通过了国家密码管理局和原国家信息产业部的资格审查，成为全国首批八家获得《电子认证服务许可证》（许可证号：ECP44010215007）的电子认证服务机构之一；2008 年 12 月，获得国家密码管理局颁发的《商用密码产品销售许可证》；2011 年 4 月，通过了国家密码管理局电子政务电子认证服务能力评估，获得《电子政务电子认证服务机构》（编号：A021）资格。2013 年，对电子认证服务系统进行 SM2 算法升级，并通过了国家密码管理局组织的安全性审查。2015 年，GDCA 通过了 WebTrust 国际安全审计认证，具备了国际标准化的运营管理和服务水平，可以提供全球化的电子认证服务。为适应业务发展需要，2016 年 5 月，“广东数字证书认证中心有限公司”更名为“数安时代科技股份有限公司”。2017 年 8 月 11 日，GDCA 开始在新三板挂牌交易，股票简称：数安时代，股票代码：871932。

GDCA 更名后，原“广东数字证书认证中心有限公司”的资产、债务、权益和经营业务全部由“数安时代科技股份有限公司”承继。在更名前与 GDCA 以“广东数字证书认证中心有限公司”名义签订的合同、协议项下应由“广东数字证书认证中心有限公司”享有的权利和承担的义务均由“数安时代科技股份有限公司”承继。

数安时代秉持“权威、公信、专业、创新”的企业价值观，履行“信任联接天下”的企业使命，致力于成为“一流的网络信任服务商”。

1.1.2 电子政务电子认证证书策略和业务规则（CP/CPS）

本电子政务电子认证证书策略和业务规则根据国家相关法律法规的要求，详细阐述了 GDCA 在电子政务领域提供的电子认证服务整个过程、电子认证业

务所遵循的规范以及电子政务电子认证服务各方所承担的责任范围等。本规范适用于 GDCA 以及分支机构，并通过公开发布的渠道告知电子签名证书持有者、依赖方等相关参与者，以确保 GDCA 在电子政务领域所提供的电子认证服务是权威、安全、可靠的规范化第三方服务。对于 GDCA 所提供的认证服务过程的责任范围，本证书策略和业务规则也给予了明确的规定。

1.2 文档名称与标识

本文档称作《数安时代科技股份有限公司电子政务电子认证证书策略和业务规则》（简称《GDCA 电子政务 CP/CPS》），CP/CPS 为“Certificate Policy/Certificate Practice Statement”的缩写。在本文档中，电子政务 CP/CPS 等同于本节中定义的文档名称和适用名称。

1.3 电子政务电子认证活动参与者

1.3.1 电子政务电子认证服务机构

电子政务电子认证活动参与者包括但不限于电子政务电子认证服务机构、电子政务注册机构、电子政务证书持有者、电子政务依赖方和电子政务其他参与者。本 CP/CPS 的电子政务依赖方是指政务部门，电子政务证书持有者是指政务部门或面向政务部门的企事业单位、社会团体、社会公众。

1.3.2 注册机构

GDCA 的数字证书电子政务注册机构（下文简称注册机构）是经 GDCA 正式授权后的业务分支机构，包括证书注册审核（RA）中心、证书本地受理（LRA）点等。注册机构是为 GDCA 的证书申请者建立注册过程的实体。

1.3.3 证书持有者

在电子签名应用中，电子政务证书持有者（下文简称证书持有者）即是电子签名人、证书持有人，证书持有者包括 GDCA 颁发证书的所有最终用户，可以是个人、机构或基础设施的组成部件如路由器、防火墙、服务器或在组织中用于安全通信的其他设备。

1.3.4 依赖方

GDCA 的证书电子政务依赖方（下文简称依赖方）是指基于对 GDCA 提供电子政务电子认证活动中电子签名的信赖而从事有关活动的实体。该实体可以是，也可以不是 GDCA 的一个证书持有者。

1.3.5 其他参与者

电子政务其他参与者（下文简称其他参与者）是指为 GDCA 的电子政务电子认证活动提供相关服务的其他实体。

1.4 证书应用

1.4.1 适合的证书应用

GDCA 签发的数字证书常见的应用范围包括电子商务、电子政务及其他社会信息化等领域的应用，以确保互联网上信息传递双方身份的合法性和真实性以及信息的完整性和保密性。根据证书的功能以及使用证书的实际应用，目前 GDCA 签发的电子政务证书类型包括：

1. 个人类型：颁发给各级政务部门的工作人员和参与电子政务业务的社会公众的证书，用以代表个体的身份，如：某局局长、某局员工或参加纳税申报的个人的身份证书等。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等，在不违背相关法律法规、本 CP/CPS 以及证书持有者协议的情况下，此类证书也可用于其他用途。
2. 机构类型：颁发给机构的数字证书，即用以代表政务机关和参与电子政务业务的企事业单位、社会团体或其他组织的身份，如：代表单位和部门等机构身份证书。此类证书通常用于数字签名、加解密以及网上身份认证等，在不违背相关法律法规、本 CP/CPS 以及证书持有者协议的情况下，也可用于其他用途。
3. 设备类型：为电子政务系统中的服务器或设备颁发的数字证书，用以代表服务器或设备身份的真实性，如：服务器身份证书、SSL 服务器证书、IPSec VPN 设备证书等。此类证书通常用于网上设备的身份认

证，在不违背相关法律法规、本 CP/CPS 以及证书持有者协议的情况下，也可用于其他用途。

4. 其他类型证书：为满足电子政务相关应用的特殊需求而提供的其他应用类型的证书，如：代码签名证书等。

1.4.2 限制的证书应用

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证书，也禁止在任何违法犯罪活动或法律禁止的相关业务下使用证书，否则由此造成的法律后果由证书持有者自行承担。

1.5 策略管理

GDCA 安全策略委员会是 GDCA 在电子政务领域电子认证服务所有策略的最高管理机构，负责审核批准电子政务 CP/CPS。

1.5.1 策略文档管理机构

策略文档管理机构为 GDCA 安全策略委员会，作为策略管理机构负责制订、发布、更新本电子政务 CP/CPS。GDCA 安全策略委员会由公司管理层、行政中心、技术中心、运营服务中心等拥有决策权的合适代表组成。

本策略文档的对外咨询服务等日常工作由行政管理部门负责。

1.5.2 联系人

GDCA 将对电子政务 CP/CPS 进行严格的版本控制，并由 GDCA 指定专门的机构负责相关事宜。任何有关本 CP/CPS 的问题、建议、疑问等，都可以按以下方式进行联系。

- 联系部门：GDCA 行政管理部门
- 联系人：王女士
- 网站地址：https://www.gdca.com.cn/
- 电子邮箱地址：GDCA@gdca.com.cn
- 联系地址：中华人民共和国广东省广州市越秀区越华路 112 号珠江国

际大厦 30 楼 3001 室

- 邮政编码：510030
- 电话号码：020-83487228

1.5.3 决定 CP/CPS 符合策略的机构

GDCA 安全策略委员会是决定电子政务 CP/CPS 符合策略的机构。

1.5.4 CP/CPS 批准程序

本机构的电子政务 CP/CPS 由 GDCA 安全策略委员会组织 CP/CPS 编写小组拟定文档，CP/CPS 编写小组完成后提交 GDCA 安全策略委员会审核，经该委员会批准后，正式在 GDCA 官方网站上发布，从对外发布之日起三十日之内向国家密码管理局备案。

1.5.5 CP/CPS 修订

GDCA 根据国家的政策法规、技术要求、标准的变化及业务发展情况及时修订本电子政务 CP/CPS，CP/CPS 编写小组根据相关的情况拟定电子政务 CP/CPS 修订建议，提交 GDCA 安全策略委员会审核，经该委员会批准后，正式在 GDCA 官方网站上发布。

修订后的 CP/CPS，从对外发布之日起三十日之内向国家密码管理局备案。

2 规则依据文件

本《电子政务电子认证证书策略和业务规则》以下列文件为依据：

《中华人民共和国电子签名法》 中华人民共和国主席令（第十八号）2019 年

《电子政务电子认证服务管理办法》	国家密码管理局	2024 年
《电子认证服务密码管理办法》	国家密码管理局	2017 年
《电子政务电子认证服业务规则规范》	国家密码管理局	2019 年
《电子政务数字证书格式规范》	国家密码管理局	2010 年
《证书应用综合服务接口规范》	国家密码管理局	2023 年
《电子政务电子认证基础设施建设要求》	国家密码管理局	2010 年
《电子政务电子认证服务质量评估要求》	国家密码管理局	2019 年

《信息安全技术 证书认证系统密码及其相关安全技术规范》 国家标准 2018 年

3 术语和定义

数字证书	由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。
数字签名	通过使用非对称密码加密系统对电子记录进行加密、解密变换来实现的一种电子签名。
鉴别	确定个人、组织或事物如其所声称的人或事物的过程。在 PKI 上下文中，鉴别指的是确定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正确的个人或组织的过程。
实体鉴别	确认一个实体所声称的身份
验证	对证书申请者进行身份标识的过程。验证是身份标识的子集，并且在建立证书申请者身份的过程中指的就是身份标识。
密码算法	描述密码处理过程的一组运算规则或规程。
电子认证服务	是指为电子签名相关各方提供真实性、可靠性验证的活动。
电子认证服务机构	GDCA 及授权的下级操作中级 CA 被称为电子认证服务机构（Certificate Authority，CA），也就是证书认证机构，是颁发证书的实体。
证书注册机构	CA 批准的一个实体，它帮助证书申请者申请证书，批准或拒绝证书申请，撤销证书或更新证书。
证书撤销列表	一个定期(或根据要求)发行的、并由发证机关数字签名的信息列表，用来识别在有效期内提前被撤销的证书。这个列表通常标明 CRL 发布者的名字，发布的日期，下一次 CRL 发布的日期，被撤销证书的序列号，撤销证书的时间和原因。
证书持有者	拥有电子政务电子认证服务机构签发的有效证书的实体。
证书申请者	申请从电子政务电子认证服务机构获得证书的实体。
证书依赖方	信赖一个证书或一个数字签名的个人或组织机构。

4 符号和缩略语

GDCA	Global Digital Cybersecurity Authority CO., LTD.	数安时代科技股份有限公司
CA	Certificate Authority	认证机构
RA	Registration Authority	注册机构
CRL	Certificate Revocation List	证书撤消列表
FAQ	Frequently Askde Questions	经常问到的问题
USB KEY	Universal Serial Bus Key	采用 USB 接口的证书存储介质
KM	Key Management Center	密钥管理中心
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
LRA	Local Registration Authority	本地注册受理点
CPS	Certification Practice Statement	电子认证业务规则
OCSP	Online Certificate Status Protocol	在线证书状态查询协议
PIN	Personal Indentification Number	个人身份识别码
PKCS	Public KEY Cryptography Standards	公开密钥密码标准
PKI	Public Key Infrastructure	公开密钥基础设施
RFC	Request For Comments	请求评注标准(一种互联网建议标准)
X.509		国际电信同盟认证体系的证书标准

5 管理规范

5.1 管理机构

同本 CP/CPS 1.5.1、1.5.3。

5.2 联系方式

同本 CP/CPS 1.5.2。

5.3 CP/CPS 批准程序

同本 CP/CPS 1.5.4、1.5.5。

6 电子政务电子认证服务业务要求

GDCA 电子政务电子认证服务严格按照《电子政务电子认证服务管理办法》所规定的服务内容及要求开展。

6.1 数字证书服务

6.1.1 服务内容

GDCA 面向电子政务活动中的政务部门和企事业单位、社会团体、社会公众等电子政务用户提供证书申请、证书签发、证书更新、证书撤销等证书生命周期管理服务。

6.1.2 数字证书类型

GDCA 提供以下类型的数字证书：

1. 机构证书：用以代表政务机关和参与电子政务业务的企事业单位、社会团体或其他组织的身份，如：代表单位和部门等机构身份证书等。
2. 个人证书：为各级政务部门的工作人员和参与电子政务业务的社会公众颁发的证书，用以代表个体的身份，如：某局局长、某局职员或参加纳税申报的个人的身份证书等。
3. 设备证书：为电子政务系统中的服务器或设备颁发的数字证书，用以代表服务器或设备身份的真实性，如：服务器身份证书、SSL 服务器证书、IPSec VPN 设备证书等。
4. 其他类型证书：为满足电子政务相关应用的特殊需求而提供的其他应用类型的证书，如：代码签名证书等。

以上各类数字证书格式符合《电子政务数字证书格式规范》的要求，在标识实体名称时，保证了实体身份的唯一性，且名称类型支持 X.500、RFC-822、X.400 等标准协议格式。

6.1.3 身份标识与鉴别

6.1.3.1 命名

GDCA 严格按照《电子政务数字证书格式规范》的要求为电子政务数字证书命名。

6.1.3.1.1 名称类型

GDCA 颁发的数字证书，含有颁发机构和证书持有者主体甄别名。GDCA 对证书申请者的身份和其它属性进行鉴别，并以不同的标识记录其信息。证书持有者的标识命名，以甄别名（Distinguished Name）形式包含在证书主体内，是证书持有者的唯一识别名。GDCA 的证书符合 X.509 标准，分配给证书持有者实体的甄别名，采用 X.500 标准命名方式。

GDCA 证书颁发机构的主体甄别名命名规则如下：

属性	值
国家（C）	CN
省（S）	证书颁发者所在省份，或者不用
地区（L）	证书颁发者所在城市，或者不用
机构（O）	Guang Dong Certificate Authority Co.,Ltd 或 Global Digital Cybersecurity Authority Co., Ltd.
机构部门（OU）	GDCA 可能依据用户类型、应用领域、区域的不同采用不同的颁发者为用户颁发证书，所以 GDCA 证书中可以包含不同的颁发者名称。
通用名（CN）	此属性为 CA 名

GDCA 证书持有者的主体甄别名命名规则如下：

属性	值
国家（C）	CN
省（S）	证书持有者所在省份，或者不用
地区（L）	证书持有者所在城市，或者不用
机构（O）	机构属性如下定义： 对于有确定机构的证书持有者，是证书持有者所在机构名称。
机构部门（OU）	可以包含以下一个或多个内容：

	证书持有者所在机构的具体部门； 其他描述身份或证书类型的文字。
电子邮件（E）	证书持有者的电子邮件地址，或者不用
通用名（CN）	域名（设备证书），或机构名（机构类型证书），或个人姓名（个人类型证书），或其他可识别的名称

