广东数字证书认证中心有限公司

电子认证业务规则

版本：V4.1　　生效日期：2015 年 3 月 10 日

目 录

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

一、 概括性描述

1.1 概述

1.1.1 公司简介

广东数字证书认证中心有限公司（GUANG DONG CERTIFICATE AUTHORITY CO., LTD，简称 GDCA 或者广东 CA）成立于 2003 年 3 月 6 日，是全资国有控股企业。2005 年 9 月，广东数字证书认证中心有限公司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：ECP4401021007）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。

本着“权威、创新、服务、公信”的运营理念，GDCA 致力于为电子商务、电子政务及社会信息化等应用提供优质的电子认证服务。

1.1.2 电子认证业务规则（CPS）

本电子认证业务规则（简称 CPS）根据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》等法律法规的要求，详细阐述了 GDCA 提供的电子认证服务整个过程、电子认证服务所遵循的规则以及电子认证服务相关参与者所承担的责任。本 CPS 由 GDCA 以及分支机构通过公开发布的形式告知电子签名订户、依赖方和其他相关参与者，以确保 GDCA 所提供的电子认证服务是合法、专业、权威的第三方电子认证服务。对于 GDCA 所提供电子认证服务过程的责任范围，本 CPS 也给予了明确的规定。

本 CPS 所阐述的内容遵循《GDCA 证书策略》（http://www.gdca.com.cn/channel/001005005001），同时也遵循《粤港电子签名证书互认证书策略》（http://www.gdei.gov.cn/flxx/dzzw/xxaq/201208/t20120808_108276.html）。在执行本 CPS 的过程中，《GDCA 证书策略》与《粤港电子签名证书互认证书策略》存在歧义的内容应按以下规则处理：应用于粤港跨境互认的证书遵循《粤港电子签名证

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

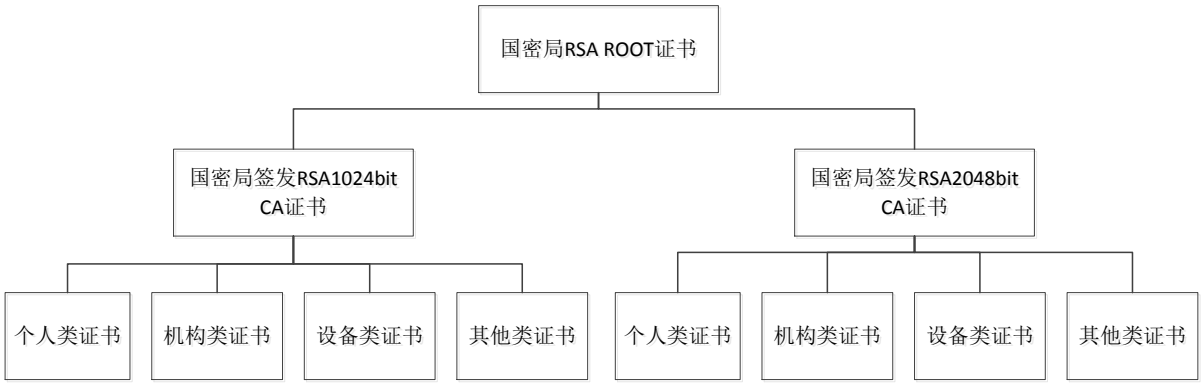
书互认证书策略》，应用于除粤港跨境互认外的证书遵循《GDCA 证书策略》。证书是否应用于粤港跨境互认项目可根据证书策略的对象标识符进行辨别。

GDCA 遵循 CA/浏览器论坛（CA/Browser Forum，国际组织，又称国际 CA 浏览器联盟，是制定 CA 国际标准的机构）(www.cabforum.org)发布的最新版本的 Guidelines、Baseline Requirment 进行签发和管理公共可信任 SSL 数字证书，并将持续根据其发布的版本进行修订，如果本 CPS 和 CA/浏览器论坛（CA/Browser Forum）发布的 Guidelines、Baseline Requirment 等相关规范中的条款有不一致的地方，则以 CA/浏览器论坛正式发布的规范为准。

1.1.3 GDCA 证书层次架构

GDCA 目前有 4 个根证书，分别为国家密码管理局（下称国密局）RSA ROOT 证书、GDCA ROOT 证书、国密局 SM2 ROOT 证书和 GDCA TrustAUTH R5 ROOT 证书。每个根 CA 下设子 CA，以签发用户证书。

1）国密局 RSA ROOT 证书（2048-bit）



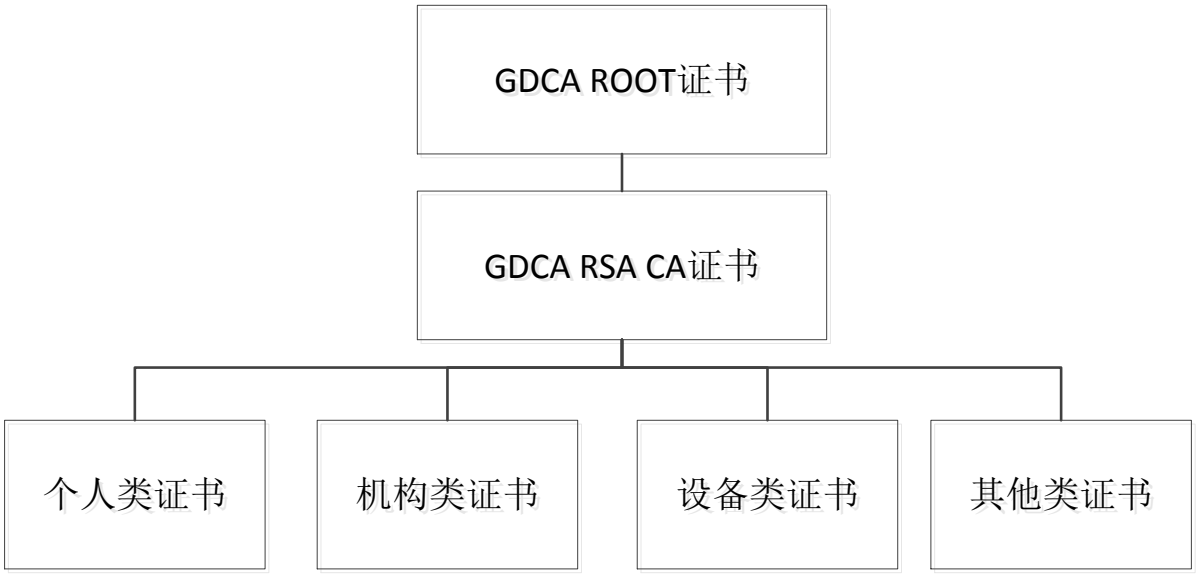
国密局 RSA ROOT 证书的根密钥长度为 2048-bit，下设两个子 CA 证书，其中：（1）国密局签发 RSA1024-bit CA 证书，签发密钥长度为 1024-bit 的个人类证书、机构类证书、设备类证书和其他类证书；（2）国密局签发 RSA2048-bit CA 证书，签发密钥长度为 2048-bit 和 1024-bit 的个人类证书、机构类证书、设备类证书和其他类证书。

国密局 RSA ROOT 证书将于 2025 年 8 月 23 日到期。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

国密局签发的 RSA1024-bit CA 证书将于 2015 年 7 月 19 日到期，2015 年 1 月 1 日起，GDCA 将不再使用该 CA 证书签发订户证书。国密局签发的 RSA2048-bit CA 证书将于 2018 年 12 月 15 日到期，2016 年 12 月 15 日起，GDCA 将不再使用该 CA 证书签发订户证书。

2）GDCA ROOT 证书（1024-bit）



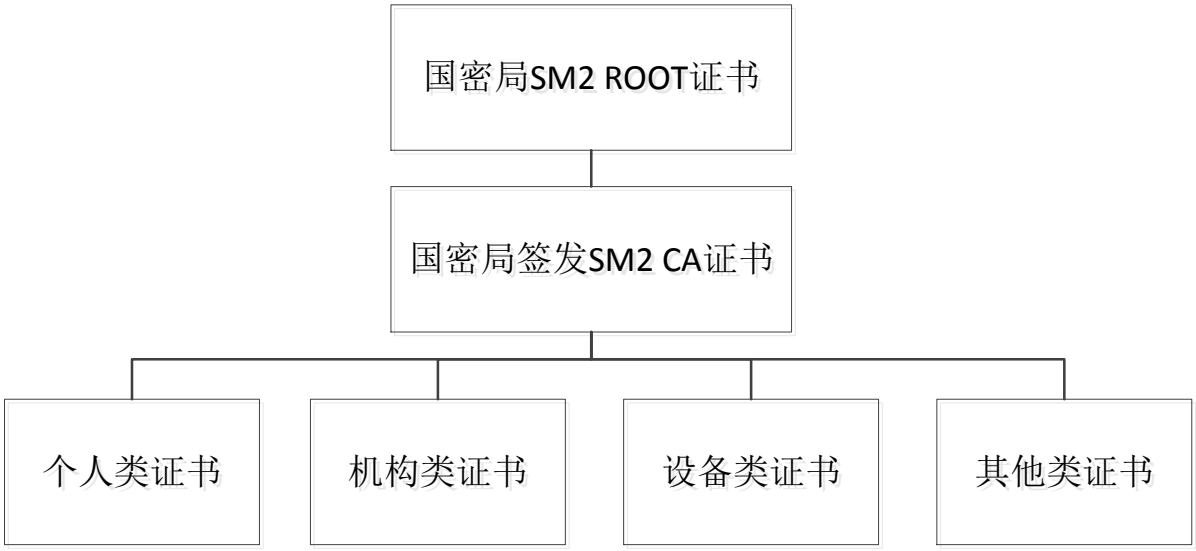
GDCA ROOT 证书的根密钥长度为 1024-bit，下设 GDCA RSA CA 证书，签发密钥长度为 1024-bit 的个人类证书、机构类证书、设备类证书和其他类证书。

GDCA ROOT 证书将于 2027 年 6 月 29 日到期。

GDCA RSA1024-bit CA 证书将于 2024 年 1 月 12 日到期，2016 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