6.1.3.1.2 对名称意义化的要求

DN 项中的名称标识符具有一定的代表性意义，可为个人证书持有者的身份证号码、机构证书持有者的机构代码等。

6.1.3.1.3 证书持有者的匿名或伪名

本 CP/CPS 规定，GDCA 的证书申请者在进行电子证书申请时不能够使用匿名或伪名。

6.1.3.1.4 理解不同名称的形式的规则

GDCA 签发的电子证书符合 X.509 V3 标准，甄别名格式遵守 X.500 标准。甄别名的命名规则由 GDCA 定义。

6.1.3.1.5 名称的唯一性

在 GDCA 信任域内，不同证书申请者的证书的主体甄别名不能相同，必须是唯一的。但对于同一证书申请者，GDCA 可以用其唯一的主体甄别名为其签发多张证书。当证书申请中出现不同证书申请者存在相同名称时，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。

6.1.3.1.6 商标的识别、鉴别与角色

GDCA 不接受使用商标作为名称标识符的证书申请者申请。

6.1.3.2 证书申请人的身份确认

6.1.3.2.1 证明持有私钥的方法

GDCA 通过两个条件来证明证书申请者对私钥的持有：

（1)通过证书请求中所包含的数字签名来证明证书申请者持有与注册公钥对应的私钥。

a）证书申请者在客户端生成公私钥对；

b) 证书申请者使用私钥对证书请求信息签名，并连同公钥一同提交 CA 系

统；

c) CA 使用证书申请者公钥验证证书申请者签名。

（2）证书持有者必须妥善保管自己的私钥，即只有证书持有者可以持有私钥。

6.1.3.2.2 组织机构身份的鉴别

申请机构证书应按要求提交相关的申请资料，如合法身份证明文件、授权文件等。

GDCA 必须对上述材料进行审核以及对证书申请者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政府批文等，或通过签发有效文件的权威第三方数据库确认。
2. 确认经办人是否得到足够的授权，检查组织机构授权给经办人申请办理证书事宜的授权文件及核查经办人有效身份证件。
3. 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。

GDCA 根据审核和鉴证结果，作出批准申请或拒绝申请的操作，如批准申请，GDCA 将保留相关证明材料，与申请表一并存档保存。

6.1.3.2.3 个人身份的鉴别

申请个人证书应按要求提交相关的申请资料，如合法身份证明文件、授权申请文件等。合法的身份证明文件包括：身份证、户口簿、护照、军官证、警官证等。

GDCA 必须对上述材料进行审核以及对证书申请者的身份进行鉴证，包括如下内容：

1. 确认个人身份的真实性和有效性。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。

3. 把证书签发给政府部门个人时，还应进行以下鉴证工作：申请人提交由所属政府部门签章的证明文件，明确组织、部门与证书中所列的名称一致。

GDCA 根据审核和鉴证结果，作出批准申请或拒绝申请的操作，如批准申请，GDCA 将保留相关证明材料，与申请表一并存档保存。

6.1.3.2.4 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 必须对证书申请者进行身份鉴证，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，证书申请者为机构的，按照本电子政务 CP/CPS 6.1.3.2.2 节描述执行；证书申请者为个人的，身份鉴别按照本电子政务 CP/CPS 6.1.3.2.3 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。

6.1.3.2.5 不进行验证的证书申请者信息

证书中的信息必须经过验证，未经验证的信息不得写入证书。

6.1.3.2.6 授权确认

机构证书申请者可授权经办人来办理数字证书业务，但需要在相关业务表格上加盖单位有效公章，并提供授权文件，作为机构对经办人的授权确认。

6.1.3.2.7 互操作准则

对于其他的电子认证服务机构，可以与 GDCA 进行互操作，并且与 GDCA 签署相应的协议。

GDCA 将依据协议的内容，接受非 GDCA 的发证机构鉴别过的信息，并为之签发相应的证书。

如果国家法律法规对此有规定，GDCA 将严格予以执行。

6.1.3.3 密钥更新请求的标识与鉴别

在证书持有者证书到期前，证书持有者需要获得新的证书以保持证书使用的连续性。GDCA 一般要求证书持有者产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。然而，在某些情况下，允许证书持有者为一个现存的密钥对

申请一个新证书，称作“证书更新”。对于密钥更新而言，证书持有者证书除公钥、有效期和序列号改变外，其他信息都没改变；对于证书更新而言，和密钥更新相比，证书持有者证书公钥也不改变。

6.1.3.3.1 常规的密钥更新请求的标识与鉴别

对于一般正常情况下的更新密钥申请，证书持有者须提交能够识别原证书的足够信息，如证书持有者甄别名、证书序列号等，对申请的鉴别基于以下几个方面：

- 申请对应的原证书存在并且由认证机构签发；
- 用原证书上的证书持有者公钥对申请的签名进行验证；
- 基于原注册信息进行身份鉴别。

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，证书持有者在申请密钥更新前，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。

6.1.3.3.2 撤销后密钥更新请求的标识与鉴别

GDCA 不提供证书被撤销后的密钥更新。

6.1.3.4 撤销请求的标识与鉴别

当 GDCA 或注册机构有充分的理由撤销证书持有者的证书时，有权依法撤销证书，这种情况无须进行鉴证。如果证书持有者主动要求撤销证书，则按照本 CP/CPS 6.1.3.2 节描述进行身份鉴别。

6.1.4 数字证书服务操作要求

6.1.4.1 证书申请

6.1.4.1.1 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)。

6.1.4.1.2 注册过程与责任

1. 证书的注册过程

- 证书申请者填写相应的证书申请表单。
- 证书申请者携带相应的证明材料到 GDCA 的注册机构（RA 或 LRA）

进行证书申请，注册机构审核通过后，录入申请资料。其中审核员和信息录入员分别为两个不同的系统操作人员。

- 注册机构向 GDCA 提交证书请求，通过应用安全协议发送至 GDCA。
- 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）将证书交付给证书申请者。

2. 责任

- 证书申请者有责任向 GDCA 提供真实、完整和准确的证书申请信息和资料。
- 注册机构承担对证书申请者提供的证书申请信息与证明资料的一致性检查工作，同时承担相应审核责任。
- 注册机构对申请材料有保密的责任。

6.1.4.2 证书申请处理

6.1.4.2.1 识别与鉴别功能

当 GDCA 及其注册机构接受到证书申请者的证书申请后，应按本 CP/CPS 6.1.3.2.2、6.1.3.2.3 及 6.1.3.2.4 的要求，对证书申请者进行身份识别与鉴别。

GDCA 在处理证书申请过程中，将通过有效手段确保证书信息与正确的申请信息相符，并将证书签发给正确的申请者。

6.1.4.2.2 证书申请批准和拒绝

1. 证书申请的批准

如果符合下述条件，注册机构（RA）可以批准证书申请：

1) 该申请完全满足本 CP/CPS6.1.3.2 关于证书申请者身份的标识和鉴别规定；
2) 申请者接受或者没有反对证书申请者协议的内容和要求；
3) 申请者已经按照规定支付了相应的费用。

2. 证书申请的拒绝

如果发生下列情形，注册机构（RA）可以拒绝证书申请：

1) 该申请不符合本 CP/CPS 6.1.3.2 关于证书申请者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证书申请者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。

如果申请者未能成功通过身份鉴别，GDCA 将拒绝申请者的证书申请，并立即通知申请者证书申请失败。

6.1.4.2.3 处理证书申请的时间

在证书申请者提交资料齐全并符合要求的情况下，GDCA 将在 48 小时内作出响应，并在 7 个工作日内完成证书申请处理。

注册机构能否在上述时间期限内处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了 GDCA 的管理要求。

6.1.4.3 证书签发

6.1.4.3.1 证书签发中注册机构（RA）和电子认证服务机构（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，证书签发系统签发证书。

GDCA 在批准证书申请之后，将签发证书。证书的签发意味着电子政务电子认证服务机构最终完全正式地批准了证书申请。

通常 GDCA 签发的证书在 24 小时内生效。

6.1.4.3.2 电子认证服务机构（CA）和注册机构（RA）通知证书申请者证书的签发

GDCA 会采取以下几种通告方式告知证书申请者：

1、通过面对面的方式，通知证书申请者（如申请者到受理点领取等方式）；

2、邮政信函结合电子邮件的方式；

3、其他 GDCA 认为安全可行的方式。

6.1.4.4 证书接受

6.1.4.4.1 构成接受证书的行为

1、证书申请者自行访问专门的 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证书持有者接受了证书。

2、GDCA 注册机构代替证书申请者下载证书，下载的证书将被保存在数字证书载体中，当证书持有者接受了该数字证书载体即代表证书持有者接受了证书。

3、订户接受了获得证书的方式，并且没有提出反对证书或者证书中的内容。

4、订户反对证书或者证书内容的操作失败。

在证书持有者接受到证书后，证书持有者应立即对证书进行检查和测试。

6.1.4.4.2 电子认证服务机构对证书的发布

证书持有者接受证书后，对于证书申请者明确表示拒绝发布证书信息的，GDCA 不发布该证书信息。没有明确表示拒绝的，GDCA 在规定的时间内将该证书持有者证书发布到 GDCA 的目录服务系统。

6.1.4.4.3 电子认证服务机构对其他实体的通告

除证书持有者外，GDCA 及注册机构将不对其他实体进行通告。

6.1.4.5 密钥对和证书的使用

6.1.4.5.1 证书持有者的私钥和证书的使用

证书申请者在提交了证书申请并接受了 GDCA 所签发的证书后，均视为已经同意遵守与 GDCA、依赖方有关的权利和义务的条款。证书持有者接受到电子证书，应妥善保存其证书对应的私钥。

证书持有者只能在适用的法律、本 CP/CPS 以及订户协议规定的范围内使用私钥和证书，对于签名证书，其私钥可用于对信息的签名，证书持有者应知悉并确认签名的内容。对于加密证书，其私钥可用于对采用对应公钥加密的信息进行解密。在证书到期或被撤销之后，证书持有者必须停止使用该证书对应的私钥。

6.1.4.5.2 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依赖方信任的证书；

3) 通过查询 CRL 或 OCSP 确认该签名对应的证书是否被撤销；

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；

6）检查证书的有效期。

以上条件不满足的话，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。

6.1.4.6 证书与密钥更新

证书更新是指密钥不变，证书有效期延长，指在不改变证书注册信息的情况下，为证书持有者签发一张新证书。密钥更新是指密钥和证书同时更新。被撤销和已过期的证书不能进行密钥更新和证书更新。密钥更新业务规则参照证书更新执行。

6.1.4.6.1 证书更新的情形

对于 GDCA 签发给证书持有者的证书，证书持有者在证书到期前可进行证书更新。到期前，证书持有者可访问 GDCA 证书服务网站或者到 GDCA 的注册机构进行证书更新的申请。申请证书更新无需填写注册信息，系统会自动获取所需的信息。

6.1.4.6.2 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. 证书私钥泄露而撤销证书。
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。

出现上述情况，除非证书持有者特别要求，GDCA 一般建议证书持有者不进行证书密钥更新操作，而是注销原有证书，重新按证书申请的要求申请新证书。

6.1.4.6.3 证书更新申请的提交

证书持有者、证书持有者的授权代表（如机构证书等）或证书对应实体的拥有者（如设备证书等）在证书满足更新条件时，应按要求向注册机构提出更新申请。可采取当面提交更新申请表或在线提交带有证书持有者数字签名的更新申请。

6.1.4.6.4 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. 证书持有者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。

6.1.4.6.5 颁发新证书时对证书持有者的通告

同本 CP/CPS6.1.4.3.2。

6.1.4.6.6 构成接受更新证书的行为

同本 CP/CPS6.1.4.4.1。

6.1.4.6.7 电子认证服务机构对更新证书的发布

同本 CP/CPS6.1.4.4.2。

6.1.4.6.8 电子认证服务机构对其他实体的通告

同本 CP/CPS 6.1.4.4.3。

6.1.4.7 证书补办

补办是指在证书有效期限内，证书持有者出现证书载体丢失或证书载体损坏时进行证书补发的操作。补发操作成功时，旧证书将被撤销，新证书有效期从补发成功之日起到旧证书失效日止。证书补办业务的操作流程，按照证书申请的身份鉴别和受理流程执行。

6.1.4.8 证书变更

证书变更指改变证书中除证书持有者公钥之外的信息而签发新证书的情形。

6.1.4.8.1 证书变更的情形

如果证书持有者提供的注册信息发生改变，必须向 GDCA 提出证书变更。

如果证书内包含信息的变更可能影响证书持有者权利义务的改变，则证书持有者不能申请证书变更，只能撤销该证书，再重新申请新的证书。

证书变更的申请和证书申请所需的流程、条件是一致的。

6.1.4.8.2 请求证书变更的实体

请求证书变更的实体为证书持有者。

6.1.4.8.3 证书变更请求的处理

证书变更按照初次申请证书的注册过程进行处理。

6.1.4.8.4 颁发新证书时对证书持有者的通告

同本 CP/CPS 6.1.4.3.2。

6.1.4.8.5 构成接受变更证书的行为

同本 CP/CPS 6.1.4.4.1。

6.1.4.8.6 电子认证服务机构对变更证书的发布

同本 CP/CPS 6.1.4.4.2。

6.1.4.8.7 电子认证服务机构对其他实体的通告

同本 CP/CPS 6.1.4.4.3。

6.1.4.9 证书撤销

6.1.4.9.1 证书撤销的情形

当发现以下的情况，证书必须被撤销：

1) 政务机构的证书持有者不从事原岗位工作；
2) 司法机构要求撤销证书持有者证书；
3) 证书持有者提供的信息不真实；
4) 证书持有者没有或无法履行有关规定和义务；
5) 认证机构、注册机构或证书持有者有理由相信或强烈的怀疑一个证书持有者的私钥安全已经受到损害；
6) 政务机构有理由相信或强烈怀疑其下属雇员的私钥安全已经受到损害；
7) 和证书持有者达成的证书持有协议已经终止；
8) 证书持有者请求撤销其证书；
9) 法律法规规定的其他情形。

6.1.4.9.2 请求证书撤销的实体

证书持有者、注册机构、GDCA、证书持有者所属的组织机构或证书使用唯一依赖方有权发起证书撤销申请。

6.1.4.9.3 撤销请求的流程

1. 证书持有者主动提出注销申请

1) 证书持有者向注册机构提出证书注销申请，并填写《证书业务申请表》。注册机构核实申请撤销实体的身份和授权实体的身份。

2) 注册机构将《证书业务申请表》提交给 GDCA，由 GDCA 完成撤销。

2. 证书持有者被强制撤销证书

1) 当 GDCA 或注册机构有充分的理由需要撤销证书持有者的证书时，GDCA 或注册机构的有关人员可以通过内部确定的流程提请撤销证书。

2) 在证书撤销后，GDCA 或注册机构将通过适当的方式，包括邮件、电话、传真等，通知证书持有者证书已被撤销及被撤销的理由。若未能联络证书持有者时，在必要的情况下，GDCA 对撤销的证书将通过网站进行公告。