3）国密局 SM2 ROOT 证书

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

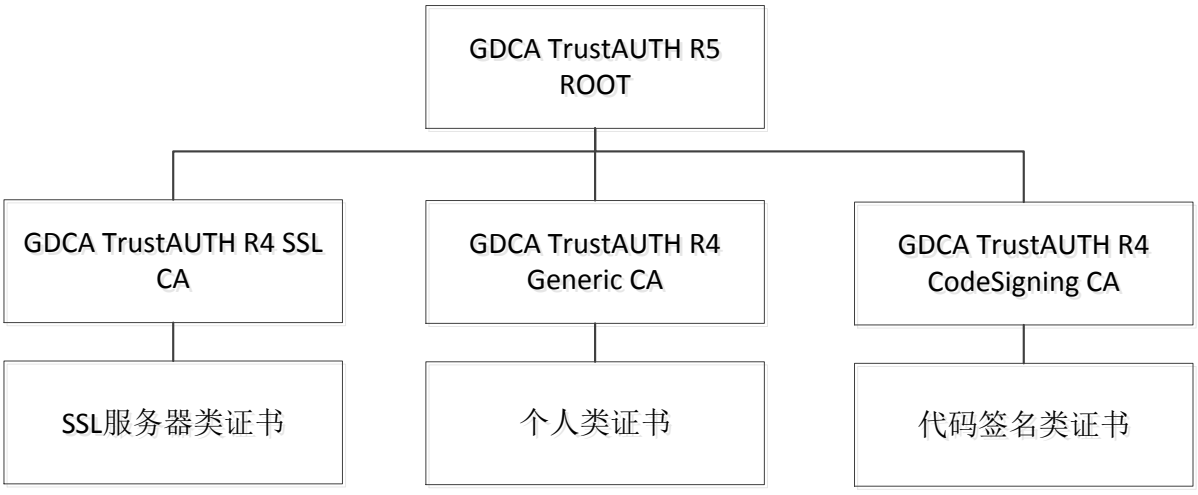


国密局 SM2 ROOT 证书的根密钥长度为 256-bit，下设国密局签发 SM2 CA 证书，签发采用国密算法 SM2 的个人类证书、机构类证书、设备类证书和其他类证书。

国密局 SM2 ROOT 证书将于 2042 年 7 月 7 日到期。

国密局签发的 SM2 CA 证书将在 2033 年 7 月 22 日到期，2030 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

4）GDCA TrustAUTH R5 ROOT 证书



GDCA TrustAUTH R5 ROOT 证书的根密钥长度为 4096-bit，下设三个子 CA 证书，其中：（1）GDCA TrustAUTH R4 SSL CA 证书，签发密钥长度为 2048-bit 的 SSL 服务

器类证书；（2）GDCA TrustAUTH R4 Generic CA 证书，签发密钥长度为 2048-bit 的个人类证书;（3）GDCA TrustAUTH R4 CodeSigning CA 证书，签发密钥长度为 2048-bit 的代码签名类证书。

GDCA TrustAUTH R5 ROOT 证书将于 2044 年 12 月 1 日到期。

GDCA TrustAUTH R4 SSL CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 Generic CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 CodeSigning CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

对于 GDCA TrustAUTH R4 SSL CA 证书签发的用户证书：GDCA 遵循 CA/B 论坛（https://www.cabforum.org.）发布的最新版本的 Baseline Requirment 进行签发和管理公共可信任 SSL 数字证书，如果本 CPS 和 Baseline Requirment 中的条款有不一致的地方，则以 Baseline Requirment 的内容为准。

1.2 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电子认证业务规则》（简称《GDCA CPS》），CPS 为“Certificate Practice Statement”的缩写。在本文档中，CPS 等同于本节中定义的文档名称和适用名称。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

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、提供数字证书验证服务等手段而成为电子认证活动的参与主体。

1.3.2 注册机构

GDCA 的数字证书注册机构是经 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 订户

在电子签名应用中，订户即是电子签名人、证书持有人，是 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、服务器或用于安全通信的其他设备。

1.3.4 依赖方

GDCA 的证书依赖方是指基于对 GDCA 提供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 的一个证书订户。

1.3.5 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。

1.4 证书应用

1.4.1 适合的证书应用

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、电子商务及其他社会化活动中，以实现身份认证、电子签名、关键数据加密等目的，同时也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。

GDCA 签发的证书，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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

- 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。

1.4.1.1 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。针对不同的安全保障级别和信任级别，分以下两类：

第1类个人证书——适用于对安全要求较低的电子商务中低额交易和非电子政务领域，包括但不限于在线会话的客户端鉴别、安全电子邮件、特定应用系统的身份认证。

第 2 类个人证书——除了第 1 类个人证书的适用范围之外，还适用于对安全要求较高的领域，包括但不限于电子政务及电子商务中提供的数字签名、加解密和身份认证。

1.4.1.2 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。针对不同的安全保障级别和信任级别，分以下两类：

第1类机构证书——适用于对安全要求较低的电子商务中低额交易和非电子政务领域，包括但不限于在特定应用系统中提供的数字签名、加解密和身份认证。

第 2 类机构证书——除了第 1 类机构证书的适用范围之外，还适用于对安全要求较高的领域，包括但不限于电子政务及电子商务中提供的数字签名、加解密和身份认证。

1.4.1.3 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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

1.4.1.4 SSL 服务器类证书

SSL 服务器证书标识 Web 网站或者 Web 服务器的身份，可以用于证明网站的身份或者资质、提供 SSL 加密通道，不得用于各类交易、支付的签名或验证。

1.4.1.5 代码签名类证书

代码签名证书标识软件代码的来源或者所有者，只能用于各类代码的数字签名，不得用于各类交易、支付、加密等应用。

代码签名证书订户必须承诺，不得将代码签名证书用于对恶意软件、病毒代码、侵权软件、黑客软件等的签名。

1.4.1.6 各类证书的证书策略对象标识符

第 1 类个人证书策略对象标识符: (1.2.156.112559.1.1.1.1).

第 2 类个人证书策略对象标识符: (1.2.156.112559.1.1.1.2).

第 1 类机构证书策略对象标识符: (1.2.156.112559.1.1.2.1).

第 2 类机构证书策略对象标识符: (1.2.156.112559.1.1.2.2).

设备证书策略对象标识符: (1.2.156.112559.1.1.3.1).

SSL 服务器类证书策略对象标识符: (1.2.156.112559.1.1.4.1).

代码签名类证书策略对象标识符: (1.2.156.112559.1.1.5.1).

粤港互认证书策略对象标识符：2.16.156.339.1.1.1.2.1（自然人）/ 2.16.156.339.1.1.2.2.1（法人）

1.4.2 限制的证书应用

每一类型的证书，都只能应用于证书所代表的主体身份适合的用途。例如，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，机构证书不能作为个人和设备证书来使用，设备证书也不能作为个人和机构证书来使用。任何不符合的应用，不受本 CPS 的保护。

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订户自行承担。特别声明，证书不设计用于、不打算用于、也不

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

1.5 策略管理

GDCA 安全策略委员会是 GDCA 电子认证服务所有策略的最高管理机构，负责审核批准 CPS，并作为 CPS 实施检查监督的最高决定机构。

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 CPS。GDCA 安全策略委员会由来自于公司管理层、行政中心、营销中心、技术中心、运营服务中心等拥有决策权的合适代表组成。

GDCA 安全策略委员会的所有成员在就证书策略进行管理和批准时，均享有一票决定权，如果选票相同，委员会主任可拥有双票决定权。

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 将对电子认证业务规则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 CPS 的问题、建议、疑问等，都可以按以下方式进行联系。

联系人：GDCA 行政管理部门

网站地址：http://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东风中路 448 号成悦大厦第 23 楼

邮政编码：510030

电话号码：020-83487228

传真号码：020-83486610

1.5.3 决定 CPS 符合策略的机构

GDCA 安全策略委员会是公司 CPS 策略制定的最高权威机构，审定批准 CPS，是决定 CPS 符合策略的机构。

1.5.4 CPS 批准程序

本机构的 CPS 由 GDCA 安全策略委员会组织 CPS 编写小组拟定文档,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，并根据《电子认证服务管理办法》中规定，从对外发布之日起的三十日之内向工业和信息化部备案。

1.5.5 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 CPS，CPS 编写小组根据相关的情况拟定 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 CPS，从对外发布之日起三十日之内向工业和信息化部备案。

1.6 定义和缩写

1.6.1 术语定义一览表

GDCA	广东省数字证书认证中心的缩写
GDCA 安全策略委员会	GDCA 认证服务体系内的最高策略管理监督机构和 CPS 一致性决定机构
电子认证服务机构	GDCA 及授权的下级操作子 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。
注册机构	注册机构（Registration Authority，RA）负责处理证书申请者和证书订户的服务请求，并将之提交给认证服务机构，为最终证书申请者建立注册过程的实体，负责

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

	对证书申请者进行身份标识和鉴别，发起或传递证书撤销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。
本地注册受理点	本地注册受理点（Local Registration Authority）是受理证书服务的终端机构，作为 GDCA 认证服务体系架构内直接面向用户的服务主体，经过 CA 或 RA 的授权从事各类服务。
录入员	负责录入证书申请者提交的信息，协助用户办理数字证书申请、撤销、更新等手续。
审核员	负责审核证书申请信息，协助用户办理数字证书申请、撤销、更新等手续。
电子签名认证证书	电子认证服务提供者签发的用以证明证书持有人的电子签名、身份、资格即其他有关信息的电子文件。
数字证书	使用数字签名作为识别签名人身份和表明签名人认可签名数据的一种电子签名认证证书。
电子签名	具有识别签名人身份和表明签名人认可签名数据的功能的技术手段。
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。
电子签名人	是指持有电子签名制作数据并以本人身份或者以其所代表的名义实施电子签名的人。
电子签名依赖方	是指基于对电子签名认证证书或者电子签名的信赖而从事有关活动的人。
私钥（电子签名制作数据）	在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。
公钥（电子签名验证数据）	是指订户验证电子签名的数据。
订户	从电子认证服务机构接收证书的实体，也被称为证书持

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

	有人。在电子签名应用中，订户即为电子签名人。
依赖方	依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。