6.1.4.9.4 撤销请求宽限期

如果出现密钥泄露或有泄露嫌疑等事件，撤销要求必须在泄密或有泄密嫌疑 8 小时以内发现提出。其他撤销原因的撤销要求必须在变更前的 48 小时内提出。

6.1.4.9.5 电子认证服务机构处理撤销请求的时限

GDCA 处理撤销请求的周期为 24 小时。

6.1.4.9.6 依赖方检查证书撤销的要求

GDCA 提供在线撤销状态查询，依赖方可在 GDCA 的网站上进行查询。

6.1.4.9.7CRL 发布频率

GDCA 的 CRL 发布周期为 8 小时，即在 8 小时内发布最新 CRL。但在特殊紧急情况下可以使 CRL 立即生效（假使网络传输条件能够保证），CRL 的立即生效由 GDCA 制定的发布策略决定。

6.1.4.9.8CRL 发布的最大滞后时间

GDCA 的 CRL 发布最大滞后时间为发布周期之后的 24 小时内。

6.1.4.9.9 在线状态查询的可用性

GDCA 提供证书状态在线查询服务（OCSP），并提供 7*24 小时查询服务。

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

6.1.4.9.11 撤销信息的其他发布形式

GDCA 不提供撤销信息的其他发布形式。

6.1.4.10 证书状态服务

6.1.4.10.1 操作特征

证书持有者可以通过 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。

6.1.4.10.2 服务可用性

提供 7*24 小时的证书状态查询服务。即在网络允许的情况下，证书持有者能够实时获得证书状态查询服务。

6.1.4.10.3 可选特征

无规定。

6.1.4.11 订购结束

订购结束是指当证书有效期满或证书撤销后，该证书的服务时间结束。

订购结束包含以下两种情况：

1) 证书有效期满，证书持有者不再延长证书使用期或者不再重新申请证书时，证书持有者可以终止订购；
2) 在证书有效期内，证书被撤销后，即订购结束。

一旦用户在证书有效期内终止使用 GDCA 的证书认证服务，GDCA 在批准其终止请求后，将实时把该证书持有者的证书注销，并按照 CRL 发布策略进行发布；GDCA 定期将订购结束后的证书及相应证书持有者数据进行归档。

6.1.4.12 密钥生成、备份与恢复

6.1.4.12.1 密钥对生成

1. 签名密钥对生成

GDCA 证书申请者必须使用国家密码管理局批准许可的设备生成签名密钥对，例如由密码机、密码卡、USB Key、IC 卡等生成。证书申请者在选择这些设备前，应事先向 GDCA 咨询有关系统兼容和接受事宜。GDCA 向证书申请者提供符合国家密码管理相关规定的设备作为证书申请者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。

证书申请者签名密钥对的产生，必须遵循国家的法律政策规定。GDCA 支持多种模式的签名密钥对产生方式，证书申请者可根据其需要进行选择密钥生成模块。但是不管何种方式，密钥对产生的安全性都应该得到保证。GDCA 在技术、业务流程和管理上，已经实施了安全保密的措施。

证书持有者负有保护私钥安全的责任和义务，并承担由此带来的法律责任。

2. 加密密钥对生成与恢复

GDCA 证书申请者的加密密钥对由 GDCA 代证书申请者向 GDCA 密钥管理中心申请生成，并由 GDCA 密钥管理中心进行管理。当证书持有者需要恢复加密密钥时，按照 GDCA 密钥管理中心的规范、流程，接受证书持有者的申请，为证书持有者恢复相应的加密密钥。

3. 加密私钥传送给证书申请者

由证书签发机构代替证书申请者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证书申请者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证书申请者证书载体时，证书申请者使用自己的证书载体解密该私钥并存储。

4. 公钥传送给证书签发机构

证书申请者的签名证书公钥通过安全通道，经注册机构传递到 GDCA。

证书申请者的加密证书公钥，由 GDCA 密钥管理中心通过安全通道传递到 GDCA 中心。

从注册机构（RA）到 GDCA 以及从 GDCA 密钥管理中心到 GDCA 的传递过程中，采用国家密码管理局许可的通讯协议及密钥算法，保证了传输中数据的安全。

5. 电子认证服务机构公钥传送给依赖方

依赖方可以从 GDCA 的网站下载根证书和 CA 证书，从而得到 CA 的公钥。

6. 密钥的长度

SM2 CA 证书和证书申请者证书的密钥长度均为 256bit。RSA CA 证书的密钥长度为 4096bit，可签发密钥长度为 RSA2048bit 的证书申请者证书。

如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，GDCA 将会完全遵从。

7. 公钥参数的生成和质量检查

公钥参数必须使用国家密码管理局批准许可的加密设备和硬件介质生成。

对于参数质量的检查，同样由通过国家密码管理局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。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。

8. 密钥使用目的

证书持有者的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥对可以用于信息加密和解密。

6.1.4.12.2 会话密钥的封装与恢复的策略和行为

非对称算法组织数字信封的方式来封装会话密钥，数字信封使用信息接受者的公钥对会话密钥加密，接受者用自己的私钥解密并恢复会话密钥。

6.2 应用集成支持服务

6.2.1 证书应用接口程序

GDCA 提供应用接口程序供应用系统集成和调用，证书应用接口程序符合《GM/T 0020 证书应用综合服务接口规范》的要求，包括证书环境设置、证书解析、随机数生成、签名验证、加解密、时间戳以及数据服务接口等功能，并提供 C、C#、Java 等多种接口形态。

6.2.2 证书应用方案支持

GDCA 针对电子政务信息系统的实际业务需求，提供电子认证安全需求分析、电子认证法律法规、技术体系的咨询服务，并设计满足业务要求的电子认证及电子签名服务方案。

6.2.3 证书应用接口集成

GDCA 具备面向各类应用的证书应用接口集成能力，并能够达到以下要求：

1. 具备在多种应用环境下进行系统集成的技术能力，包括基于 Java、.NET 等 B/S 应用模式以及基于 C、VC 等 C/S 应用模式的系统集成能力。
2. 提供满足不同应用系统平台的证书应用接口组件包，包括 com 组件、java 组件、ActiveX 控件等。
3. 提供集成辅助服务，包括接口说明、集成手册、测试证书、集成示例、演示 DEMO 等。

6.3 信息服务

6.3.1 服务内容

根据政务部门对证书应用信息的管理及决策需求，GDCA 提供证书发放和应用情况信息汇总及统计分析的信息管理服务，信息服务包括：

1. 证书信息服务

GDCA 严格按照《电子政务电子认证服务业务规则规范》的要求和本《电子政务电子认证证书策略和业务规则》向用户提供数字证书申请、签发、存档、查询、废止等服务。

2. CRL 信息服务

GDCA 在证书申请者证书签发时，通过目录服务器自动将该证书公布，CRL 发布周期为 8 小时，即在 8 小时内发布最新 CRL。GDCA 每年签发一次电子认证服务机构证书的证书撤销列表。

3. 服务支持信息服务

GDCA 以页面和接口的形式提供查询服务，接口符合《GM/T 0020 证书应用综合服务接口规范》的要求。

4. 决策支持信息服务

GDCA 证书信息可为政府主管部门提供科学管理和领导决策提供可靠依据。

6.3.2 服务管理规则

GDCA 在提供信息服务时，做好相关信息的隐私保障机制，实现信息保护对用户的承诺。GDCA 对技术、客服等凡是能够接触用户信息的工作人员进行保密培训，并签署保密协议，严禁泄露或私自使用用户信息和业务信息。

1. 私有信息类型的敏感度

对于以下信息，GDCA 按照日常安全保密制度严格执行：

1) 企业、政府主管单位、政府办公人员等的隐私信息；

2) 集成商、应用系统开发商、合作伙伴等的商业秘密；

3) 政府部门的敏感信息和工作秘密。

证书发行过程中涉及的用户申请信息都是敏感信息，而发布的证书和 CRL 信息不属于敏感信息，证书发布根据用户要求进行公布或不公布。

2. 允许的私有信息收集

GDCA 仅允许在证书发行和管理时才能收集 CP/CPS 声明的私有信息，且只收集对发行和使用证书有用的私有信息。除了已与用户沟通确认外，GDCA 不收集更多的私有信息。

3. 允许的私有信息使用

GDCA 承诺只在 CA 或 RA 中使用私有信息。

若在某项业务中开展证书应用而获得的私有信息，在使用时，必须获得该业务应用单位的许可。

4. 私有信息的安全存储

GDCA 采取安全手段对用户私有信息进行安全存储，确保用户私有信息不发生泄露、未授权访问等安全事件。

5. 允许的个人信息发布

GDCA 和注册机构仅能面向证书应用单位发布与之相关的私有信息，协助证书应用单位进行证书业务管理。

任何特定的私有信息发布应遵循相关法律和政策执行。

6. 所有者纠正私有信息的机会

GDCA 允许用户在其证书生命周期内对其私有信息进行更正。

7. 对司法及监管机构发布私有信息

GDCA 或注册机构在以下情况下，可执行将私有信息发给获得相应授权的人员：

1) 根据国家相关法律法规，为司法机关提供私有信息；
2) 在私有信息所有者同意的情况下，可将私有信息提供给任何人；
3) 按照明确的法定权限的要求或许可。

6.3.3 服务方式

GDCA 的信息服务以页面或接口的形式面向应用系统或证书用户提供服务，接口符合《GM/T 0020 证书应用综合服务接口规范》的要求。

6.4 使用支持服务

6.4.1 服务内容

6.4.1.1 面向证书持有者的服务支持

数字证书管理：包括数字证书的导入、导出，以及客户端证书管理工具的安装、使用、卸载等。

数字证书应用：基于数字证书的身份认证、电子签名、加解密等应用过程中出现的各种异常问题，如：证书无法读取、签名失败、证书验证失败等。

证书存储介质硬件设备使用：包括证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等。

电子认证服务支撑平台使用：为用户提供在 GDCA 的数字证书在线服务平台中使用的各类问题，如：证书更新失败、下载异常、无法提交注销申请等。

6.4.1.2 面向应用提供方的服务支持

电子认证软件系统使用：提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等系统的使用支持问题，如证书信息无法查询、数据同步失败、服务无响应等。

电子签名服务中间件的应用：解决服务中间件在集成时出现的各种情况，

如客户端平台适用性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

6.4.2 服务能力

GDCA 提供多种服务方式，包括呼叫中心座席服务、在线服务、现场服务等，在 GDCA 官网上可查询相应的服务方式。

6.4.2.1 座席服务

用户拨打 GDCA 的服务热线，通过语音系统咨询证书应用问题，热线座席根据用户的问题请求，协助用户处理。

6.4.2.2 在线服务

在线服务通过提供自助信息查询系统、网络实时通讯系统、远程终端协助系统，以及在线帮助与传统模式的结合，满足用户多种服务帮助的需求。

自助信息查询系统：将知识库信息按照不同的类型、属性、层次等方式、结构进行分类存储，用户可以按照咨询问题或者已知条件在信息系统上进行记发式的检索，查找目标问题的答案。

网络实时通讯系统：用户通过在线帮助网站远程发起支持请求，网站客服人员能够第一时间同登陆网站的访客取得联系，进行交流。

远程终端协助系统：用户通过安装远程终端软件，可以通过互联网或者局域网向客户服务人员发起协助请求。由服务人员通过远程终端控制功能，实时检测用户的软件硬件环境，通过同屏显示指导、帮助用户解决应用故障。

在线帮助与传统模式的结合：将在线服务系统与电话服务结合，方便客户既可以打电话、也可以自助上网，随时查询自己的服务记录、请求处理状态、产品配置信息等等。

6.4.2.3 现场服务

根据用户的实际需求，由技术支持工程师上门现场为用户处理数字证书应用中存在的问题。

6.4.2.4 满意度调查

通过多种用户可接受的调查方式进行客户回访，包括电话、WEB 网站、邮件系统、短信、传真等。向用户提供调查表格以供用户填写，调查表格应清晰载明此次回访的目的及内容。并将用户回访中产生的相关文档进行归档、保存。

6.4.2.5 投诉受理

向用户公布电子政务电子认证服务监管部门的投诉受理方式。

可通过电话、网站平台、电子邮件、即时通讯工具等方式及时接受客户投诉，投诉受理过程中应记录投诉问题，并将结果及时反馈给用户。

将投诉受理中产生的相关文档进行归档、保存。

6.4.2.6 培训

培训方式由 GDCA 与客户双方约定的形式开展。

培训内容主要包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答、操作手册等。

6.4.3 服务质量

GDCA 坐席服务、在线服务、现场服务时间做到充分满足各类用户的需要。现场服务时间为 5 天*8 小时，线上提供正常工作时间话务响应服务及 7 天*24 小时自助服务。GDCA 设有专门的投诉热线受理和客户满意度调查，保证优质的客户服务质量。

应对技术问题和技术故障按照一般事件、严重事件、重大事件进行分类，制定响应处理流程和机制，以确保服务的及时性和连续性。

6.5 安全保障

6.5.1 认证机构设施、管理和操作控制

6.5.1.1 物理控制

1. GDCA 所在的物理环境严格按照《GM/T 0034 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》的要求实施，具有电磁屏蔽、消防、物理访问控制、入侵检测报警灯相关措施，并取得了相关部门的检测证书。

2. GDCA 所有员工佩戴标识身份的工牌，工作人员需使用身份识别卡或结合口令或指纹鉴定才能进出机房。
3. 所有门禁系统能够记录人员进出信息，记录信息能够保存六个月。
4. 针对不同的人员角色 GDCA 设置不同的访问权限，只有经过授权的人员才能进入相应的区域，非授权人员不能进入。
5. GDCA 采用双链路冗余供电线路和双链路网络线路。
6. 对于报废的存储介质，经过检查无残留信息后，通过物理损坏的方式进行销毁，对于含有敏感数据的存储介质，采用物理销毁或进行安全覆盖。
7. GDCA 办公场所有保安不间断执勤，监控室 24 小时有专人值班，每天有专人负责巡检机房设备。

6.5.1.2 操作过程控制

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、管理和撤销等涉及密钥操作的职位都被 GDCA 视为可信角色。这些角色包括但不限于：密钥和密码设备的管理人员、系统管理人员、安全审计人员、业务管理人员及业务操作人员等，具体岗位名称和要求以 GDCA 的岗位说明为准。