1.6.2 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
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)
X.509		国际电信同盟认证体系的证书标准

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

二、 信息发布与信息管理

2.1 GDCA 信息库

GDCA 信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。GDCA 信息库内容包括但不限于以下内容：CP 和 CPS 现行和历史版本、证书、CRL、订户协议，以及其它由 GDCA 不定期发布的信息。GDCA 将及时发布包括证书、CPS 修订和其它资料等内容，这些内容必须保持与 CPS 和有关法律法规一致。GDCA 信息库可以通过网址：http://www.gdca.com.cn 查询，或由 GDCA 随时指定的其它通讯方法获得。

2.2 认证信息的发布

GDCA 在官方网站 http://www.gdca.com.cn 发布信息库，该网站是 GDCA 发布所有信息最首要、最及时、最权威的渠道。

GDCA 通过目录服务器发布订户的证书和 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吊销证书列表；同时，GDCA 提供在线证书状态查询服务，订户或依赖方可实时查询证书的状态信息。

同时，GDCA 也将会根据需要采取其他可能的形式进行信息发布。

2.3 发布的时间和频率

GDCA 在订户证书签发或者注销时，通过目录服务器或官方网站自动将证书和 CRL 发布，发布周期为不大于 24 小时，即在 24 小时内发布最新 CRL；在紧急的情况下，GDCA 可以自行决定证书和 CRL 的发布时间。GDCA 每年发布一次电子认证服务机构的 CA 证书撤销列表（ARL）。

信息库其他内容的发布时间和频率，由 GDCA 独立做出决定，这种发布应该是即时的、高效的，并且是符合国家法律的要求的。

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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

GDCA 通过网络安全防护、系统安全设计、安全管理制度确保只有经过授权的人员才能进行信息库的增加、删除、修改、发布等操作。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

三、 身份标识与鉴别

3.1 命名

3.1.1 名称类型

GDCA 颁发的数字证书，含有颁发机构和证书订户主体甄别名，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 GDCA Certificate Authority
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 证书订户的主体甄别名命名规则如下：

属性	值
国家（C）	CN
省（S）	订户所在省份，或者不用
地区（L）	订户所在城市，或者不用
机构（O）	机构属性如下定义： ● 对于有确定机构的订户，是订户所在机构名称； ● 对于没有确定机构的订户，是 GDCA。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

机构部门（OU）	可以包含以下一个或多个内容： ● 订户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）	订户的电子邮件地址，或不用
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

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。证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主体公钥中的公钥绑定的实体信息。

3.1.3 订户的匿名或伪名

本 CPS 规定，GDCA 的订户在进行数字证书申请时不能使用匿名或伪名。

3.1.4 理解不同名称的形式的规则

GDCA 签发的数字证书符合 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。

3.1.5 名称的唯一性

在 GDCA 信任域内，不同订户的证书的主体甄别名不能相同，必须是唯一的。但对于同一订户，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订户存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

证书申请者必须证明持有与所要注册公钥相对应的私钥，证明的方法包括在证书申请消息中包含数字签名（PKCS#10）、其它与此相当的密钥标识方法，或者 GDCA 要求的其它证明方式，包括提交的初始化信息（被分配的密钥存储介质和对应的 PIN 码）等。

3.2.2 机构身份的鉴别

任何组织（政府机构、企事业单位等），在以组织名义申请机构类证书、设备类证书、SSL服务器类证书等各类型证书时，应进行严格的身份鉴别，如通过查询可信数据库验证其真实性、面对面鉴别身份材料以及其他可以获得申请者明确的身份信息的方式等。机构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（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别，包括以下内容：

1. 机构订户需按申请证书的类别提交数字证书申请表、机构合法成立的文件和复印件、业务办理授权书、经办人有效身份证件的原件和复印件以及其他证明文件。
2. 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、企事业单位组织机构代码证等，或通过签发有效文件的权威第三方数据库确认；申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。
3. GDCA可以通过查询可信第三方数据库等方式，对申请者及其申请材料进行验证，避免信息填写错误，但注册信息最终以申请者确认为准。如有需要，GDCA可通过第三方得到的电话号码、邮政信函等方式与申请机构进行联络，以确认被申请者某个信息的真实性，如验证代理人的职位或验证申请表中的某个人是否是申请人。
4. 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比对经办人有效身份证件的原件或者复印件。授权代表人身份

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

鉴别方法包括面对面的审核方式。

5. 在域名、设备名称被作为证书主题内容申请证书时，还需要验证该组织是否拥有该权利，例如要求提交域名所有权文件、归属权证明文件或者申请者对所有权的书面承诺等。
6. 如果认为有需要，GDCA还可以通过从第三方获取的信息来验证该申请者个人的身份，如果GDCA无法从第三方得到所有所需的信息，可委托第三方进行调查，或要求申请者提供额外的信息和证明材料。

此外，必要时，GDCA 还可以设定其它所需要的鉴别方式和资料。

对于粤港跨境互认的证书，必须以面对面审核的方式确认授权代表身份，通过法定的身份证明文件（包括但不限于个人身份证、护照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），确认授权代表的真实身份。

对于GDCA TrustAUTH R4 SSL CA及GDCA TrustAUTH R4 CodeSigning CA签发的订户证书,GDCA建立评估标准用于识别存在潜在高风险欺诈情况的证书请求。对于识别为“高风险”的证书请求，GDCA直接予以拒绝。

3.2.3 个人身份的鉴别

对于所有类型的个人身份证书，包括个人类证书、代码签名类证书、SSL服务器类证书等，在申请时都必须对个人申请者进行真实身份的鉴别，如通过查询可信数据库验证其真实性、面对面鉴别身份材料以及其他可以获得申请者明确的身份信息的方式等。个人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必须对个人申请者的身份进行鉴证，包括如下内容：

1. 个人类订户需按申请证书的类别分别提交数字证书申请表、个人身份证明的文件和复印件；如果委托他人办理，额外提供委托办理授权书、经办人有效身份证件的原件和复印件。
2. 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。
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，但注册信息最终以申请者确认为准。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

4. 如果委托他人办理，核查授权经办人有效身份证件的原件和复印件。
5. 个人身份鉴别方法包括有面对面的审核方式。面对面审核时，将申请者本人和两份身份证明文件（包括原件和复印件）进行比较。身份证明文件必须是有效的身份证件。
6. 对于以某个组织中的个人身份名义申请的，还需要提交其所在单位提供的证明材料。
7. 当申请信息包含机构信息时，需要确认该机构是否存在，以及申请人是否属于该机构的成员。如要求提交任职证明文件、查询第三方数据库、发送确认电子邮件等。
8. 如果认为有需要，GDCA还可以通过从第三方获取的信息来验证该申请者个人的身份，如果GDCA无法从第三方得到所有所需的信息，可委托第三方进行调查，或要求申请者提供额外的信息和证明材料。
9. 此外，必要时，GDCA 还可以设定其它所需要的鉴别方式和资料。

申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。GDCA在进行了法律规定的有限审查以后，不承担对申请者的身份证明文件（如身份证等）进行合法性甄别的义务。

对于粤港跨境互认的证书，必须以面对面审核的方式确认申请者个人身份，通过法定的身份证明文件（包括但不限于个人身份证、护照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），确认授权代表的真实身份。

对于GDCA TrustAUTH R4 SSL CA证书及GDCA TrustAUTH R4 CodeSigning CA证书签发的订户证书，GDCA建立评估标准用于识别存在潜在高风险欺诈情况的证书请求。对于识别为“高风险”的证书请求，GDCA直接予以拒绝。

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. 设备类订户需要提交数字证书申请表，设备拥有者身份证明的文件和复印件、业务办理授权书、经办人有效身份证件的原件和复印件。
2. 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CPS §3.2.2节描述执行；订户为个人的，身份鉴别按照本CPS §3.2.3节描述执行。

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，但注册信息最终以申请者确认为准。
4. 核查授权经办人有效身份证件的原件和复印件。

3.2.5 域名的确认和鉴别

如果证书的名称为域名（或互联网 IP 地址），除了在对申请者递交的书面材料进行审核外，GDCA 需要申请者提供额外的域名(或互联网 IP 地址)使用权证明材料，或向相应的域名注册服务机构(或互联网 IP 注册服务机构)或者其它第三方查询，以确定申请者是否有权使用相应的域名(或互联网 IP 地址)。GDCA 还需要采取其它独立的审查措施，以确认该域名（或互联网 IP 地址）的归属权，如果要求申请者提供相应的协助，该申请者不得拒绝这种请求。

3.2.6 没有验证的订户信息

通常，除了该类型证书所必须要求的身份信息需要得到明确、可靠的验证以外，以下信息可以在申请时不被要求验证：

1. 订户的电子邮件地址；
2. 证书其他任何不被要求验证的信息。

对于没有验证的订户信息，GDCA 不承诺相关信息的真实性，不承担相关的法律责任。

3.2.7 授权确认

机构订户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或提供授权文件，作为机构对经办人的授权确认。

如有需要，GDCA 可通过第三方得到的电话号码、邮政信函等方式与申请机构进行联络，以确认被授权申请人的某个信息的真实性，如验证代理人的职位或验证申请表中的某个人是否是申请人。如果 GDCA 无法从第三方得到所有需要的信息，可要求第三方进行调查，或要求证书申请者提供额外的信息和证明材料。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

3.2.8 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，但是该电子认证服务机构的 CPS 必须符合 GDCA CP 要求，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。

3.3 密钥更新请求的标识与鉴别

在订户证书到期前，订户需要获得新的证书以保持证书使用的连续性。GDCA 一般要求订户产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。

3.3.1 常规密钥的更新的标识与鉴别

对于一般正常情况下的更新密钥申请，订户须提交能够识别原证书的足够信息，如订户甄别名、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；
- 用原证书上的订户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，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

GDCA 不提供证书被吊销后的密钥更新。

3.4 吊销请求的标识与鉴别

当 GDCA 或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。如果订户主动要求吊销证书，则按照本 CPS$3.2 节描述进行身份

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

鉴别。

3.5 授权服务机构的标识和鉴别

适用于 GDCA TrustAUTH R4 SSL CA 证书及 GDCA TrustAUTH R4 CodeSigning CA 证书签发的订户证书，GDCA 自行担任证书 RA，不再另行设立 RA。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

四、 证书生命周期操作要求

自 CA 认证系统签发之日算起，GDCA 签发的个人类型证书、机构类型证书的有效期为 3 年或以内；设备类型数字证书的有效期为 5 年或以内；SSL 服务器证书和代码签名证书的有效期为 3 年或以内。一个完整的证书生命周期包括申请、验证、签发、发布、更新、注销、吊销、归档等过程。

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

- 订户填写相应的证书申请表单。
- 订户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）将证书交付给订户。

2. 责任

- 订户有责任向 GDCA 提供真实、完整和准确的证书申请信息和资料。
- 注册机构承担对订户提供的证书申请信息与身份证明资料的一致性检查工作，同时承担相应审核责任。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

4.2 证书申请处理

4.2.1 识别与鉴别功能

当 GDCA 及其注册机构接受到订户的证书申请后，应按本 CPS 3.2.2、3.2.3、3.2.4 及 3.2.5 的要求，对订户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。

4.2.2 证书申请批准和拒绝

4.2.2.1 证书申请的批准

GDCA 注册机构成功完成了证书申请所有必需的确认步骤并提交证书请求后，GDCA 通过发行正式证书来批准证书申请，一旦证书被发行，CA 将没有继续的责任去调查证书信息的正确性。

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 CPS 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，注册机构（RA）可以拒绝证书申请：

1. 该申请不符合本 CPS 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。

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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

4.2.3 处理证书申请的时间

GDCA 授权的注册机构将做出合理努力来尽快确认证书申请信息，一旦注册机构收到了所有必须的相关信息，将在 7 个工作日内处理证书申请。

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。

4.3 证书签发

4.3.1 证书签发过程中注册机构（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，证书签发系统签发订户证书。

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。

4.3.2 电子认证服务机构和注册机构对订户的通告

GDCA 会采取以下几种通告方式告知订户：

1、电子或纸质的受理回执；

2、电子邮件（e-mail）；

3、通过面对面的方式，通知订户（如申请者到受理点领取等方式）；

4、其他 GDCA 认为安全可行的方式。

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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

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。

对于 GDCA TrustAUTH R4 SSL CA 及 GDCA TrustAUTH R4 CodeSigning CA 证书签发的订户证书，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，证书下载完毕即代表订户接受了证书。

2、GDCA 注册机构在订户的允许下，代替订户下载证书，并把证书通过邮件方式发送给订户，即代表订户接受了证书。

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。

4.4.2 电子认证服务机构对证书的发布

订户接受证书后，GDCA 在 24 小时内将该订户证书发布到 GDCA 的目录服务系统。

GDCA 采用主、从目录服务器结构来分布所签发证书。签发完成的数据直接发布到主目录服务器中，然后通过主从映射，将主目录服务器的数据自动同步到从目录服务器中，供订户和依赖方查询和下载。

4.4.3 电子认证服务机构对其他实体的通告

GDCA 及注册机构将不对其他实体进行通告。其他实体可以通过从目录服务器中查询到 GDCA 已经签发的数字证书。

4.5 密钥对和证书的使用

4.5.1 订户的私钥和证书的使用

订户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。订户接受到数字证书，应妥善保存其证书对应的私钥。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

订户只能在本 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，订户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。在证书到期或被吊销之后，订户必须停止使用该证书对应的私钥。

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。

4.6 证书更新

证书更新指在不改变证书订户的公钥或其他任何信息的情况下，为订户签发一张新证书。证书更新时无需再提交证书注册信息，订户提交能够识别原证书的足够信息，如订户甄别名、证书序列号等，使用原证书的私钥对包含公钥的更新申请信息签名。

4.6.1 证书更新的情形

对于 GDCA 签发给订户的证书，订户在证书到期前 30 天起便可进行证书更新。到期前 30 天内至到期后 30 天内，订户可访问 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。证书到期 30 天后，如果订户还未申请证书更新，GDCA 视情况有权吊销该证书。证书吊销后订户如需继续使用，必须重新申请新证书。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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 证书更新请求的处理

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。

在证书更新时，订户可以用原有的私钥对更新请求进行签名，GDCA 将会对用户的签名和公钥、更新请求内包含的用户信息进行正确性、合法性和唯一性的验证和鉴别：

- 订户对申请信息进行签名，CA 用其原有证书中的公钥对签名进行验证
- 订户注册信息没有发生变化，CA 基于其原有注册信息对其进行签发新的证书

订户也可以选择一般的初始证书申请流程进行证书更新，按照本 CPS$3.2 的要求提交相应的证书申请和身份证明资料。GDCA 在任何情况下都可将这种初始证书申请的鉴别方式作为证书更新时的鉴别处理手段。

4.6.4 颁发新证书时对订户的通告

同本 CPS$4.3.2

4.6.5 构成接受更新证书的行为

同本 CPS$4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

同本 CPS$4.4.2

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

4.6.7 电子认证服务机构对其他实体的通告

同本 CPS$4.4.3

4.7 证书密钥更新

证书密钥更新时无需再提交证书注册信息，订户提交能够识别原证书的足够信息，如订户甄别名、证书序列号、原证书对应的私钥对证书密钥更新请求签名等，并上送新的公钥申请签发新证书。

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。

鉴于第 1 类个人证书和第 1 类机构证书适用于对安全要求较低的应用领域，该类证书不被允许进行密钥更新，需要注销原有证书，重新申请证书。

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 证书密钥更新请求的处理

GDCA 对证书密钥更新请求的处理通过证书更新请求处理流程完成。

GDCA 证书密钥更新请求的处理流程同本 CPS$4.6.3 节描述。

4.7.4 颁发新证书时对订户的通告

同本 CPS$4.3.2。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

4.7.5 构成接受密钥更新证书的行为

同本 CPS$4.4.1。

4.7.6 电子认证服务机构对密钥更新证书的发布

订户接受证书后，GDCA 在其规定的时间内将该订户更新后的证书发布到 GDCA 的目录服务系统。

4.7.7 电子认证服务机构对其他实体的通告

同本 CPS$4.4.3

4.8 证书变更

当证书信息发生变化时，订户须重新办理证书。GDCA 不予接受对已发出的证书的内容作出变更的请求。

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。

如果证书内包含信息的变更可能影响订户权利义务的改变，则订户不能申请证书变更，只能吊销该证书，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。

4.8.2 请求证书变更的实体

请求证书变更的实体为证书订户。

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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

4.8.4 颁发新证书时对订户的通告

同本 CPS$4.3.2

4.8.5 构成接受变更证书的行为

同本 CPS$4.4.1。

4.8.6 电子认证服务机构对变更证书的发布

订户接受证书后，GDCA 在其规定的时间内将该订户证书发布到 GDCA 的目录服务系统。

4.8.7 电子认证服务机构对其他实体的通告

同本 CPS$4.4.3

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

当发现以下的情况，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) 证书主体(无论是 CA 还是订户)违反了 CPS 规定的重要职责；
3) CPS 中职责的履行被延迟或受不可抗力的阻碍；自然灾害；计算机或通信失败；法律、规章或其它法律的改变；政府行为；或其它超过个人控制的原因并且对他人信息构成威胁的；
4) 订户主动提出吊销请求；
5) GDCA 发现订户在申请时提供的证明材料不真实；
6) GDCA 已经履行催缴义务后，订户仍未缴纳服务费。

发生下列情形，对于 GDCA 证书服务系统中使用的证书，例如 CA、RA、受理点或其它服务主体（包括服务系统中的设备使用的证书）使用的证书，可以吊销其证书：

1. GDCA 与 RA、受理点等签订的协议终止或者发生改变；

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

2. 证书私钥发生安全性损害或者被怀疑发生安全性损害；
3. 出于管理的需要。

证书订户如果发现或者怀疑证书私钥安全发生损害，应立即通知 GDCA 进行吊销。对于 SSL 服务器类证书，若出现以下任意一项或几项情形，也需进行证书吊销操作：

1. 在任何 GDCA 得知证书中的域名或 IP 地址的使用不再被法律所允许的情形，如域名注册者使用域名的权利已被法院或仲裁机构撤销、与域名注册机构的合约终止、域名注册者更新域名失败等；
2. GDCA 得知一个通配符证书被用来验证一个欺诈性误导的子域名；
3. GDCA 由于某种原因终止运行，并且未安排其他 CA 提供吊销证书的支持性操作；
4. GDCA 签发证书的权利已届满或被撤销或终止，除非 GDCA 已作出安排，继续维护 CRL/OCSP；
5. 证书的技术内容或格式造成了对应用软件供应商或依赖方不可接受的风险。

4.9.2 请求证书吊销的实体

请求证书吊销实体为订户、注册机构、GDCA 和经司法机构授权的司法人员。

4.9.3 吊销请求的流程

4.9.3.1 订户主动提出注销申请

1) 订户向注册机构提出证书注销申请，并填写《证书吊销（注销）申请表》，GDCA 只接受订户现场提出注销申请，不接受非现场方式提出的证书注销申请。注册机构核实申请吊销实体的身份和授权实体的身份。
2) 注册机构将《证书吊销（注销）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相信需要吊销最终订户的证书时，GDCA 或注册机构的有关人员可以通过内部确定的流程提请吊销证书。
2) 在证书吊销后，GDCA 或注册机构将通过适当的方式，包括邮件、电话、传真

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

等，通知最终订户证书已被吊销及被吊销的理由。若未能联络订户时，在必要的情况下，GDCA 对吊销、挂起的证书将通过网站进行公告。

4.9.3.3 电子认证服务机构本身证书的吊销

GDCA 本身证书的吊销，必须经过相关监管部门确定后才可以进行。

4.9.4 吊销请求宽限期

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

4.9.5 电子认证服务机构处理吊销请求的时限

GDCA 处理吊销请求的周期为 24 小时。

4.9.6 依赖方检查证书吊销的要求

GDCA 提供在线吊销状态查询，依赖方可在 GDCA 的网站上进行查询。

4.9.7 CRL 发布频率

GDCA 的 CRL 发布周期为 24 小时，即在 24 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。