2. 每项任务需要的角色

GDCA 在具体业务规范中对关键任务进行严格控制，敏感操作需要多个可信角色共同完成，例如：

- 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
- 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
- 审核和签发证书：需要 2 个可信人员共同完成

3. 每个角色的识别与鉴别

GDCA 所有承担可信角色的在职人员都应经过一定程序的鉴证。鉴证程序在 GDCA 的人员聘用管理条例中规定。

4. 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，即 GDCA 的可信角色由不同

的人担任。GDCA 进行职责分离的角色，包括但不限于下列角色：

a） 证书业务受理

b） 证书或 CRL 签发

c） 系统工程与维护

d） CA 密钥管理

e） 安全审计

6.5.1.3 人员控制

6.5.1.3.1 资格、经历和无过失要求

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和良好的从业经历。
5. 无违法犯罪记录。

GDCA 要求充当可信角色的人员至少必须具备忠诚、可信赖及对工作的热诚、无影响 CA 运行的其它兼职工作、无同行业重大错误记录等。

6.5.1.3.2 背景审查程序

GDCA 或与有关的政府部门和调查机构合作，完成对可信员工的背景调查。

所有的可信员工和申请调入的可信员工都必须书面同意对其进行背景调查。背景调查分为：基本调查和全面调查。

基本调查包括对工作经历，职业推荐，教育，社会关系方面的调查。

全面调查除包含基本调查项目外还包括对犯罪记录，社会关系和社会安全方面的调查。

调查程序包括：

a) 人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

b) 人事部门通过电话、信函、网络、走访、等形式对其提供的材料的真实性进行鉴定。

c) 在背景调查中，对发现以下情形的人员，可以直接拒绝其成为可信人员的资格：

- 存在捏造事实或资料的行为；
- 借助不可靠人员的证明；
- 使用非法的身份证明或者学历、任职资格证明；
- 工作中有严重不诚实的行为。

d) 用人部门通过现场考核、日常观察、情景考验等方式对其考察。关键和核心岗位的人员通过录入考察期后，还需要额外期限的考察。根据考察的结果做出相应的安排。

e) 经考核，GDCA 与员工签订保密协议，以约束员工不许泄露 CA 证书服务的所有保密和敏感信息。同时，GDCA 还将按照本机构的人员管理相关条例对所有承担可信角色的在职人员进行职位考察，以便能够持续验证这些人员的可信程度和工作能力。

6.5.1.3.3 培训要求

GDCA 根据可信角色的职位需求，给予相应的岗前培训，综合培训内容如下：

- GDCA 运营体系；
- GDCA 技术体系；
- GDCA 安全管理机制；
- 岗位职责统一要求；
- PKI 基础知识；
- 身份验证和审核策略和程序；
- 灾难恢复和业务连续性管理；
- CP、CPS 政策及相关标准和程序；
- GDCA 管理政策、制度及办法等；
- 国家关于电子认证服务的法律、法规及标准、程序；
- 其他需要进行的培训等。

6.5.1.3.4 再培训周期和要求

GDCA 将根据系统升级、策略调整等要求，不定期的要求人员进行继续培

训。

6.5.1.3.5 工作岗位轮换周期和顺序

GDCA 在职人员的工作岗位轮换周期和顺序将依据本机构的安全管理策略而制定。

6.5.1.3.6 未授权行为的处罚

当出现在职人员未经授权或超出权限使用 GDCA 系统、操作认证业务等情况时，GDCA 一经确认，将立即撤销该人员的登录证书、同时终止其系统访问权限，并视该人员未授权行为的情节严重性，实施对该名人员的通报批评、罚款、辞退以及提交司法机构处理等措施。

6.5.1.3.7 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、管理人员等独立签约者，GDCA 的统一要求如下：

- 人员档案的备案管理；
- GDCA 提供统一的岗前培训辅导和再培训要求，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。

6.5.1.3.8 提供员工的文档

在培训或再培训期间，GDCA 提供给员工的培训文档包括但不限于以下几类：

- GDCA 员工手册；
- GDCA 证书策略、电子认证业务规则；
- GDCA 技术体系文档；
- GDCA 岗位职责说明书；
- 内部操作文件，包括业务连续性管理和灾难恢复方案等；
- GDCA 安全管理制度等。

6.5.1.4 审计日志程序

6.5.1.4.1 记录事件的类型

所有发生在 GDCA 的重大安全事件都会记录在审计跟踪档案中，这些记录，不论是手动生成或者是系统自动生成，都应该包含以下信息：

1. 事件发生的日期和时间；

2. 记录的序列号；
3. 记录的类型；
4. 记录的来源；
5. 记录事件的实体。

这些事件包括但不限于：

1. 密钥生命周期内的管理事件，包括密钥生成、备份、存储、恢复、使用、撤销、归档、销毁、私钥泄露等；
2. 密码设备生命周期内的管理事件，包括设备接收、安装、卸载、激活、使用、维修等；
3. 证书生命周期内的管理事件，包括证书的申请、批准、更新、撤销等；
4. 系统、网络安全事件，包括：成功或不成功访问 CA 系统的活动，系统日常运行产生的日志文件，系统变更、系统崩溃，硬件故障和其他异常等；
5. 信息安全设备记录的安全事件；
6. 系统操作事件，包括系统启动和关闭，系统权限的创建、删除，设置或修改密码；
7. CA 设施的访问，包括授权人员进出 CA 设施、非授权人员进出 CA 设施及陪同人和安全存储设施的访问；
8. 可信人员管理记录，包括系统权限的创建、删除及变更等。

6.5.1.4.2 处理日志的周期

GDCA 每月进行一次日志跟踪处理，检查违反政策及其它重大事件，每季度进行发证系统日志分析。所有的审计日志定期由专人进行检查和审阅，以便发现重要的安全和操作事件，及时采取相应的措施进行处理。

6.5.1.4.3 审计日志的保存期限

GDCA 妥善保存电子认证服务的审计日志，在数据库保存审计日志至少两个月，保存期限为电子签名认证失效后五年。

6.5.1.4.4 审计日志的保护

GDCA 的审计日志储存在数据库里，并且实现备份，其中包括有关文档中的审计信息和事件记录。GDCA 执行严格的物理和逻辑访问控制措施，以确保

只有授权人员才能接近这些审查记录，严禁未授权的访问、阅读、修改和删除等操作。

6.5.1.4.5 审计日志备份程序

GDCA 的审计跟踪文档由运维人员和审计人员每月进行审计日志和审计文档的归档备份。所有文档包括最新的审计跟踪文档应储存在磁盘中并存放在安全的文档库内。

6.5.1.4.6 审计收集系统

GDCA 审计日志收集系统涉及：

1) 证书管理系统；
2) 证书签发系统；
3) 证书目录系统；
4) 远程通信系统；
5) 证书受理系统；
6) 访问控制系统；
7) 网站、数据库安全管理系统；
8) 其他需要审计的系统。

GDCA 使用审计工具满足对上述系统审计的各项要求。

6.5.1.4.7 对导致事件实体的通告

GDCA 发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

GDCA 有权决定是否对导致事件的实体进行通告。

6.5.1.4.8 脆弱性评估

CA 安全程序根据政策、技术和管理的变化、重大变更及时进行薄弱环节分析，属于可以弥补的薄弱环节，及时弥补，属于不可弥补的薄弱环节，GDCA 每年对系统进行脆弱性评估，以降低系统运行的风险。

6.5.1.5 记录归档

GDCA 对以下几类事件进行归档记录，包括但不限于：

1. 证书系统建设和升级文档；

2. 证书和证书撤销列表；
3. 证书申请文档，证书服务批准和拒绝的信息，与证书持有者的协议；
4. 审计记录；
5. 证书策略、电子认证业务规则文档；
6. 员工资料，包括但不限于背景调查、录用、培训等资料；
7. 各类外部、内部评估文档。

6.5.1.5.1 归档记录的保存期限

对于不同的归档记录，其保留期限是不同的。对于系统操作事件和系统安全事件记录，其归档应保留到完成安全脆弱性评估或一致性审计。

1. 对证书持有者证书生命周期内的管理事件的归档，保留 5 年以上。
2. 对 CA 证书和密钥生命周期内的管理事件的归档，其保留期限不少于 CA 证书和密钥生命周期。
3. 用户申请资料、证书持有者证书的归档保留期限不少于证书失效后 5 年。
4. CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，额外保留 5 年。

6.5.1.5.2 归档文件的保护

审计跟踪文档的保护在以下章节中作详细说明。其中档案介质采用物理安全方式进行保护，并且保留一个严格限制的入口，只有 GDCA 的业务管理人员可以访问。

6.5.1.5.3 归档文件的备份程序

对于系统生成的电子归档记录，每周进行备份，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。

所有存档的文件和数据库除了保存在 GDCA 的存储库，还在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。GDCA 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。

6.5.1.5.4 记录时间戳要求

GDCA 的所有日志都有时间记录，均由操作人员手工记录或系统自动添加。

6.5.1.5.5 归档收集系统

GDCA 的审计跟踪档案收集系统在本 CP/CPS 6.5.1.4 节中作详细说明。

分离媒体数据存储和该媒体安全存储的归档不属于 GDCA 系统。

6.5.1.5.6 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 GDCA 档案信息的 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。

6.5.1.6 电子认证服务机构密钥的更替

在证书到期以前，GDCA 将按照证书策略的规定对根密钥进行更换，生成新的证书。在进行密钥的生成时，严格按照 GDCA 关于密钥管理的规范。CA 密钥更替必须遵循以下原则：

1. 在 CA 证书生命周期结束前停止签发新的下级证书，确保在 CA 的证书到期时所有下级证书也全部到期。
2. 在停止签发新的下级证书后至证书到期时，继续使用 CA 私钥签发 CRL，直到最后一张下级证书过期。
3. 生成和管理 CA 密钥对时，严格遵守密钥规范。
4. 及时发布新的 CA 证书。
5. 确保整个过渡过程安全、顺利，不出现信任真空期。

GDCA 的管理员证书密钥更换由 KM 业务管理员提出申请。密钥更换时，GDCA 需要签发三个新证书：

1. 新私钥签名的包含新公钥的 GDCA 证书；
2. 新私钥签名的包含旧公钥的 GDCA 证书；
3. 旧私钥签名的包含新公钥的 GDCA 证书。

6.5.1.7 数据备份

GDCA 建立数据备份管理机制，采用本地定时备份（Data Guard）、定时备份（EXP）、本地实时备份、异地定时备份和异地灾备系统备份相结合的方式备份重要数据库的数据。对关键系统数据，包括证书数据、系统配置数据、用户数据、审计日志数据和其他敏感信息进行异地备份，并确保其处于安全的设施内。

6.5.1.8 损害和灾难恢复

6.5.1.8.1 事故和损害处理程序

为了及时响应和处理事故和损害发生的情况，GDCA 建立了一系列应急处理预案和事故处理方案，例如：

1. GDCA 系统故障处理规范
2. GDCA 重大事故应急预案
3. GDCA 系统备份与恢复方案

相关岗位的工作人员将按照以上方案和相关制度的规定，积极实施抢修恢复计划和措施，每季度进行数据灾难恢复演练，每年进行一次重大事故应急演练。

6.5.1.8.2 计算资源、软件和或数据的损坏

GDCA 对业务系统及其他重要系统的资源、软件及数据进行了备份，并制定了相应的应急处理流程。当发生网络通信资源毁坏、计算机设备不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，GDCA 将按照灾难恢复计划实施恢复。

6.5.1.8.3 实体私钥损害处理程序

在故意的、人为的或是自然灾难的情况下，GDCA 将采取下列步骤以恢复安全环境：

1. GDCA 认证系统的口令由业务管理员、业务操作员、系统管理员进行变更。
2. 根据灾难的性质，部分或全部证书需要撤销或之后重新认证。
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。
4. 及时访问安全现场尽可能合理地恢复操作。
5. 如果需要恢复业务管理员的配置文件，应由系统管理员执行恢复。

如果需要恢复 GDCA 业务操作员的配置文件，则由另外一名 GDCA 安全业务操作员或业务管理员对其进行恢复。

当 CA 根私钥被攻破、遗失、被篡改或泄露，GDCA 启动重大事件应急处理程序，由安全策略委员会和相关的专家进行评估，制定行动计划。如果需要注销 CA 证书，将会采取以下措施：

1. 立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其他公共媒体对证书持有者进行通告，采取措施避免用户利益遭受更大损失。
2. 立即通知相关依赖方关闭与证书认证服务相关的系统。
3. 立即撤销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书持有者和依赖方查询。同时 GDCA 立即生成新的密钥对。
4. 新的根证书签发后，按照 GDCA CP/CPS 关于证书签发的规定，重新签发下级证书和下级操作中级 CA 证书。
5. GDCA 新的证书签发后，将立即通过 GDCA 信息库、目录服务器、HTTP 等方式发布。

当中级 CA 私钥出现遗失、被篡改、破解、泄露或被第三者窃用的疑虑时，操作 CA 应：

1. 立即向 GDCA 进行汇报并生成新的密钥对和证书请求，申请签发新的证书。
2. GDCA 立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其他公共媒体对证书持有者进行通告，采取措施避免用户利益遭受更大损失。
3. 立即通知相关依赖方关闭与证书认证服务相关的系统。
4. 立即撤销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书持有者和依赖方查询。
5. 新的中级 CA 证书签发后，按照 GDCA CP/CPS 关于证书签发的规定，重新签发证书持有者证书。
6. GDCA 新的证书签发后，将立即通过 GDCA 信息库、目录服务器、HTTP 等方式进行发布。

证书持有者的私钥可能出现损毁、遗失、破解、被篡改，或者被第三者窃用时，证书持有者应按照 GDCA 电子政务 CP/CPS 的规定，首先申请证书撤销，并按照规定重新申请新的证书。

6.5.1.8.4 灾难后的业务连续性能力

GDCA 在遭遇本节 6.5.1.8.1、6.5.1.8.2 和 6.5.1.8.3 中描述的灾难后，通过

其备份机制，将在 24 小时之内恢复各项业务的正常运行。

6.5.1.9 认证机构或注册机构终止

因各种情况，GDCA 需要终止运营时，将严格按照《电子政务电子认证服务管理办法》的要求，处理好相关承接事项，包括档案记录管理者的身份问题。

6.5.2 认证系统技术安全控制

6.5.2.1 密钥对的生成与安装

1）CA 密钥对的产生

CA 密钥对必须在安全的物理环境中，由多个可信人员在国家密码主管部门批准和许可的密码设备中生成。GDCA 密钥生成、保存的密码模块符合国家密码主管部门的要求，并通过国家密码主管部门的鉴定、认证。