4.9.8 CRL 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。

4.9.9 在线状态查询的可用性

GDCA 向证书订户和依赖方提供在线证书状态查询服务。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

4.9.10 在线状态查询要求

用户可以自由进行在线状态查询，GDCA 没有设置任何的读取权限。如果依赖方无法查询 CRL，则应通过 OCSP 或访问网站的形式对证书状态进行查询。

4.9.11 吊销信息的其他发布形式

GDCA 不提供吊销信息的其他发布形式。

4.9.12 密钥损害的特别要求

除本 CPS 中$4.9.1 规定的情形外，当订户或注册机构的证书密钥已经失密或者可能已经失密时，必须及时向 GDCA 提出证书吊销请求。

4.9.13 证书挂起的情形

不适用。

4.9.14 请求证书挂起的实体

不适用。

4.9.15 挂起请求的流程

不适用。

4.9.16 挂起的期限限制

不适用。

4.10 证书状态服务

4.10.1 操作特征

订户可以通过 CRL、LDAP、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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

4.10.2 服务可用性

GDCA 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，订户能够实时获得证书状态查询服务。

4.10.3 可选特征

证书状态的其他可选服务方式为订户利用 GDCA 指定的 CRL 地址，通过目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的查询。

4.11 订购结束

订购结束包含以下情况：

1) 当订户停止使用 GDCA 提供的数字证书时，必须向 GDCA 提出证书注销的申请。申请流程为本 CPS$4.9.3 的规定。GDCA 注销证书后，表明订户的订购行为正式结束。
2) 当证书有效期结束后，订户未按时续缴服务费时，GDCA 吊销证书后，表明订户的订购行为正式结束。
3) 证书有效期期满，没有进行证书更新或密钥更新，表示订户订购行为正式结束。

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，将实时把该订户的证书注销，并按照 CRL 发布策略进行发布；GDCA 详细记录吊销证书的操作过程并定期将订购结束后的证书及相应订户数据进行归档。

4.12 密钥生成、备份与恢复

4.12.1 密钥生成、备份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

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

对于 GDCA TrustAUTH R4 SSL CA 证书及 GDCA TrustAUTH R4 CodeSigning CA 证书签发的订户证书，GDCA 不提供代用户生成签名密钥对的操作。

GDCA 不提供订户私钥的托管和恢复服务。

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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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 的建筑物和机房建设按照下列标准实施：

1) GB/T 25056-2010《信息安全技术 证书认证系统密码及其相关安全技术规范》
2) 国密局[2010]7 月《电子政务电子认证基础设施建设要求》
3) GB50174-2008《电子信息系统机房设计规范》
4) GB6650-1986：《计算机机房用活动地板技术条件》
5) GB2887-2011《计算机场地通用规范》
6) GB30003-93《电子计算机机房施工及验收规范》
7) GB50222-95《建筑内部装修设计防火规范》
8) GB50116-98《火灾自动报警系统设计规范》
9) GB50057-94《建筑物防雷设计规范》
10) GB5054-95《低压配电设计规范》
11) GB/J19-87《采暖通风与空气调节设计规范》
12) SJ/T10796-1996《计算机机房用活动地板技术条件》
13) YD/T754-95《通讯机房静电防护通则》

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。

5.1.1.1 公共区域

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

5.1.1.2 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。

5.1.1.3 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。

5.1.1.4 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。

5.1.1.5 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。

5.1.2 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

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

5.1.3 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。

5.1.4 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·m2 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。

5.1.5 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。

5.1.6 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。

5.1.7 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。

5.1.8 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

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

商提供的方法先将其初始化并进行物理销毁。

5.1.9 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。

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。

5.2.2 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

5.2.3 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。

5.2.4 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：

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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

5.3 人员控制

5.3.1 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. 具备良好的团队合作精神。
6. 无违法犯罪记录。
7. 关键和核心岗位的工作人员必须具备相关的工作经验，或通过 GDCA 相关的培训和考核后方能上岗。

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。

5.3.2 背景审查程序

GDCA 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。背景调查必须符合法律法规的要求，调查内容、调查方式和从事调查的人员不得有违反法律法规的行为。背景调查应使用合法手段，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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

5.3.3 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 安全管理策略和机制；
- 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；

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

- 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。

GDCA 将员工参加培训的情况形成记录并存档，对于签发 SSL 服务器证书和代码签名证书的操作员和审核员，上岗前必须通过培训并达到 Baseline Requirement 中要求的从事该项工作所必须的技能水平。

5.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受 GDCA 组织的培训一次。对于认证系统运营相关的人员，每年至少进行一次相关技能和知识培训。此外，GDCA 将根据机构系统升级、策略调整等要求，不定期的要求人员进行继续培训。

5.3.5 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。

5.3.6 在职人员的工作考察

GDCA 行政部门每季度组织工作人员对各部门进行工作记录检查和在职人员绩效考核，在职人员填写绩效改进表后交由部门经理审核，由部门经理进行绩效评估。

5.3.7 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，将立即吊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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

5.3.8 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；
- 具有 1 年以上相关业务工作经验；
- 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。

5.3.9 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、电子认证业务规则和有关的协议和规范；
- 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。

5.4 审计日志程序

5.4.1 记录事件的类型

所有发生在 GDCA 的重大安全事件都会自动地打上时间印章并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、吊

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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. 证书申请事件，包括订户接受订户协议，接受申请的单位、申请资料的验证、申请及验证资料的保存等；
4. 证书生命周期内的管理事件，包括证书的申请、批准、更新、吊销等； 系统安全事件，包括：成功或不成功访问 CA 系统的活动，对于 CA 系统网络的非授权访问及访问企图，对于系统文件的非授权的访问及访问企图，安全、敏感的文件或记录的读、写或删除，系统崩溃，硬件故障和其他异常；
5. 防火墙和路由器记录的安全事件；
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，包括网络权限的帐号申请记录，系统权限的申请、变更、创建申请记录，人员情况变化。

5.4.2 处理日志的周期

GDCA 每周进行一次日志跟踪处理，检查违反政策及其它重大事件，每月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。

5.4.3 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十年。

5.4.4 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

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

5.4.5 审计日志备份程序

GDCA 的审计跟踪文档由业务管理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。

5.4.6 审计收集系统

GDCA 设置自动审核系统以审核记录与资料，自动向有关人员或系统报告审核事件。

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。

5.4.7 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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

5.4.8 脆弱性评估

CA 安全程序根据政策、技术和管理的变化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。

5.5 记录归档

5.5.1 归档记录的类型

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. 证书和证书吊销列表；
3. 证书申请支持文档，证书服务批准和拒绝的信息，与证书订户的协议；
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。

5.5.2 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. 对订户证书生命周期内的管理事件的归档，保留 10 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. 订户证书的归档保留期限不少于证书失效后 10 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 10 年。

5.5.3 归档文件的保护

GDCA 数据库由 GDCA 主密钥进行加密和保护。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

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

入口，只有 GDCA 的业务管理人员可以访问。

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，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。

所有归档的电子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。

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

GDCA 的审计跟踪档案收集系统在本 CPS$5.4 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。

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 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。

5.6 电子认证服务机构根证书有效期限

GDCA 的根证书有效期最长不超过 30 年，任何由其签发的证书，包括子 CA 证书和订户证书，其有效期都短于根证书的有效期，任何由子 CA 其签发的订户证书，其有效期都短于子 CA 证书的有效期。

根证书及子 CA 证书的有效期，在证书内有明确的表示。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

5.7 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. 在下级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：

- 新私钥签名的包含新公钥的 GDCA 证书；
- 新私钥签名的包含旧公钥的 GDCA 证书；
- 旧私钥签名的包含新公钥的 GDCA 证书。

5.8 损害与灾难恢复

5.8.1 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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

5.8.2 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。

5.8.3 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吊销或之后重新认证。
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。
6. 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订户进行通告，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，供证书订户和依赖方查询。同时 GDCA 立即生成新的密钥对。
4. 新的根证书签发后，按照 GDCA CPS 关于证书签发的规定，重新签发下级证书和下级操作子 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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

当子 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订户进行通告，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，供证书订户和依赖方查询。
5. 新的子 CA 证书签发后，按照 GDCA CPS 关于证书签发的规定，重新签发订户证书。
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。

证书订户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，订户应按照 GDCA 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。

5.8.4 灾难后的业务连续性能力

GDCA 在遭遇本节 5.8.1、5.8.2 和 5.8.3 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。

5.9 电子认证服务机构或注册机构的终止

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；

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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 通知订户的过程尽快完成；由于非密钥受损原因终止 GDCA，在 GDCA 通知所有订户后，采取适当的步骤减轻 GDCA 终止对订户影响。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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 签名密钥对生成

GDCA 订户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 支持多种模式的签名密钥对产生方式，对于第 1 类个人证书、第 1 类机构证书，可以使用硬件密码模块（如：USB Key），也可以使用标准的软件密码模块（如：浏览器自带的密码模块，Web 服务器软件提供的密钥生成功能等），证书申请者可根据其需要进行选择。对于第 2 类个人证书、第 2 类机构证书、设备证书，则必须使用硬件密码模块生成密钥。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。

证书订户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。

6.1.1.2 加密密钥对生成

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。

对于 GDCA TrustAUTH R4 SSL CA 及 GDCA TrustAUTH R4 CodeSigning CA 证书签发的订户证书，订户密钥对由订户自身的服务器或其它设备内置的密钥生成机制生成，GDCA 不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

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

对的生成和存储设备。

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。

对于 GDCA TrustAUTH R4 SSL CA 及 GDCA TrustAUTH R4 CodeSigning CA 证书签发的订户证书，私钥由订户自行生成，GDCA 不需要将私钥传递给订户。

6.1.3 公钥传送给证书签发机构

由证书签发机构对密钥管理中心提出密钥请求，密钥管理中心对产生的加密公钥使用通信证书进行数字信封加密，以数据流的方式传送给证书签发机构，由证书签发机构对获取的密文数据进行解密，并将解密的密钥信息进行签发证书。密钥传送过程中使用的通信证书在证书签发机构搭建时生成。

对于 GDCA TrustAUTH R4 SSL CA 及 GDCA TrustAUTH R4 CodeSigning CA 证书签发的订户证书，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。

6.1.4 电子认证服务机构公钥传送给依赖方

GDCA 的公钥包含在 GDCA 自签发的根 CA 证书和业务 CA 证书中，通过 GDCA 官方网站进行发布。GDCA 支持从 GDCA 的网站下载的方式传递公钥，以供证书订户和依赖方查询使用。

6.1.5 密码算法技术标准

GDCA 支持的 RSA 密钥长度为 1024 位或以上，适用于 GDCA TrustAUTH R4 SSL CA 证书、GDCA TrustAUTH R4 Generic CA 证书和 GDCA TrustAUTH R4 CodeSigning CA 证书签发的订户证书，其密钥长度至少为 2048 位或以上。如果国家法律法规、政府

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

6.1.6 证书载体

GDCA 根据不同的应用需求，使用实现了 PKCS#11 或通过国家密码管理局审查的 USB key 作为证书载体。USB key 是一种具有安全文件系统的加密硬件设备，其内部芯片以智能卡为核心安全模块，既安全可靠，又方便携带，当受到暴力破坏时，具有自动销毁密钥功能。

6.1.7 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，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。

6.1.8 密钥使用目的

订户的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等；加密密钥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。

6.2 私钥保护和密码模块工程控制

6.2.1 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、备份和恢复应遵循 FIPS140-2 标准的相关规定。由于 FIPS140-2 标准并非是国家密码主管部门认可和支持的标准，国家对于密码产品有严格的管理要求，因此，GDCA 在选择加密设备时，仅参照 FIPS140-2 标准的要求，是在国家密码管理政策许可前

提下的选择性适用，具体参照设备厂商提供的资料。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。

6.2.2 私钥多人控制（m 选 n）

GDCA 私钥的生成、更新、吊销、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。

6.2.3 私钥恢复

为维护国家权益，密钥管理中心的密钥采用密钥恢复机制，对密钥管理中心生成的加密密钥对由密钥管理中心管理，确保国家对任何使用密钥加密的数据都能依照法律流程进行司法恢复，维护国家权益。

6.2.4 私钥托管

订户加密证书对应的私钥由广东省密钥管理中心托管，订户的签名证书对应的私钥由自己保管，密钥管理中心不负责托管。

广东省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。

6.2.5 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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

6.2.6 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。

私钥到期后，GDCA 在 10 天内完成归档操作。私钥归档保存至少 7 年。

6.2.7 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。对于存放在软件密码模块中的私钥，如果订户愿意并且自行承担相关风险，订户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。

6.2.8 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。

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。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，订户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。

6.2.9 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

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。对于存放在订户计算机软件密码模块中的私钥，订户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，其他人员使用订户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。

6.2.10 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。

订户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。

6.2.11 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吊销后，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。

订户的私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，由订户决定其销毁方法，订户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，订户必须按照本 CPS 的规定执行。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

6.2.12 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。

6.3 密钥对管理的其他方面

6.3.1 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。

6.3.2 订户托管密钥归档和销毁

无规定。

6.3.3 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，但并不完全保持一致。

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。

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。

对于不同的证书，其密钥对允许通过证书更新的最长使用期限如下：

- 对国密签发的 RSA2048 位 CA 证书，其密钥对的最长允许使用年限是 10 年，可少于 10 年
- 对国密签发的 RSA1024 位 CA 证书，其密钥对的最长允许使用年限是 10 年，

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

可少于 10 年

- 对国密签发的 SM2CA 证书，其密钥对的最长允许使用年限是 20 年，可少于 20 年
- 对于 GDCA 的 RSA4096 位根 CA 证书，其密钥对的最长允许使用年限是 30 年，可少于 30 年。
- 对于 GDCA 的 RSA1024 位根 CA 证书，其密钥对的最长允许使用年限是 30 年，可少于 30 年。
- 对于 GDCA 的 RSA1024 位根 CA 签发的 RSA1024 的 CA 证书，其密钥对的最长允许使用年限是 20 年，可少于 20 年。
- 对于 RSA2048 位最终订户证书，其密钥对的最长允许使用年限是 8 年，可少于 8 年
- 对于 RSA1024 位最终订户证书，其密钥对的最长允许使用年限是 4 年，可少于 4 年
- 对于 SM2 最终订户证书，其密钥对的最长允许使用年限是 4 年，可少于 4 年

6.4 激活数据

6.4.1 激活数据的产生和安装

为了保护私钥的安全，证书订户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。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订户。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：

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

- 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

6.4.2 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。

订户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。如果证书订户使用口令或 PIN 码保护私钥匙，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户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。

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，对于申请证书的订户激活数据的生命周期，规定如下：

1、订户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，建议订户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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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，按照国标《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。

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，并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。

6.6 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：

1. 制定公司内部的升级变更申请制度，并要求工作人员严格按照流程执行；
2. 制定公司内部的采购流程及管理制度；
3. 开发程序必须在开发环境进行严格测试成功后，再申请部署于生产环境；

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

4. 变更部署前进行有效的在线备份；

5. 第三方验证和审查；

6. 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，严格遵循国家密码管理局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具备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。

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

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

中心等设备或系统。

为了确保网络安全，GDCA 认证业务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。

6.8 时间戳

认证系统的各种系统日志、操作日志都应该有相应的时间标识。这些时间标识不需要采用基于密码的数字时间戳技术。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

七、 证书、证书吊销列表和在线证书状态协议

7.1 证书

GDCA 使用的详细证书格式符合国家相关标准要求，是 ITU-T 推荐的一个国际标准 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 5280：Internet X.509 公钥基础设施证书和 CRL 结构（2008 年 5 月）。

7.1.1 版本

GDCA 证书符合 X.509 V3 版证书格式，版本信息存放在证书版本格式栏内。

7.1.2 证书扩展项

GDCA 除了使用 X.509 V3 版证书标准项和标准扩展项以外，还使用了自定义扩展项。

1、证书标准项

- 证书版本号(Version)

指明 X.509 证书的格式版本，值为 V3。

- 证书序列号（SerialNumber）

即由 GDCA 分配给证书的唯一的数字型标识符。

- 签名算法标识符（Signature）

指定由 GDCA 签发证书时所使用的签名算法。

- 签发机构名（Issuer）

用来标识签发证书的 CA 的 X.500 DN 名字。即 GDCA 各个属性，包括国家、省、市、机构、单位部门、和通用名。

CN = GDCA Guangdong Certificate Authority

OU = Guangdong Certificate Authority

O = GDCA Certificate Authority

L = Guangzhou

S = Guangdong

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

C = CN

- 证书有效期（Validity）

用来指定证书的有效期，包括证书开始生效的日期和时间以及失效的日期和时间。每次使用证书时，需要检查证书是否在有效期内。

- 证书用户名（Subject）

指定证书持有者的 X.500 唯一名字。包括国家、省、市、机构、单位部门和通用名，还可包含 email 地址等个人信息等。

- 证书持有者公开密钥信息（subjectPublicKeyInfo）

证书持有者公开密钥信息域包含两个重要信息：证书持有者的公开密钥的值；公开密钥使用的算法标识符。此标识符包含公开密钥算法和 hash 算法。

2、证书扩展项

- 颁发机构密钥标识符（Issuer Unique Identifier）

此域用在当同一个 X.500 名字用于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500 名字。

- 主题密钥标识符（Subject Unique Identifier）

此域用在当同一个 X.500 名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500 名字。

- 密钥用法（key usage）

指定各种密钥的用法：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。

- CRL 发布点

由 GDCA 指定的 CRL 发布点。

3、自定义扩展项

针对不同的证书应用服务需求，GDCA 可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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

- 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。

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

GDCA 签发的证书，其识别名称不允许为匿名或者伪名，必须是有确定含义的识别名称。

7.1.6 证书策略对象标识符

证书策略对象标识符同本 CPS $1.4.1.6。

7.2 证书吊销列表

GDCA 定期签发 CRL，供用户查询使用。

7.2.1 版本

GDCA 的证书吊销列表采用 X.509 v2 版的证书格式。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

7.2.2 CRL 和 CRL 条目扩展项

GDCA 的证书吊销列表（CRL）是一个带有时间戳并且经过数字签名的已吊销证书的列表。CRL 的签发者是 CA，GDCA 通过发布 CRL 提供它所签发的数字证书的状态信息。

- CRL 的版本号：用来指定 CRL 的版本信息，GDCA 采用的是同 X.509 V3 证书对应的 CRL V2 版本。
- 签名算法：GDCA 采用 sha1 RSA 签名算法。
- 颁发者：指定签发机构的 DN 名，由国家、省、市、机构、单位部门和通用名等组成。
- 生效时间：指定一个日期/时间值，用以表明本 CRL 发布的时间。
- 更新时间：指定一个日期/时间值，用以表明下一次 CRL 将要发布的时间（本标准强制使用该域）。
- 吊消证书列表：指定已经吊销或者挂起的证书列表。本列表中含有证书的序列号和证书被吊销的日期和时间。
- 颁发机构密钥标识符（Issuer Unique Identifier）：本项标识用来验证在 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥。

7.3 在线证书状态协议

GDCA 采用 IETF PKIX 工作组开发的一个在线证书状态协议 (Online Certificate Status Protocol，OCSP，RFC2560)，该协议定义了一种标准的请求和响应信息格式以确认证书是否被撤销了。在 GDCA 官方网站下载 OCSP 查询客户端并按照 GDCA 官方网站发布的 OCSP 操作说明进行配置，即可使用 GDCA 的在线证书状态查询服务。GDCA 签发的 OCSP 响应至少包含以下所述的 OCSP 机构基本域和内容：

- Version：客户端使用的 OCSP 协议的版本号；GDCA 的在线证书状态协议为 v1 版。
- signatureAlgorithm：签发 OCSP 的算法；
- responderID：签发 OCSP 的实体。签发者公钥的 SHA1 数据摘要值和证书甄别名。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

- producedAt：OCSP 响应生成的日期和时间；
- Signature：OCSP 响应消息的数字签名。
- Nonce(一次性随机数)：在状态请求消息中的每一个 requestExtensions 变量和响应消息中的 responseExtension 变量中包含一次性随机数，防止重放攻击。
- 证书状态：证书的最新状态，包括有效、吊销和未知。