2）证书持有者密钥对的产生

证书持有者在使用硬件密码模块时，必须使用国家密码管理局批准许可的设备生成签名密钥对，例如由密码机、密码卡、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 向证书持有者提供符合国家密码管理相关规定的设备作为证书持有者签名密钥对的生成和存储设备。

GDCA 一般不提供代证书持有者生成签名密钥对，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。

证书持有者的加密密钥对由 GDCA 代证书持有者向密钥管理中心申请生成，并由密钥管理中心进行管理。当证书持有者需要恢复加密密钥时，按照密钥管理中心的规范、流程，接受证书持有者的申请为证书持有者恢复相应的加密密钥。

6.5.2.2 私钥保护和密码模块工程控制

GDCA 所用的密码模块都是经国家密码管理局认可的产品，符合《GM/T 0028 密码模块安全技术要求》。

GDCA 私钥的生成、更新、撤销、备份和恢复等操作采用多人控制机制，即采取五选三方式，将私钥的管理权限分散到 5 位密钥管理员中，至少在其中三人在场并许可的情况下，插入管理员卡并输入 PIN 码，才能对私钥进行操作。

证书持有者的私钥由证书持有者自己通过密码设备控制，证书持有者有责任妥善保管私钥（签名证书）。

6.5.2.3 密钥对管理的其他方面

1. 公钥归档

对系统产生的公钥数据进行定时的归档保存，对保存的公钥信息进行对称加密，确保能获取安全完整的公钥信息。

公钥到期后，GDCA 在 10 天内完成归档操作。

2. 证书操作期和密钥对使用期限

证书的有效期是由 RA 注册审核系统中的证书颁发模板定制，证书颁发机构可以根据颁发证书业务类型的需求定义证书的操作期，目前 GDCA 签发的个人类型电子证书和机构类型电子证书的证书操作期为 3 年或以内，最长不超过 5 年；设备类型数字证书的证书操作期为 10 年或以内。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外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外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。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

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。

6.5.2.4 激活数据

1. 激活数据的产生和安装

为了保护私钥的安全，证书持有者生产和安装激活数据必须保证安全可靠，从而避免私钥被泄漏、被偷窃、被非法使用、被篡改、或者被非法授权的披露。

CA 私钥的激活数据，必须按照有关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。证书持有者私钥的激活数据，包括用于下载证书的口令（以密码信封等形式提供）、USBKey、IC 卡的登陆口令等，都必须在安全可靠的环境下随机产生。

GDCA 产生的激活数据，包括用于下载证书的口令（（以密码信封等形式提供）、USBKey、IC 卡的登陆口令等，都是在安全可靠的环境下随机产生。这些激活数据，都是通过安全可靠的方式，例如离线当面递交、邮政专递等方式交给证书持有者。对于非一次性使用的激活数据，GDCA 建议用户自行进行修改。

所有的保护口令都应该是不容易被猜到的，应该遵循以下几个原则：

- 至少 8 位字符
- 至少包含一个小写字母
- 不能包含很多相同的字符
- 不能和操作员的名字相同
- 不能使用生日、电话等数字
- 用户名信息中的较长的子字符串

2. 激活数据的保护

对于 CA 私钥的激活数据，必须将激活数据按照可靠的方式分割后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。

证书持有者的激活数据必须在安全可靠的环境下产生，必须进行妥善保管，或者记住以后进行销毁，不可被他人所获悉。如果证书持有者使用口令或 PIN 码保护私钥匙，证书持有者应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书持有者使用生物特征保护私钥，证书持有者也应注意防止其生物特征被人非法窃取。同时为了配合业务系统的安全需要，应该经常对激活数据进行修改。

3. 激活数据的其他方面

当私钥的激活数据进行传送时，应保护他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者全部，比如记录有口令的在纸页必须粉碎。

考虑到安全因素，对于申请证书的证书持有者激活数据的生命周期，规定如下：

1、证书持有者用于申请证书的口令，申请成功后失效。

2、用于保护私钥或者 IC 卡、USB Key 的口令，建议证书持有者根据业务应用的需要随时予以变更，使用期限超过 3 个月后应要进行修改。

6.5.2.5 计算机安全控制

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》、《电子政务电子认证服务管理办法》，参照 ISO27001 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。

实行严格的双因素验证机制，为每位拥有系统（包括 CA 系统、RA 系统）访问权限的人员分配唯一的账户，账户的访问权限限制为执行工作职责要求的最小权限。访问时同时采用数字证书及用户名和口令两种登录方式。

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。

2. 计算机安全评估

GDCA 的认证系统，通过了国家密码管理局的安全性审查。

GDCA 的认证系统、计算机及网络安全，每年由国家密码管理局主管部门

对认证系统、计算机、网络安全进行年度评估审查，如有必要，根据相关专家及领导意见，对认证系统及系统安全进行升级改造。

6.5.2.6 生命周期技术控制

1. CA 系统运行管理

GDCA 每天由专人负责巡检机房设备的工作情况，定期由技术人员检查软件系统的运行情况。部署了漏洞扫描系统、入侵检测系统和防火墙等，以确保网络环境的安全稳定。

CA 系统的访问管理

设置关键岗位和职责分工，对于 CA 系统的访问权限进行严格限制，未授权人员不得访问 CA 系统。

2. CA 系统的开发和维护

原则上不对 CA 系统进行技术开发和直接调用其数据，仅将 LDAP 和 RA 系统对外提供查询和访问服务。

6.5.2.7 网络的安全控制

GDCA 证书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。

证书认证系统只开放与申请证书、查询证书等相关的操作功能，供用户通过网络进行。只有 GDCA 授权的员工能够进入 GDCA 证书服务器、GDCA 证书目录服务器、GDCA 操作中心等设备或系统。

为了确保网络安全，GDCA 证书认证系统安装部署了入侵检测、安全审计、防毒防范和网管系统，并且及时更新防火墙、入侵监测、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。

6.5.2.8 时间戳

GDCA 的业务系统的系统时间均通过 NTP 协议与该时间戳服务同步。

7 电子政务电子认证服务操作规范

7.1 数字证书服务操作规范

7.1.1 数字证书格式

GDCA 提供的数字证书完全符合《GM/T 0015 基于 SM2 密码算法的数字证书格式规范》的要求。

7.1.2 身份标识与鉴别

1. 命名

数字证书命名符合《GM/T 0015 基于 SM2 密码算法的数字证书格式规范》的要求，不使用匿名和假名。

2. 初始身份确认

1) 证明持有私钥的方法

GDCA 通过以下方式证明证书持有者对私钥的持有：

（1)通过证书请求中所包含的数字签名来证明证书持有者持有与注册公钥对应私钥。

a) 证书申请者在客户端生成公私钥对；

b) 证书申请者使用私钥对证书请求信息签名，并连同公钥一同提交 CA 系统；

c) CA 使用证书申请者公钥验证签名。

（2）证书持有者必须妥善保管自己的私钥，即只有证书持有者可以持有私钥。

如以上条件满足，则证书持有者可以被视作其私钥的唯一持有者。

2) 组织机构身份的鉴别

机构申请数字证书时，应按照 GDCA 的要求提交相应的申请材料，包括：申请表、企业法人营业执照等机构证明文件、经办人的有效身份证件、加盖公章的授权申请文件等。

GDCA 有权利对组织机构提交的证明材料进行验证和审核，如审核通过，GDCA 将所有证明文件连同申请表一并归档保存。

3) 个人身份的鉴别

申请个人证书应提交申请表、合法身份证明文件及其复印件，合法的身份证明文件包括身份证、户口簿、护照、军官证、警官证等。GDCA 有权利对个人提交的所有证明文件进行审核和查验，如审核通过，GDCA 将所有证明文件连同申请表一并归档保存。

在把证书签发给政府部门个人时，还应进行以下鉴证工作：

a) 申请人提交由所属政府部门签章的证明文件，明确部门的名称。

b) GDCA 对上述材料进行审核，做出批准申请或拒绝申请的操作。

c) 如批准申请，将保留该材料，与其他证明文件一并归档保存。

3. 密钥更新请求的识别与鉴别

1） 常规密钥更新请求的识别与鉴别

对于一般正常情况下的密钥更新申请，证书持有者应提交能够识别原证书的足够信息，并使用更新前的私钥对包含新公钥的申请信息签名。对申请的鉴别满足以下条件：

a) 密钥更新请求中，应确保更新请求与申请者身份的关联和申请行为的有效性，采取现场受理和远程在线等方式对用户身份进行实体鉴别。

b) 当用户证书已过期时，重新进行与初始身份确认相同的实体鉴别流程。

c) 当用户证书未过期时，用户采取在线更新方式的，应由用户在线提交更新申请并进行数字签名，以实现对用户身份的实体鉴别。

2） 撤销之后的密钥更新请求的识别与鉴别

GDCA 不提供证书被撤销后的密钥更新。

4. 撤销请求的身份标识与鉴别

证书持有者本人申请撤销证书时的身份标识和鉴别采用与初始身份验证相同的流程。

如果是因为证书持有者没有履行 GDCA 的《电子政务电子认证证书策略和业务规则》所规定的义务，由 GDCA、注册机构申请撤销证书持有者的证书时，不需要对证书持有者身份进行标识和鉴别。

7.1.3 数字证书服务操作要求

7.1.3.1 证书申请

证书申请者提交证书申请时，应按照初始身份鉴别的要求，填写申请表，提交身份证明材料。GDCA 将根据证书申请者提交的资料进行以下操作：

1. 对接收到的申请材料进行检查；
2. 核查材料是否充分；
3. 验证证书申请信息的完整性；
4. 对申请材料保密；
5. 确认用户接受服务协议。

7.1.3.2 证书申请处理

GDCA 在接收到证书申请后应：

1. 按照初始身份鉴别的要求，对证书申请者的身份进行识别和鉴证；
2. 对证书申请者申请行为的合法性进行鉴证，确认申请行为得到合法授权；
3. 依据鉴证结果，做出接受或拒绝证书申请的决定。在 48 小时内，告知证书申请者结果及相应的原因。
4. 如接受申请，应妥善保管证书申请者申请时提交的所有资料。

7.1.3..3 证书签发

1. 证书签发中 RA 和 CA 的行为

同本 CP/CPS 6.1.4.3.1。

2. CA 和 RA 通知证书申请者证书的签发

同本 CP/CPS 6.1.4.3.2。

7.1.3.4 证书接受

1. 构成接受证书的行为

证书持有者接受证书的方式可以有如下几种：

A. 通过面对面的提交，证书持有者接受载有证书和私钥的介质。

B. 证书持有者通过网络将证书下载到本地存放介质。

完成以上行为表明证书持有者接受证书。在证书持有者接受到证书后，证书持有者应立即对证书进行检查和测试。

2. 电子认证服务机构对证书的发布

同本 CP/CPS 6.1.4.4.2。

3. 电子认证服务机构对其他实体的通告

同本 CP/CPS 6.1.4.4.3。

7.1.3.5 密钥对和证书使用

证书持有者的密钥对和证书须用于其规定的、批准的用途。签名密钥对用于签名与签名验证，加密密钥对用于加密解密。如果密钥对允许用于身份鉴别，则可以用于身份鉴别。密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用是不受保障的。

1. 证书持有者的私钥和证书使用

证书持有者只能在本 CP/CPS 规定的应用范围内使用私钥和证书，对于签名证书，其私钥可用于对信息的签名，证书持有者应知悉并确认签名的内容。对于加密证书，其私钥可用于对采用对应公钥加密的信息进行解密。在证书到期或被撤销之后，证书持有者必须停止使用该证书对应的私钥。

2. 依赖方的公钥和证书使用

当依赖方接受到签名信息后，应该：

A. 获得对应的证书及信任链；

B. 验证证书的有效性；

C. 确认该签名对应的证书是依赖方信任的证书；

D. 证书的用途适用于相应的签名；

E. 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。依赖方应将加密证书连同加密信息一起发送给接受方。

7.1.3.6 证书更新

证书更新指在不改变证书注册信息的情况下，为证书持有者签发一张新证书。

1. 更新申请的提交

证书持有者、证书持有者的授权代表或证书对应实体的拥有者在证书满足更新条件时，应按要求向 GDCA 提出更新申请。可采取当面提交更新申请表或在线提交带有证书持有者数字签名的更新申请。

2. 处理证书更新请求

GDCA 将根据提交的申请进行处理，包括申请验证、鉴别、签发证书。对申请的验证和鉴别基于以下几个方面：

A. 申请对应的原证书存在并且由 GDCA 签发。

B. 用原证书（有效期内的证书）上的证书持有者公钥对申请的签名进行验证。

C. 基于原注册信息，按照密钥更新时的要求，进行身份鉴别。

在以上验证和鉴别通过后才可以进行证书更新。

证书更新可以通过以下方式进行：

A. 面对面的更新方式；

B. 在线的自动更新方式。

3. 通知证书持有者新证书的签发

同本 CP/CPS 6.1.4.3.2。

4. 构成接受更新证书的行为

同本 CP/CPS 6.1.4.4.1。

5. CA 对更新证书的发布

同本 CP/CPS 6.1.4.4.2。

6. CA 通知其他实体证书的签发。

同本 CP/CPS 6.1.4.4.3。

7.1.3.7 证书补发

同本 CP/CPS 6.1.4.7。

7.1.3.8 证书变更

用户要求 GDCA 对已签发数字证书进行证书主题变更。证书变更业务的操作流程，按照证书申请的身份鉴别和受理流程执行。

7.1.3.9 证书撤销

1. 证书撤销的发起

GDCA 认可以下实体发起的证书撤销请求：

A. GDCA、注册机构、电子政务机构或其他部门在满足证书撤销条件的前提下，可以依法主动撤销证书持有者的证书。

B. 对于个人证书，证书持有者可以请求撤销他们自己的个人证书。

C. 对于机构证书，只有机构授权的代表有资格请求撤销已经签发给机构的证书。

D. 对于设备证书，只有拥有该设备的机构授权的代表有资格请求撤销已经签发给该设备的证书。

2. 证书撤销的处理

A. GDCA 在接到证书持有者的撤销请求后，通过核实身份证明材料、验证预留信息等方式，确认请求确实来自证书持有者。

B. 对于验证通过的请求，在 CA 系统中执行撤销证书操作，并在 24 小时内将撤销证书发布到证书撤销列表中。

C. GDCA 在确信出现证书撤销条件的情况而需要立即撤销证书时，可以立即撤销证书。

D. 证书撤销后，通过电话、短信、网站等方式告知用户或依赖方证书撤销结果。

3. 依赖方检查证书撤销的要求

对于安全保障要求比较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：

A. 应根据证书标明的发布地址获取证书撤销列表。

B. 应验证撤销列表的签名，确认其来自于该证书对应的签发机构。

C. 应验证证书撤销信息，确认证书是否被注销。

4. CRL 发布频率

GDCA 的 CRL 发布周期为 8 小时，即在 8 小时内发布最新 CRL。但在特殊紧急情况下可以使 CRL 立即生效（假使网络传输条件能够保证），CRL 的立即生效由 GDCA 制定的发布策略决定。