7.3.1 OCSP 请求和响应处理

一个 OCSP 请求包含以下数据：

协议版本、服务要求、目标证书标识和可选的扩展项等。

在接受一个请求之后，OCSP 服务端响应时进行如下检测：

- 信息正确格式化
- 响应服务器被配置提供请求服务
- 请求包含了响应服务器需要的信息，如果任何一个先决条件没有满足，那么 OCSP 服务端将产生一个错误信息；否则的话，返回一个确定的回复

所有确定的回复都由 GDCA 证书签发者密钥进行数字签名，主要回复状态包括：证书有效、已撤销、未知。回复信息由以下部分组成：

- 回复语法的版本
- 响应服务器名称
- 对请求端证书的回复
- 可选扩展
- 签名算法对象标识符号
- 对回复信息散列后的签名

如果出错，OCSP 服务器会返回一个出错信息，这些错误信息没有 GDCA 证书签发者密钥的签名。出错信息主要包括：

- 未正确格式化的请求（malformedRequest）
- 内部错误（internalError）
- 请稍后再试（trylater）
- 需要签名（sigRequired）

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

◆ 未授权（unauthorized）

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

八、 认证机构审计和其他评估

8.1 评估的频率或情形

GDCA 应每季度内部进行一次一致性审计和运营评估，并每次抽取至少 3%数量的 SSL 数字证书进行评估，以保证证书服务的可靠性、安全性和可控性。所抽取的 SSL 数字证书为 GDCA TrustAUTH R4 SSL CA 和 GDCA TrustAUTH R4 CodeSigning CA 签发的订户证书。

除了内部审计和评估外，GDCA 还聘请独立的审计师事务所，按照 WebTrust 对 CA 的规则进行外部审计和评估：

1、根据《中华人民共和国电子签名法》、《电子认证服务管理办法》等的要求，每年一次接受主管部门的评估和检查。

2、GDCA 按照国家主管部门的要求、国家相关标准和本 CPS 的规定实施运营和服务，按照内部评估和审计规范，每年至少定期执行一次内部的评估审核，包括对 GDCA 内其它实体（RA、受理点等）的评估审核。

3、GDCA 聘请独立的审计师事务所，按照 WebTrust 对 CA 的审计规则，每年进行一次外部审计和评估。

4、GDCA 每年进行一次风险评估工作，识别内部与外部的威胁，并评估威胁事件发生的可能性及造成的损害，并评估目前的应对策略、技术、系统以及相关措施是否足够应对风险。

8.2 评估者的资质

GDCA 的内部审计，由 GDCA 安全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。

GDCA 聘请的外部审计机构，应该具备以下的资质：

- 必须是经许可的、有执业资格的评估机构，在业界享有良好的声誉
- 了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作
- 具备检查系统运行性能的专业技术和工具
- 具备独立审计的精神

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

8.3 评估者与被评估者之间的关系

1、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。

2、外部评估者(信息产业主管部门、独立审计师事务所以及其他机构)和 GDCA 之间是独立的关系，没有任何的业务、财务往来，或者其它任何利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对 GDCA 进行评估。

8.4 评估内容

GDCA 中心的审计工作包括以下内容：

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 CPS、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。

第三方审计师事务所按照 WebTrust For CA 规范的要求，对 GDCA 进行独立审计。

8.5 对问题与不足采取的措施

对于本机构审计结果中的问题，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，各职能部门需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 CPS 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。

第三方审计师事务所评估完成后，GDCA 按照其工作报告进行整改，并接受再次审计和评估。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

8.6 评估结果的传达与发布

GDCA 的审计结果向本机构各职能部门以及审计涉及的证书注册机构进行正式通报，对可能造成订户安全隐患，GDCA 将及时向订户通报。

第三方审计师事务所评估完成后，对于审计的结果，将通过 www.gdca.com.cn 网站进行公布。任何第三方向被评估实体通知评估结果或者类似的信息，都必须事先明确向 GDCA 表明通知的目的和方式，并征得 GDCA 的同意，法律另有规定的除外；GDCA 保留在这方面的法律权力。

8.7 其他评估

无规定。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

九、 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新

GDCA 可根据提供的电子认证相关服务向本机构的证书订户收取费用，具体收费标准根据国家有关物价管理部门的批复文件执行，现阶段广东省电子认证服务收费标准由广东省物价局批准订立。在收费标准范围内，即不超过收费标准的情况下，GDCA 有权根据市场状况，针对不同订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。

9.1.2 证书查询费用

在证书有效期内，对该证书信息进行查询，目前 GDCA 不收取查询费用。除非用户提出的特殊需求，需要 GDCA 支付额外的费用，GDCA 将与用户协商收取应该收取的费用。

如果证书查询的收费政策有任何变化，GDCA 将会及时在网站 www.gdca.com.cn 上予以公布。

9.1.3 证书吊销或状态信息的查询费用

GDCA 对于证书吊销和状态查询，目前不收取任何费用。除非用户提出的特殊需求，需要 GDCA 支付额外的费用，GDCA 将与用户协商收取应该收取的费用。

如果吊销和状态信息查询的收费政策有任何变化，GDCA 将会及时在网站 www.gdca.com.cn 上予以公布。

9.1.4 其他服务费用

1、如果用户向 GDCA 索取纸质的 CPS 或其他相关的作业文件时，GDCA 需要收取因此产生的邮递和处理工本费。

2、GDCA 将向用户提供证书存储介质及相关服务，GDCA 在与订户或者其他实

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

体签署的协议中指明该项价格。

3、其他 GDCA 将要或者可能提供的服务的费用，GDCA 将会及时公布，供用户查询。

9.1.5 退款策略

GDCA 对订户收取的费用，除了证书申请和更新费用因为特定理由可以退还外，GDCA 均不退还用户任何费用。

在实施证书操作和签发证书的过程中，GDCA 遵守严格的操作程序和策略。如果 GDCA 违背了本 CPS 所规定的责任或其它重大义务，订户可以要求 GDCA 吊销证书并退款。在 GDCA 吊销了订户的证书后，GDCA 将立即把订户为申请该证书所支付的费用全额退还给订户。

此退款策略不限制订户得到其它的赔偿。

完成退款后，订户如果继续使用该证书，GDCA 将追究其法律责任。

9.2 财务责任

9.2.1 保险范围

出现下列情形并经 GDCA 确认后，证书订户、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订户以外的第三方，导致订户或者依赖方遭受损失的；
- 订户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 未按鉴证要求对订户证书申请信息进行审核而签发了数字证书，导致订户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，致使订户或者依赖方遭受损失的；
- GDCA 未能及时吊销证书的。

9.2.2 其他资产

无规定。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

9.2.3 对最终实体的保险或担保

GDCA 如违反了本 CPS 中规定的职责，证书订户、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 9.2.1 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。

9.2.4 责任免除

有下列情形之一的，应当免除 GDCA 之责任：

1. 订户在申请和使用 GDCA 数字证书时，有违反如下义务之一的：

1） 订户有义务提供真实、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） 订户应当妥善保管 GDCA 所签发的数字证书载体和保护 PIN 码，不得泄漏 PIN 码或将数字证书载体随意交付他人；

3） 订户在应用自己的密钥或使用数字证书时，应当使用可依赖、安全的系统；

4） 订户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） 订户在使用数字证书时必须遵守国家的法律、法规和行政规章制度。不得将数字证书作为 GDCA 规定使用范围外的其他任何用途使用；

6） 订户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、被吊销的数字证书；

7） 订户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数字证书签发错误、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：

◆ 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

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

水、海啸、台风等自然现象；

- ◆ 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数字证书签发错误、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、法规规定的数字证书认证业务规则，而仍有损失产生的。

在粤港互认项目，有以下情形的应当免粤港两地政府和电子认证服务主管部门的责任：

在遵守相关法律监管要求和《粤港电子签名证书互认证书策略》的基础上，应用在粤港互认和电子认证服务主管部门的证书以及相关行为，任何由于 GDCA 或相关证书的不足或疏忽所引起的责任和索偿，GDCA、订户和依赖方对粤港两地政府免责。

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：

- ◆ GDCA 订户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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

9.3.2 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、CPS 识别的证书策略中的信息。
- GDCA 许可，只有 GDCA 订户方使用，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。

9.3.3 保护保密信息的责任

GDCA 有妥善保管与保护本节 9.3.1 中规定的保密信息的责任与义务。

9.4 个人隐私保密

9.4.1 隐私保密方案

GDCA 尊重证书订户个人资料的隐私权，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。

9.4.2 作为隐私处理的信息

GDCA 定义以下信息为证书订户的隐私信息：

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

9.4.3 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订户的隐私信息：

- 订户姓名、单位名称等。
- 订户性别、单位性质等。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

- 订户通信地址的邮政编码。
- 订户的电子邮箱。

9.4.4 保护隐私的责任

GDCA 有妥善保管与保护本节 9.4.2 中规定的证书申请者个人隐私的责任与义务。

9.4.5 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订户的个人隐私，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，在未得到证书订户的许可之前,GDCA 保证不会把证书订户的除写入数字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）。

9.4.6 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：

- 订户的基本信息。
- 订户用个人加密密钥加密的信息。
- 订户对 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。

9.4.7 其他信息披露情形

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

9.5 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 对数字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。

9.6 陈述与担保

9.6.1 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 签发给订户的证书符合 GDCA 的 CPS 的所有实质性要求。
- 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 将及时吊销证书。
- 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。

证书公开发布后，GDCA 保证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。

GDCA 不负责评估证书是否在适当的范围内使用，订户和依赖方依照订户协议和依赖方协议确保证书用于允许使用的目的。

9.6.2 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：

- 提供给证书订户的注册过程完全符合 GDCA 的 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 CPS 的规定，及时向 GDCA 提交吊销、更新等服务申请。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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、注册机构及信赖证书的有关当事人作出以下承诺：

- 已知悉和接受 GDCA 的“数字证书申请责任书”和本 CPS 中的所有条款和条件。
- 在证书的有效期内进行数字签名。
- 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，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，那么订户和代理人两者负有连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知 GDCA 或其授权的证书服务机构。
- 与订户证书所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并且在进行签名时，证书是有效证书（证书没有过期、吊销），证书的私钥为订户本身访问和使用。
- 除非经订户和发证机构间书面协议明确规定，订户保证不从事发证机构（或类似机构）所从事的业务。
- 一经接受证书，既表示订户知悉和接受本 CPS 中的所有条款和条件，并知悉和接受相应的订户协议；
- 一经接受证书，订户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 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。