CRL 的结构如下：

A. 版本号(version)

B. 签名算法标识符(signature)

C. 颁发者名称(issure)

D. 本次更新(this update)

E. 下次更新(next update)

F. 用户证书序列号/撤销日期(user certificate/revocation date)

G. CRL 条目扩展项(crl entry extensions)

H. CRL 扩展域(crl extensions)

I. 签名算法(signature algorithm)

J. 签名(signature value)

5. CRL 发布的最大滞后时间

GDCA 的 CRL 最大滞后时间不超过 24 小时。

6. CRL 备份及频率

GDCA 对 CRL 进行备份，最长时间间隔不超过 24 小时，备份保存时间不少于证书失效后 10 年。

7.在线状态查询的可用性

GDCA 提供在线查询服务（OCSP），并公布服务地址、服务接口等信息。

8. 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：

A. 应按照查询协议要求，向证书中表明的 OCSP 服务地址提交状态查询请求。

B. 查询过程应确保信息传输的机密性和完整性。

C. 应获得证书状态信息。

8. 撤销信息发布的其他形式

除了 CRL、OCSP 外，GDCA 不提供其他方式的撤销信息发布方式。

7.1.3.10 密钥生成、备份和恢复

证书持有者的签名密钥对由证书持有者的密码设备（如智能 USB KEY）或在符合《GM/T 0034 基于 SM2 密码算法的证书认证系统密码及其相关安全技

术规范》和《GM/T 0028 密码模块安全技术要求》的密码模块中生成和保管，加密密钥对由国家密码管理局和省密码管理局审查通过的密钥管理基础设施提供密钥管理服务。

密钥恢复是指加密密钥的恢复，密钥管理基础设施不负责签名密钥的恢复。密钥恢复分为两类：证书持有者密钥恢复和问责取证密钥恢复。

1. 证书持有者密钥恢复：当证书持有者的密钥损坏或丢失后，某些密文数据将无法还原，此时证书持有者可申请密钥恢复。证书持有者向 GDCA 提交申请，经审核后，通过 GDCA 向密钥管理基础设施发送请求，密钥恢复模块接受证书持有者的恢复请求，恢复证书持有者的密钥并下载到证书载体中。

2. 问责取证密钥恢复：问责取证人员向密钥管理基础设施提交申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

7.2 应用集成支持服务操作规范

7.2.1 服务策略和流程

1. 针对不同政府行业的业务背景，GDCA 根据行业提供区分性的证书模板和接口文档，具体到每个项目再对业务系统进行充分调研，指导或参与业务系统证书应用部分的开发和实施；

2. 制定项目管理制度，规范系统和程序开发行为；

3. 制定安全控制流程，明确人员职责；

4. 实施证书软件发布版本管理，并进行证书应用环境控制；

5. 项目开发程序和文档等资料妥善归档保存。

7.2.2 应用接口

GDCA 的证书应用接口为上层提供简洁、易用的调用接口，主要包括密码设备接口和通用密码服务接口。证书应用接口符合《GM/T 0020 证书应用综合服务接口规范》。

1. 密码设备调用接口

密码设备调用接口应包括服务器端密码设备的底层应用接口和客户端证书介质（如：USB KEY）的底层应用接口。

服务器端密码设备的底层应用接口符合《GM/T 0018 密码设备应用接口规范》；客户端证书介质的底层应用接口符合《GM/T 0016 智能密码钥匙密码应用接口规范》及《GM/T 0017 智能密码钥匙密码应用接口数据格式规范》。

2. 密码模块安全技术接口

采用新模式与新技术密码模块安全技术接口，符合《GM/T 0028 密码模块安全技术要求》及《GM/T 0054 信息系统密码应用基本要求》

3. 通用密码服务接口

通用密码服务接口是屏蔽了底层不同密码设备类型和底层接口的通用中间件，该接口符合《GM/T 0019 通用密码服务接口规范》，主要包括服务器端组件接口和客户端控件接口。

7.2.3 集成内容

GDCA 为电子政务应用单位提供证书应用接口程序集成工作。集成工作提供以下服务：

1. 证书应用接口的开发包；
2. 接口说明文档；
3. 集成演示 Demo；
4. 集成手册；
5. 证书应用接口开发培训和集成技术支持；
6. 协助应用系统开发商完成联调测试工作。

7.3 信息服务规范

7.3.1 服务内容

1. 证书信息服务

CA 系统中签发、更新和补办等数字证书，可实时或定时与电子政务信息系统进行数据同步，实现将证书信息同步到电子政务信息系统中。GDCA 提交的数据包括业务类型、GDCA 身份标识、用户基本信息、用户证书信息等。

2. CRL 信息服务

CRL 在 CA 系统中发布后，可实现将 CRL 实时发布到指定的电子政务信

息系统中。GDCA 提交的数据包括业务类型、GDCA 身份标识、CRL 文件、同步时间等。

3. 服务支持信息服务

GDCA 面向电子政务用户、应用系统集成商、应用系统发布与之相关的服务信息，包括 CP/CPS、FAQ、证书应用接口软件包等。

4. 决策支持信息服务

GDCA 面向电子政务用户、政府监管机构提供决策支持信息，包括用户档案信息、投诉处理信息、客户满意度信息、服务效率信息等。

7.3.2 服务管理规则

1. 对 CA 机构内的工作人员按其工作角色设定与之相应的信息访问权限，并对其所有访问操作进行详细记录。

2. 对证书应用单位的管理员设定信息访问权限，限定其仅能访问本应用所签发证书信息。

3. 应用单位管理员对非授权信息的访问，须依照政策管理规定，须经上级主管部门批准后方可进行。

4. 对问责程序需要进行的信息访问，应严格审核相应的问责人员身份及授权文件，无误后方可进行问责举证。

5. 对监管部门应管理需求进行的信息访问，应按照相关的管理规定和调取程序，为其提供信息访问权限。

7.3.3 服务方式

1. 证书信息同步服务

证书信息同步通过采用接口技术实现 CA 系统与电子政务信息系统的证书应用同步。电子政务信息系统通过部署统一的接口，GDCA 的 CA 系统通过调用统一的同步接口，实现 CA 系统向电子政务信息系统进行证书信息的自动同步功能。同时，为了保证数据传输的安全性，可通过对通信数据添加数字签名，以防止数据在传输中被篡改或数据损坏。

2. CRL 信息同步服务

CRL 信息同步服务通过采用技术实现 CA 系统与电子政务信息系统的 CRL

同步。CA 系统主动调用该接口，实时将最新的 CRL 文件同步到电子政务信息系统中。为了提高 CRL 文件传输的安全性，应对发送 CRL 数据进行数字签名，电子政务信息系统只需要根据 YNCA 身份标识找到对应的根证书链，验证 CRL 签名的有效性即可确定 CRL 的有效性。

3. 服务支持信息服务

GDCA 通过 WEB 网站面向电子政务用户发布如下信息：

A. 电子政务电子认证服务业务规则

B. 证书生命周期服务流程及相关费用

C. 证书用户操作手册

D. 证书常见问题解答（FAQ）

E. 获得证书帮助联系方式（客服电话、办公地址、邮政编码、投诉电话等）

GDCA 通过 WEB 网站面向电子政务应用系统集成商发布如下信息：

A. 数字证书应用接口软件包

B. 数字证书应用接口实施指南

C. 证书常见问题解答（FAQ）

D. 获得证书帮助联系方式（客服电话、办公地址、邮政编码、投诉电话等）

GDCA 通过 WEB 网站面向电子政务应用系统发布如下信息：

A. 时间戳服务数据接口

B. http 协议的 CRL 发布服务接口

C. LDAP 协议的 CRL 发布接口

D. LDAP 协议的证书发布接口

E. OCSP 服务接口

4. 决策支持信息服务

GDCA 面向应用提供以接口等方式提供如下信息服务：

A. 用户档案信息：分业务、地域、时段等要素提供用户信息的统计分析服务；

B. 投诉处理信息：提供特定业务、时间、特定用户群、问题类型等的投诉处理汇总信息及分析；

C. 客户满意度信息：提供面向业务的客户满意度调查信息；

D. 服务效率信息：提供面向业务的服务效率分析信息，如处理时间、服务接通率等。

7.4 使用支持服务操作规范

7.4.1 服务内容

1. 面向证书持有者的服务支持

A. 数字证书管理

包括数字证书的导入、导出，以及客户端证书管理工具的安装、使用、卸载等。

B. 数字证书应用

基于数字证书的身份认证、电子签名、加解密等应用过程中出现的各种异常问题，如：证书无法读取、签名失败、验签失败等。

C. 证书存储介质硬件设备使用

包括证书存储介质使用过程中出现的 PIN 码锁死、驱动安装、介质异常等。

D. 电子认证服务支撑平台使用

为用户提供数字证书在线服务平台中使用的各类问题，如：证书更新失败、下载异常、无法提交注销申请等。

2. 面向应用提供方的服务支持

A. 电子认证软件系统使用

提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等的使用支持问题，如证书信息无法查询、数据同步失败、服务无响应等。

B. 电子签名服务中间件的应用

解决服务中间件在集成时出现的各种情况，如客户端平台适应性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

7.4.2 服务方式

同本 CP/CPS 6.4.2。

7.4.3 服务质量

同本 CP/CPS 6.4.3。

7.5 安全保障规范

7.5.1 认证机构设施、管理和操作控制

7.5.1.1 物理控制

7.5.1.1.1 场地位置与建筑

GDCA 的建筑物和机房建设按照下列标准实施：

GB/T 25056 《信息安全技术 证书认证系统密码及其相关安全技术规范》

国密局[2010]7 月《电子政务电子认证基础设施建设要求》

GB6650：《计算机机房用活动地板技术条件》

GB50174《电子信息系统机房设计规范》

GB2887《计算机场地通用规范》

GB30003《电子计算机机房施工及验收规范》

GB50222《建筑内部装修设计防火规范》

GB50116《火灾自动报警系统设计规范》

GB50057《建筑物防雷设计规范》

GB5054《低压配电设计规范》

GB/J19《采暖通风与空气调节设计规范》

SJ/T10796《计算机机房用活动地板技术条件》

GDCA 机房位于佛山市南海区狮山镇，是一幢独立的建筑物，具备防震、防火、防水、防雷等功能，进入机房建筑区只有唯一的入口和道路，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。只有经过授权的人员才能进入授权的区域。

1. 公共区域

公共区包括入口、大堂、保安室，部署各配套设施和监控设备，进入公共区域都必须登记。

2. 操作区

操作区是 RA 操作人员、管理人员的工作区，需要同时使用身份识别卡和指纹鉴别才可以进入，人员进出操作区要有日志记录。从该层开始，所有的墙体都应采用高强度防护墙。

3. 管理区

管理区安装 RA 管理控制台，CA 管理、签发、审计控制台，网络管理、监控控制台，是 RA 和 CA 管理员、审计员和网络安全员的工作区，只允许管理区规定的管理人员进入，需要两个管理员同时使用身份识别卡和指纹鉴别才可以进入。

4. 服务区

服务区主要安装从 LDAP 服务器、OCSP 服务器、RA 注册服务器等设备；只允许服务区规定的管理人员进入，需要两个管理员同时使用身份识别卡和指纹鉴别才可以进入。

5. 核心区

核心区为屏蔽区，加装高强度的钢制防盗门，主要安装 CA 签名服务器、CA 数据库服务器、KM 密钥管理服务器、时间戳服务器等核心设备，只允许核心区规定的管理人员进入，而且需要两个管理员同时使用身份识别卡和指纹鉴别才可以进入。密码柜也安放在核心区，存放保密资料。

7.5.1.1.2 物理访问

GDCA 机房内设有 9 扇门安装电子门禁系统和 1 个物理侵入报警器，对门禁系统进行监控，实时读取门禁记录的资料，并对门禁系统设置权限。该系统能实时读取进出门资料，并有门开超时报警。工作人员都需使用身份识别卡或结合指纹才能进出，并且进出每一道门都有时间记录和相关信息提示，服务区与核心区需要两个管理员同时使用身份识别卡和指纹鉴别才可以进入，机房工作人员按照机房日常工作规范，每月对门禁记录进行整理归档，保留一年的门禁记录。

物理访问控制包括如下几个方面：

a) 门禁系统：控制各层门的进出。工作人员需使用身份识别卡或结合口令或指纹鉴定才能进出，进出每一道门应有时间纪录和信息提示。

b) 报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况都应触发报警系统。报警系统明确指出报警位置。

c) 监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对安全区域和操作区域进行 7*24 小时不间断录像。所有录像资料至少保留 6

个月，以备查询。

7.5.1.1.3 安防监控

根据机房动力环境保安监控系统的要求，本机房环境监控系统包括的子系统有：配电检测子系统、UPS 检测子系统、空调设备检测子系统、新风机检测子系统、温湿度检测子系统、漏水监测子系统、消防子系统、门禁子系统、图像监控子系统。对基础设施设备、机房环境状况、安防系统状况进行 7*24 小时实时监测，为满足故障诊断、事后审计的需要，监控记录保留时间为 6 个月以上。

7.5.1.1.4 电力与空调

本机房采用两路市电电源供电、一台柴油发电机，配置有专门的配电机房，每个机房配置有独立的配电设备、接地防雷系统。机房内采用了不间断供电系统 UPS，可提供大于 8 小时的电力。机房区域内采用了防静电措施，实现机柜、服务器、网络设备等电位连接和接地。

机房的空调采用风冷式冷凝器机组，室外风冷式冷凝器机组放置在顶楼。机房按照 300kcal/h ṁ2 热负荷计算。夏季室外设计温度：35℃；冬季室外设计温度：0℃；机房室内设计温度：22±1℃，相对湿度：55±5%/h 。同时，机房安置了新风系统，对机房进行换气，保证机房内的空气品质和解决新风供应以及机房对空气清洁度的要求等问题。

7.5.1.1.5 水患防治

为防治水害对机房的威胁，GDCA 在机房的空调室内设置漏水报警系统。漏水报警检测绳在空调周围设置，一旦发生水患立即报警，通知有关人员采取应急措施。同时在沿外墙四周做排水沟及泄水地漏，一旦发生水患，水能立即排泄出去，并对所有外窗已做封闭处理。

7.5.1.1.6 火灾防护

GDCA 机房内各区域均采用了烟感和温感火灾探测器，并安装了火灾自动报警系统及气体自动灭火系统， 该系统具有自动、手动及机械应急操作三种启动方式。

在自动状态下，当防护区发生火警时，火灾报警控制器接到防护区两独立火灾报警信号后立即发出联动信号。经过 30 秒时间延时，火灾报警控制输出信

号，启动灭火系统，同时，报警控制器接收压力讯号器反馈信号，防护区内门灯显亮，避免人员误入。

当防护区经常有人工作时，可以通过防护区门外的手动/自动转换开关，使系统自动状态转换到手状态，当防护区发生火警时，报警控制器只发出报警信号，不输出动作信号。由值班人员确认火警，按下控制面板或击碎防护区外紧急启动按钮，即可立即启动系统，喷发气体灭火剂。

当自动、手动紧急启动都失灵时，可进入储瓶间内实现机械应急操作启动。

7.5.1.1.7 介质存储

GDCA 对物理介质的存放和使用满足防火、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。采取了介质使用登记注册、介质防复制及信息加密等措施实现了对介质的安全保护。

7.5.1.1.8 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。

7.5.1.1.9 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。

7.5.1.1.10 入侵侦测报警系统

机房场所建筑区域内安装入侵侦测报警系统，进行安全布防。安全区域窗户上安装玻璃破碎报警器，建筑内天花板上安装活动侦测器，发生非法入侵应立即报警。

7.5.1.2 操作过程控制

同本 CP/CPS 6.5.1.2。

7.5.1.3 人员控制

同本 CP/CPS 6.5.1.3。

7.5.1.4 审计日志程序

同本 CP/CPS 6.5.1.4。

7.5.1.5 记录归档

同本 CP/CPS 6.5.1.5。

7.5.1.6 电子认证服务机构密钥的更替

同本 CP/CPS 6.5.1.6。

7.5.1.7 数据备份

同本 CP/CPS 6.5.1.7。

7.5.1.8 损害和灾难恢复

同本 CP/CPS 6.5.1.8。

7.5.1.9 认证机构或注册机构终止

GDCA 终止事件的原因可以分为密钥受损原因和非密钥受损原因，密钥受损原因可能包括 GDCA 根密钥丢失，非密钥受损原因可能与商业因素有关。

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 停止相关的实体；
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。

由于密钥受损和非密钥受损原因而终止 GDCA，几乎要完成相同的操作，唯一的不同在 GDCA 终止发送通知的时间限制上，由于密钥受损原因终止 GDCA，要求 GDCA 通知证书持有者的过程尽快完成；由于非密钥受损原因终止贵 CA，在 GDCA 通知所有证书持有者后，采取适当的步骤减轻 GDCA 终止对证书持有者影响。

GDCA 在暂停或终止认证服务六十个工作日前，就业务承接及其他有关事项通知有关各方，包括但不限于 GDCA 授权的发证机构和证书持有者等，并在暂停或终止认证服务四十五个工作日前向国家密码管理局报告。

7.5.2 认证系统技术安全控制

7.5.2.1 密钥对的生成与安装

7.5.2.1.1 密钥对的生成

1. 签名密钥对生成

GDCA 证书申请者必须使用国家密码管理局批准许可的设备生成签名密钥对，例如由密码机、密码卡、USB Key、IC 卡等生成。证书申请者在选择这些设备前，应事先向 GDCA 咨询有关系统兼容和接受事宜。GDCA 向证书申请者提供符合国家密码管理相关规定的设备作为证书申请者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。

证书申请者签名密钥对的产生，必须遵循国家的法律政策规定。GDCA 支持多种模式的签名密钥对产生方式，证书申请者可根据其需要进行选择密钥生成模块。但是不管何种方式，密钥对产生的安全性都应该得到保证。GDCA 在技术、业务流程和管理上，已经实施了安全保密的措施。

证书持有者负有保护私钥安全的责任和义务，并承担由此带来的法律责任。

2. 加密密钥对生成

GDCA 证书申请者的加密密钥对由 GDCA 代证书申请者向密钥管理中心

申请生成，并由密钥管理中心进行管理。

7.5.2.1.2 加密私钥传送给证书申请者

由证书签发机构代替证书申请者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证书申请者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证书申请者证书载体时，证书申请者使用自己的证书载体解密该私钥并存储。

7.5.2.1.3 公钥传送给证书签发机构

证书申请者的签名证书公钥通过安全通道，经注册机构传递到 GDCA。

证书申请者的加密证书公钥，由密钥管理中心通过安全通道传递到 GDCA 中心。

从注册机构（RA）到 GDCA 以及从密钥管理中心到 GDCA 的传递过程中，采用国家密码管理局许可的通讯协议及密钥算法，保证了传输中数据的安全。

7.5.2.1.4 电子认证服务机构公钥传送给依赖方

依赖方可以从 GDCA 的网站下载根证书和 CA 证书，从而得到 CA 的公钥。

7.5.2.1.5 密钥的长度

SM2 CA 证书和证书申请者证书的密钥长度均为 256bit。RSA CA 证书的密钥长度为 2048bit，可签发密钥长度为 RSA1024bit 和 RSA2048bit 的证书申请者证书。

如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，GDCA 将会完全遵从。

7.5.2.1.6 公钥参数的生成和质量检查

公钥参数必须使用国家密码管理局批准许可的加密设备和硬件介质生成。

对于参数质量的检查，同样由通过国家密码管理局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。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。

7.5.2.1.7 密钥使用目的

GDCA 的根 CA 密钥仅用于签署以下证书：

1. 代表根 CA 的自签证书；

2. 中级 CA 的证书及交叉证书；

3. 用于基础设施的证书（如 OCSP 响应验证证书）

证书持有者的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥对可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

7.5.2.2 私钥保护和密码模块工程控制

7.5.2.2.1 密码模块的标准和控制

GDCA 所用的密码设备都是经国家密码管理局认可的产品。密钥的生成、管理、存储、备份和恢复的密码模块须通过国家密码主管部门鉴定、认证。

7.5.2.2.2 私钥多人控制（m 选 n）

GDCA 私钥的生成、更新、撤销、备份和恢复等操作采用多人控制机制，即采取五选三方式，将私钥的管理权限分散到 5 位密钥管理员中，至少在其中三人在场并许可的情况下，插入管理员卡并输入 PIN 码，才能对私钥进行操作。

7.5.2.2.3 私钥托管

证书持有者加密证书对应的私钥由密钥管理中心托管，证书持有者的签名证书对应的私钥由自己保管，密钥管理中心不负责托管。

密钥管理中心严格保证用户密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。

7.5.2.2.4 私钥备份

私钥备份分为三种类型的备份：初始化备份（当第一次安装系统后就需进行备份）、完全备份（定期对系统中私钥库制作拷贝）、增量备份（在系统进行大的改动后，应进行特别备份）。

初始化备份是系统初始化生成时进行的私钥备份。

完全备份是指私钥库的备份采用专门的备份软件进行完整备份，每周一次。增量备份是指私钥库的备份采用专门的备份软件进行增量备份，每天一次。

7.5.2.2.5 私钥归档

密钥管理中心对所生成的密钥信息进行归档保存，保存的方式为将密钥对分成三份分别用对称加密算法进行加密并保存在密钥管理中心的数据库中和磁盘阵列中。

7.5.2.2.6 私钥导出、导入密码模块

私钥信息是及其重要的信息，私钥信息的导出必须要导出到证书载体的密文存储区中。私钥信息的导出必须要将私钥信息进行三分，并对每部分的私钥信息进行对称加密才能存储到证书载体的存储区中，导入时必须三个证书载体同时导入，解密合并后才能导入。

GDCA 不提供证书持有者私钥从硬件密码模块中导出的方法，也不允许如此操作。对于存放在软件密码模块中的私钥，如果证书持有者愿意并且自行承担相关风险，证书持有者可自主选择导入导出的方式，操作时需要采用口令保护等授权访问控制措施。

7.5.2.2.7 私钥在密码模块的存储

密钥管理中心的密码设备采用国家密码管理局批准和许可的服务器密码机，私钥的数据存储在服务器密码机硬件中，在整个生命周期都不会明文出现在硬件密码机之外。

证书持有者的私钥存储在符合国家密码管理规定的设备中，所有在设备中存储的私钥，都以密文的形式保存。对于使用软件密码模块生成的私钥，最好在硬件密码模块中存储和使用，证书持有者也可以自主选择使用有安全保护措施的特定软件密码模块。

7.5.2.2.8 激活私钥的方法

密钥管理员使用自己的管理员卡登录服务器密码机，进行激活私钥的操作，需要三名管理员同时在场。

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证书持有者私钥，证书持有者可以通过口令、IC 卡等方式进一步保护。当证书持有者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。对于存放在证书持有者计算机软件密码模块中的私钥，证书持有者应该采用合理的措施从物理上保护计算机，以防止在没有得到用户授权的情况下，其他人员使用证书持有者的计算机和相关私钥。如果存放在软件密码模块中的私钥没有口令保护，那么软件密码模块的加载意味着私钥的激活。如果使用口令保护私钥，软件密码模块加载后，还需要输入口令才能激活私钥。

7.5.2.2.9 解除私钥激活状态的方法

密钥管理员使用含有自己的管理员卡登录服务器密码机，进行解除私钥的操作，需要三名管理员同时在场。

一旦私钥被激活，除非这种状态被解除，私钥总是处于活动状态。在某些私钥的使用当中，私钥每次被激活，只能进行一次操作，如果需要进行第二次操作，需要再次进行激活。

GDCA 解除私钥激活状态的方式包括退出登陆状态、切断电源、将硬件密码模块移开、注销用户或系统等。未经授权的任何人员，绝不可以进行相关操作。

证书持有者解除私钥激活状态由其自行决定，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，切断电源时，私钥就被解除。

7.5.2.2.10 销毁私钥的方法

如果私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，如果其处于软件加密模块内，那么该软件加密模块必须被覆盖方式清除；如果位于硬件加密模块内，那么加密设备或者 IC 卡等必须被清空为零。同时，所有用于激活私钥的 PIN 码、IC 卡等也必须被销毁或者收回。

证书持有者的私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，由证书持有者决定其销毁方法，证书持有者必须保证有效销毁其私钥，并承担有关的责任。涉及到密钥到期后保存和归档的，证书持有者必须按照本 CP/CPS 的规定执行。

7.5.2.2.11 密码模块的评估

GDCA 使用国家密码管理局批准和许可的密码产品。

7.5.2.3 密钥对管理的其他方面

同本 CP/CPS 6.5.2.3。

7.5.2.3.4 激活数据

同本 CP/CPS 6.5.2.4。

7.5.2.3.5 计算机安全控制

同本 CP/CPS 6.5.2.5。

7.5.2.3.6 生命周期技术控制

同本 CP/CPS 6.5.2.6。

7.5.2.3.7 网络安全控制

同本 CP/CPS 6.5.2.7。

7.5.2.3.8 时间戳

同本 CP/CPS 6.5.2.8。

8 法律责任相关要求

8.1 要求

GDCA 在开展电子政务电子认证服务时，按照《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》等法律法规的要求，对涉及保密、隐私、知识产权、担保以及服务运营等各方面承担相关的责任和义务。

8.2 内容

8.2.1 费用

GDCA 可根据提供的电子认证相关服务向本机构的证书申请者收取费用，具体取决于市场规则和相关管理部门的规定。GDCA 有权根据市场状况，针对不同用户群体推出不同的收费策略或优惠措施。

如果 GDCA 签署的协议中指明的价格和 GDCA 公布的价格不一致，以协议中的价格为准。

8.2.2 财务责任

8.2.2.1 保险范围

出现下列情形并经 GDCA 确认后，证书持有者、依赖方等实体可以申请 GDCA 承担赔偿责任（法定或约定免责除外）。

- GDCA 将证书错误地签发给证书申请者以外的第三方，导致证书申请者或者依赖方遭受损失的；
- 证书申请者提供了虚假的注册信息或者资料，GDCA 发现后仍然签发了证书，导致依赖方遭受损失的；
- GDCA 未按鉴证要求对证书申请者证书申请信息进行审核而签发了电子证书，导致证书申请者或依赖方遭受损失的；
- 由于 GDCA 的原因导致证书私钥被破译、窃取，致使证书持有者或者依赖方遭受损失的；

- GDCA 未能及时撤销证书的。
- GDCA 对任何证书持有者、依赖方等实体有关证书赔偿的合计责任限制在不超出下述数量的范围内：

证书类型	赔偿金额上限
个人证书	800 元 RMB
机构（企业）证书	4000 元 RMB
设备证书	8000 元 RMB

8.2.2.2 对最终实体的保险或担保

GDCA 如违反了本 CP/CPS 中规定的职责，证书持有者、依赖方等实体可以申请 GDCA 承担赔偿责任（法定或约定免责除外）。在经 GDCA 确认后，可以对该实体进行赔偿。赔偿限制如下：

1) GDCA 所有的赔偿义务不得超出本节 8.2.2.1 中规定的保险范围，赔偿金额不得高于赔偿金额上限，赔偿金额上限可以由 GDCA 根据情况重新制定，GDCA 会将重新制定后的情况立刻通知相关当事人。
2) GDCA 只有在证书有效期限内承担损失赔偿责任。

8.2.2.3 责任免除

有下列情形之一的，应当免除 GDCA 之责任：

1. 证书申请者在申请和使用 GDCA 电子证书时，有违反如下义务之一的：

1) 证书申请者有义务提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息；
2) 证书持有者应当妥善保管 GDCA 所签发的电子证书载体和保护 PIN 码，不得泄漏 PIN 码或将电子证书载体随意交付他人；
3) 证书持有者在应用自己的密钥或使用电子证书时，应当使用可依赖、安全的系统；
4) 证书持有者知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知 GDCA 及相关各方，并终止使用该电子签名制作数据；
5) 证书持有者在使用电子证书时必须遵守国家的法律、法规和行政规章

制度。不得将电子证书作为 GDCA 规定使用范围外的其他任何用途使用；

6) 证书持有者必须在证书有效安全期内使用该证书；不得使用已失密或可能失密、已过有效期、被冻结、被撤销的电子证书；

7) 证书持有者有义务根据规定按时向 GDCA 及当地业务受理点交纳服务费用。

2. 由于不可抗力原因而导致电子证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“不可抗力”，是指不能预见、不能避免并不能克服的客观情况，包括但不限于：