9.6.4 依赖方的陈述与担保

- 遵守本 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。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

- 在信赖证书前，通过查询 CRL 或 OCSP 确认证书是否被吊销。
- 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。

9.6.5 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 CPS 的所有规定。

9.7 担保免责

除本 CPS 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：

- 不保证证书订户、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。
- 订户违反本 CPS 9.6.3 之承诺时，或依赖方违反本 CPS 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 将承担不超过本 CPS 9.9 规定的有限赔偿责任。

9.9 赔偿

9.9.1 GDCA 的赔偿责任

如 GDCA 违反了本 CPS 9.6.1 中的陈述，证书订户、依赖方等实体可以申请 GDCA

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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、泄露，导致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。

另外，GDCA 赔偿限制如下：

1. GDCA 所有的赔偿义务不得高于本 CPS9.2.1，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. 对于由订户或依赖方的原因造成的损失，GDCA 不承担责任，由订户或依赖方自行承担。
3. GDCA 只有在证书有效期限内承担损失赔偿责任。

9.9.2 订户的赔偿责任

如因下述情形而导致 GDCA 或依赖方遭受损失，订户应当承担赔偿责任：

1. 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致造成 GDCA 及其授权的证书服务机构或者第三方遭受损害；
2. 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知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. 订户使用证书的行为，有违反本 CPS 及相关操作规范，或者将证书用于非本 CPS 规定的业务范围；
4. 证书订户或者其它有权提出吊销证书的实体提出吊销请求后，到GDCA将该证书吊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 CPS 的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任；

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

5. 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；
6. 没有对私钥采取有效的保护措施，导致私钥丢失或被损害、窃取、泄露等；
7. 在得知私钥丢失或存在危险时，未停止使用证书并及时通知GDCA和依赖方；
8. 证书到期但仍在使用证书；
9. 订户的证书信息侵犯了第三方的知识产权；
10. 在规定的范围外使用证书，如从事违法犯罪活动；

9.9.3 依赖方的赔偿责任

如因下述情形而导致 GDCA 或订户遭受损失，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 CPS 中规定的义务；
2. 未能依照本 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 确认证书是否被吊销。

9.10 有效期限与终止

9.10.1 有效期限

本 CPS 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

在 GDCA 终止电子认证服务时，本 CPS 终止。

9.10.3 效力的终止与保留

本 CPS 终止后，其效力将同时终止，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，CPS 中对各方责任的规定及责任免除仍然适用。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

9.11 对参与者的个别通告与沟通

本 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。

9.12 修订

9.12.1 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 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 CP 的要求，符合认证业务开展的实际需要。

本 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 CPS 经过 GDCA 安全策略委员会批准后正式对外发布。

9.12.2 通知机制和期限

修订后的新版 CPS，GDCA 将通过网站方式予以公布。新版 CPS 将在自公布之日起的 15 天后生效。

9.12.3 必须修改业务规则的情形

GDCA 必须对本 CPS 进行修改的情形包括：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。

9.13 争议处理

GDCA、证书订户、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：

- 根据本 CPS 中的规定，明确责任方；
- 由 GDCA 相关部门负责与申请人协调；
- 若协调失败，再由有关法律部门进行裁决。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

- 任何与 GDCA 或授权机构就本 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。

9.14 管辖法律

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

9.15 与适用法律的符合性

无论 GDCA 的证书订户、依赖方等实体在何地居住以及在何处使用 GDCA 的证书，本 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 CPS 所涉及的任何争议，均适应中华人民共和国法律。

9.16 一般条款

9.16.1 完整协议

GDCA 的 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。

9.16.2 转让

GDCA 声明，根据本 CPS 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 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，那么本 CPS 其余的部分为可独立于这一条款而继续执行。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

9.16.4 强制执行

GDCA 声明，若证书订户、依赖方等实体未执行 GDCA 的 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。

9.16.5 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 CPS 规定担保责任的违反、延误或无法履行负责。

9.17 其他条款

GDCA 对本 CPS 具有最终解释权。

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

附录 1：证书信息

GDCA TrustAUTH R5 ROOT 证书的根密钥长度为 4096-bit，下设三个子 CA 证书，分别为（1）GDCA TrustAUTH R4 SSL CA 证书，（2）GDCA TrustAUTH R4 Generic CA 证书（3）GDCA TrustAUTH R4 CodeSigning 证书，子 CA 证书的密钥长度为 2048-bit。

1、GDCA TrustAUTH R5 ROOT

国家=CN

组织= GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.

通用名= GDCA TrustAUTH R5 ROOT

序列号= 7d 09 97 fe f0 47 ea 7a

有效期：2014年11 月26日到 2040年12月31日

SHA1 摘要= 0f 36 38 5b 81 1a 25 c3 9b 31 4e 83 ca e9 34 66 70 cc 74 b4

2、GDCA TrustAUTH R4 SSL CA

国家=CN

组织= GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.

通用名= GDCA TrustAUTH R4 SSL CA

序列号= 64 0c 3b 33 de 07 3c 61

有效期：2014年11月 26 日到 2030年12月31日

SHA1 摘要= f0 2b cb 1e 1e 56 56 73 59 80 c1 53 df 0d 43 62 92 4f 4c 10

3、GDCA TrustAUTH R4 Generic CA

国家=CN

组织= GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.

通用名= GDCA TrustAUTH R4 Generic CA

序列号= 71 22 98 3b b4 f8 69 62

有效期：2014年11月 26 日到 2030年12月31日

SHA1 摘要= 08 ef 1f 76 9a d6 10 ac a6 14 70 dd db 35 c5 d0 25 15 9d b5

4、GDCA TrustAUTH R4 CodeSigning CA

国家=CN

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

组织= GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.

通用名= GDCA TrustAUTH R4 CodeSigning CA

序列号= 26 87 dc ff e0 ef 26 7a

有效期：2014年11月 26 日到 2030年12月31日

SHA1 摘要= b0 5c 15 74 ab 17 c5 5f 15 fc 1e 42 21 dd f9 27 76 54 47 bb

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

附录 2：GDCA 电子认证业务规则修订记录表

内容 / 序号	项目	4.0 版	4.1 版
一	$1.1.2 电子认证业务规则（CPS）	证书是否应用于粤港跨境互认项目可根据证书策略的对象标识符进行判断。	证书是否应用于粤港跨境互认项目可根据证书策略的对象标识符进行辨别。
二	$1.1.3GDCA 证书层次架构	国密局签发 RSA2048-bit CA 证书，签发密钥长度为 2048-bit 的个人类证书、机构类证书、设备类证书和其他类证书。 国密局签发的 RSA2048-bit CA 证书将于 2018 年 12 月 15 日到期，2015 年 1 月 1 日起，GDCA 将不再使用该 CA 证书签发订户证书。	国密局签发 RSA2048-bit CA 证书，签发密钥长度为 2048-bit 和 1024-bit 的个人类证书、机构类证书、设备类证书和其他类证书。 国密局签发的 RSA2048-bit CA 证书将于 2018 年 12 月 15 日到期，2016 年 12 月 15 日起，GDCA 将不再使用该 CA 证书签发订户证书。
三	$1.2 文档名称与标识		删除：本 CPS 的对象标识符（OID）与《广东数字证书认证中心有限 公司证书策略》（简称《GDCA CP》）中的对象标识符一致。
四	$1.4.1.6 各类证书的证书策略对象标识符		增加本节
五	$3.2.2 机构身份的鉴别		增加：对于粤港跨境互认的证书，必须以面对面审核的方式确认授权代表身份，通过法定的身份证明文件(包括但不限于个人身份证、护照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)，确认授权代表的真实身份。
六	$3.2.3 机构身份的鉴别		增加：对于粤港跨境互认的证书，必须以面对面审核的方式确认申请者个人身份，通过法定的身份证明文件(包括但不限于个人身份证、护照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)，确认授权代表的真实身份。
七	$6.1.1.1 签名密钥对生成	订户签名密钥对的产生，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，对于第 1 类个人证书、第 1 类机构证书和代码签名类证书，可以使用硬件密码模块	订户签名密钥对的产生，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，对于第 1 类个人证书和第 1 类机构证书，可以使用硬件密码模块（如：USB Key），

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

		（如：USB Key），也可以使用标准的软件密码模块(如：浏览器自带的密码模块，Web 服务器软件提供的密钥生成功能等)，证书申请者可根据其需要进行选择。对于第 2 类个人证书、第 2 类机构证书、设备证书和 SSL 服务器类证书，则必须使用硬件密码模块生成密钥。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。	也可以使用标准的软件密码模块(如：浏览器自带的密码模块，Web 服务器软件提供的密钥生成功能等)，证书申请者可根据其需要进行选择。对于第 2 类个人证书、第 2 类机构证书和设备证书，则必须使用硬件密码模块生成密钥。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。
八	$6.1.1.2 加密密钥对生成		增加：对于 GDCA TrustAUTH R4 SSL CA 及 GDCA TrustAUTH R4 CodeSigning CA 证书签发的订户证书，订户密钥对由订户自身的服务器或其它设备内置的密钥生成机制生成，GDCA 不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。
九	$6.1.2 加密私钥传送给订户		增加：对于 GDCA TrustAUTH R4 SSL CA 及 GDCA TrustAUTH R4 CodeSigning CA 证书签发的订户证书，私钥由订户自行生成，GDCA 不需要将私钥传递给订户。
十	$6.1.3 公钥传送给证书签发机构		增加：对于 GDCA TrustAUTH R4 SSL CA 及 GDCA TrustAUTH R4 CodeSigning CA 证书签发的订户证书，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。
十一	$6.3.2 订户托管密钥归档和销毁		增加：订户托管密钥归档和销毁：无规定。
十二	$7.1.6 证书策略对象标识符		增加本节。
十三	$9.12.1 修订程序		第一段增加：“符合 CP 的要求”描述

地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813