1) 自然现象或者自然灾害，包括地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；

2) 社会现象、社会异常事件或者政府行为，包括政府颁发新的政策、法律和行政法规，或战争、罢工、骚乱等社会异常事件。

3. 因 GDCA 的设备或网络故障等技术故障而导致电子证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“技术故障”引起原因包括但不限于：

◆ 不可抗力；

◆ 关联单位如电力、电信、通讯部门而致；

◆ 黑客攻击；

◆ GDCA 的设备或网络故障。

4. GDCA 已谨慎地遵循了国家法律、法规规定的电子证书认证业务规则，而仍有损失产生的。

8.2.3 业务信息保密

8.2.3.1 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：

◆ GDCA 证书持有者的数字签名及解密密钥。

◆ 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。

- 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。

8.2.3.2 不属于保密的信息

GDCA 将以下信息视为不保密信息：

- 由 GDCA 发行的证书和 CRL 中的信息。
- 由 GDCA 支持、CP/CPS 识别的证书策略中的信息。
- GDCA 许可，只有 GDCA 证书持有者方使用，在 GDCA 网站公开发布的信息。
- 其他：GDCA 信息的保密性取决于特殊的数据项和申请。

8.2.3.3 保护保密信息的责任

GDCA 有妥善保管与保护本节 8.2.3.1 中规定的保密信息的责任与义务。

8.2.4 个人隐私保密

8.2.4.1 隐私保密方案

GDCA 尊重证书申请者个人资料的隐私权，保证完全遵照国家对个人资料隐私保护的相关规定及法律。同时，GDCA 将确保全体职员严格遵从安全和保密标准对个人隐私给予保密。有关个人隐私保护相关的政策可以在 GDCA 官网（https://www.gdca.com.cn/）进行查询。

8.2.4.2 作为隐私处理的信息

GDCA 定义以下信息为证书申请者的隐私信息：

- 证书申请者的有效证件号码如身份证号码、单位机构代码。
- 证书申请者的联系电话。
- 证书申请者的通信地址和住址。
- 证书申请者的银行帐号。

8.2.4.3 不被视为隐私的信息

GDCA 定义包括但不限于以下信息不被视为证书持有者的隐私信息：

- 证书申请者姓名、单位名称等。
- 证书申请者性别、单位性质等。
- 证书申请者通信地址的邮政编码。
- 证书申请者的电子邮箱。

8.2.4.4 保护隐私的责任

GDCA 有妥善保管与保护本节 8.2.4.2 中规定的证书申请者个人隐私的责任与义务。

8.2.4.5 使用隐私信息的告知与同意

GDCA 将采取适当的步骤保护证书申请者的个人隐私，并将采取可靠的安全手段保护已存储的个人隐私信息。除非根据法律或政府的强制性规定，在未得到证书申请者的许可之前，GDCA 保证不会把证书申请者的除写入电子证书的个人资料外的个人信息提供给无关的第三方（包括公司或个人）。

8.2.4.6 依法律或行政程序的信息披露

当行政机关需要 GDCA 提供相应的证书使用者的相关信息时，GDCA 需提供如下信息：

- 证书申请者的基本信息。
- 证书申请者用个人加密密钥加密的信息。
- 证书申请者对 GDCA 网站的登录情况。
- GDCA 将按照法律要求向执法人员提供相关信息。

8.2.4.7 其他信息披露情形

如果证书申请者要求 GDCA 提供某类特定客户支援服务如资料邮寄时，GDCA 则需要把证书申请者的姓名和邮寄地址等信息提供第三者如邮寄公司。

8.2.5 知识产权

- 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。
- GDCA 对电子证书系统软件具有所有权、名称权、利益分享权。
- GDCA 有权决定采用何种软件系统。
- 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。
- GDCA 发行的证书和 CRL 均为受 GDCA 支配的财产。
- 对外运营管理策略和规范为 GDCA 财产。
- 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。

8.2.6 陈述与担保

8.2.6.1 电子认证服务机构的陈述与担保

GDCA 在提供电子认证服务活动过程中的承诺如下：

- GDCA 签发给证书申请者的证书符合 GDCA 的 CP/CPS 的所有实质性要求。
- GDCA 将向证书申请者通报任何已知的，将在本质上影响证书申请者的证书的有效性和可靠性事件。
- GDCA 根据本 CP/CPS 的要求及时撤销证书。
- GDCA 拒绝签发证书后，将立即向证书申请者归还所付的全部费用。
- 根据本 CP/CPS 的要求验证申请人的身份。

证书公开发布后，GDCA 证书中的信息是经过验证的。

GDCA 不负责评估证书是否在适当的范围内使用，证书申请者和依赖方依照证书申请者协议和依赖方协议确保证书用于允许使用的目的。

8.2.6.2 注册机构的陈述与担保

GDCA 的注册机构在参与电子认证服务过程中的承诺如下：

- 提供给证书持有者的注册过程完全符合 GDCA 的 CP/CPS 的所有实质

性要求。

- 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。
- 注册机构将按 CP/CPS 的规定，及时向 GDCA 提交撤销、更新等服务申请。

8.2.6.3 证书申请者的陈述与担保

证书申请者一旦接受 GDCA 签发的证书，就被视为向 GDCA、注册机构及信赖证书的有关当事人作出以下承诺：

- 已知悉和接受 GDCA 的“电子证书申请责任书”和本 CP/CPS 中的所有条款和条件。
- 在证书的有效期内进行数字签名。
- 证书申请者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，愿意承担任何提供虚假、伪造等信息的法律责任。
- 如果存在代理人，那么证书申请者和代理人两者负有连带责任。证书申请者有责任就代理人所作的任何不实陈述与遗漏，通知 GDCA 或其授权的证书服务机构。
- 与证书持有者证书所含公钥相对应的私钥所进行的每一次签名，都是证书持有者自己的签名，并且在进行签名时，证书是有效证书（证书没有过期、撤销），证书的私钥为证书持有者本身访问和使用。
- 除非经证书持有者和发证机构间书面协议明确规定，证书持有者保证不从事发证机构（或类似机构）所从事的业务。
- 一经接受证书，既表示证书申请者知悉和接受本 CP/CPS 中的所有条款和条件，并知悉和接受相应的证书申请者协议；
- 一经接受证书，证书申请者就应当承当如下责任：始终保持对其私钥的控制，使用可信的系统，采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用；
- 不得拒绝任何来自 GDCA 公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

- 证书在本 CP/CPS 中规定使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的。
- 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。

8.2.6.4 依赖方的陈述与担保

- 遵守本 CP/CPS 的所有规定。
- 确认证书在规定的范围和期限使用证书
- 在信赖证书前，对证书的信任链进行验证
- 在信赖证书前，通过查询 CRL 或 OCSP 确认证书是否被撤销
- 一旦由于疏忽或者其他原因违背了合理检查的条款，依赖方愿意就此而给 GDCA 带来的损失进行补偿，并且承担因此造成的自身或他人的损失。
- 不得拒绝任何来自 GDCA 公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

8.2.6.5 其他参与者的陈述与担保

GDCA 从事电子认证活动的其他参与者作出如下承诺：

遵守本 CP/CPS 的所有规定。

8.2.7 担保免责

除本 CP/CPS 8.2.6.1 中的明确承诺外，GDCA 不承担其他任何形式的保证和义务：

- 不保证证书持有者、信赖方、其他参与者的陈述内容。
- 不对电子认证活动中使用的任何软件做出保证。
- 不对证书在超出规定目的以外的应用承担任何责任
- 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
- 证书持有者违反本 CP/CPS 8.2.6.3 之承诺时，或依赖方违反本 CP/CPS 8.2.6.4 之承诺时，得以免除 GDCA 之责任。

8.2.8 有限责任

证书持有者、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 将承担不超过本 CP/CPS 8.2.9 规定的有限赔偿责任。

8.2.9 赔付责任

8.2.9.1 GDCA 的赔偿责任

如 GDCA 违反了本 CP/CPS 8.2.6.1 中的陈述，证书持有者、依赖方等实体可以申请 GDCA 承担赔偿责任(法定或约定免责除外)。如出现下述情形，GDCA 承担有限赔偿责任：

1. GDCA 将证书错误的签发给证书申请者以外的第三方，导致证书持有者或依赖方遭受损失的；
2. 在证书申请者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，导致证书申请者或依赖方遭受损失的；
3. 在 GDCA 明知证书申请者提交信息或资料存在虚假谎报的情况，但仍然向证书申请者签发证书，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，导致证书申请者或依赖方遭受损失的；
5. GDCA 未能及时撤销证书，导致依赖方遭受损失的。

另外，GDCA 赔偿限制如下：

1. GDCA 所有的赔偿义务不得高于本 CP/CPS 8.2.2.1，这种赔偿上限可以由 GDCA 根据情况重新制定，GDCA 会将重新制定后的情况立刻通知相关当事人。
2. 对于由证书持有者或依赖方的原因造成的损失，GDCA 不承担责任，由证书持有者或依赖方自行承担。
3. GDCA 只有在证书有效期限内承担损失赔偿责任。

8.2.9.2 证书持有者的赔偿责任

如因下述情形而导致 GDCA 或依赖方遭受损失，证书持有者应当承担赔偿

责任：

1. 证书持有者申请注册证书时，因故意、过失或者恶意提供不真实资料，导致造成 GDCA 及其授权的证书服务机构或者第三方遭受损害；
2. 证书持有者因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知 GDCA 及其授权的证书服务机构，以及不当交付他人使用造成 GDCA 及其授权的证书服务机构、第三方遭受损害；
3. 证书持有者使用证书的行为，有违反本 CP/CPS 及相关操作规范，或者将证书用于非本 CP/CPS 规定的业务范围；
4. 证书持有者或者其它有权提出撤销证书的实体提出撤销请求后，到 GDCA 将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果 GDCA 按照本 CP/CPS 的规范进行了有关操作，那么该证书的证书持有者必须承担所有损害赔偿责任；
5. 提供的资料或信息不真实、不完整或不准确；
6. 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；
7. 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；
8. 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；
9. 证书到期但仍在使用证书；
10. 证书持有者的证书信息侵犯了第三方的知识产权；
11. 在规定的范围外使用证书，如从事违法犯罪活动；

8.2.9.3 依赖方的赔偿责任

如因下述情形而导致 GDCA 或证书持有者遭受损失，依赖方应当承担赔偿责任：

1. 没有履行 GDCA 与依赖方的协议和本 CP/CPS 中规定的义务；
2. 未能依照本 CP/CPS 规范进行合理审核，导致 GDCA 及其授权的证书服务机构或第三方遭受损害；
3. 在不合理的情形下信赖证书，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，但仍然信赖证书；

4. 依赖方没有对证书的信任链进行验证；

5. 依赖方没有通过查询 CRL 或 OCSP 确认证书是否被撤销。

8.2.10 有效期限与终止

8.2.10.1 有效期限

本 CP/CPS 在发布日期零时正式生效，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 GDCA 终止电子认证服务时失效。

8.2.10.2 终止

在 GDCA 终止电子认证服务时，本 CP/CPS 终止。

8.2.10.3 效力的终止与保留

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，CP/CPS 中对各方责任的规定及责任免除仍然适用。

8.2.11 对参与者的个别通告与沟通

本 CP/CPS 终止后，GDCA 将就文档失效的有关事项通知参与本机构电子认证活动的各有关当事人。

8.2.12 修订

8.2.12.1 修订程序

经 GDCA 安全策略委员会授权，CPS 编写小组每年至少审查一次本 CP/CPS，确保其符合国家法律法规和主管部门的要求及相关国际标准，符合认证业务开展的实际需要

本 CP/CPS 的修改和更新，由 CPS 编写小组提出修订报告，经 GDCA 安全策略委员会批准后，由 CPS 编写小组负责组织修订，修订后的电子政务 CP/CPS 经过 GDCA 安全策略委员会批准后正式对外发布。

8.2.12.2 通知机制和期限

修订后的 CP/CPS，GDCA 将通过网站方式予以公布。

8.2.12.3 必须修改业务规则的情形

GDCA 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。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。

8.2.13 争议处理

GDCA、证书持有者、依赖方等实体在电子认证活动中产生争议可按以下步骤解决：

1. 根据本 CP/CPS 中的规定，明确责任方；
2. 由 GDCA 相关部门负责与申请人协调；
3. 若协调失败，再由有关法律部门进行裁决。
4. 任何与 GDCA 或授权机构就本 CP/CPS 所涉及的任何争议提起诉讼的，受 GDCA 工商注册所在地人民法院管辖。

8.2.14 管辖法律

GDCA 的 CP/CPS 受国家已颁布的《中华人民共和国电子签名法》和《电子政务电子认证服务管理办法》法律法规管辖。

8.2.15 与适用法律的符合性

无论 GDCA 的证书持有者、依赖方等实体在何地居住以及在何处使用 GDCA 的证书，本 CP/CPS 的执行、解释和程序有效性均适用中华人民共和国的法律。任何与 GDCA 或授权注册机构就本 CP/CPS 所涉及的任何争议，均适应中华人民共和国法律。

8.2.16 一般条款

8.2.16.1 完整协议

GDCA 的 CP/CPS 完整的文档结构包括：标题、目录、主体内容 3 部分。

关于对目录和主体内容修改后的替代内容，将完全代替所有先前部分、并被放置在 GDCA 的网站中以供查阅和浏览。

8.2.16.2 分割性

如果本 CP/CPS 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，GDCA 可以在最低必要的限度下修订该条款，使其继续有效，其余部分不受影响。

8.2.16.3 强制执行

GDCA 声明，若证书持有者、依赖方等实体未执行 GDCA 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。

8.2.16.4 不可抗力

GDCA 不对因战争、瘟疫、火灾、地震和其他天灾等不可抗力的事件所造成本 CP/CPS 规定担保责任的违反、延误或无法履行负责。

8.2.17 其他条款

GDCA 对本 CP/CPS 具有最终解释权。

附录:GDCA 电子政务电子认证证书策略和业务规则修订记录

版本	生效日期	修订内容
V 1.0	2011 年 5 月 1 日	依据国家法律法规，遵循《电子政务电子认证业务规则规范》等规范要求，编制《GDCA 电子政务电子认证业务规则》。
V 2.0	2015 年 9 月 1 日	根据目前的电子政务电子认证业务情况及系统建设情况对 V1.0 版的业务规则具体内容进行了更新，及文档整体框架调整。
V 2.1	2025 年 1 月 13 日	根据国家密码管理局《电子政务电子认证服务管理办法》等要求，对业务规则进行整体的更新及修订，包括增加对证书策略的描述等。