
# 广东数字证书认证中心有限公司

# EV 证书电子认证业务规则

版本：V1.1　　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：510010 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：510010 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：510010 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：510010 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：510010 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：510010 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：510010 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 EV CPS）描述了 GDCA 签发 EV 证书时所遵循的程序，符合 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)发布的扩展验证证书指南(Guidelines for Extended Validation Certificates）的要求。

本 CPS 适用于 GDCA 的 EV ROOT CA、EV SSL CA、EV CodeSigning CA，以及相关用户、订户、依赖方等实体。本 CPS 作为一个单独的文件，涵盖了签发和管理 EV 证书相关的具体操作和流程。

按照本 CPS 签发的 EV 证书，其对象是向 GDCA 申请并通过所有相关身份鉴别的各类机构。

所有 GDCA EV 证书的订户及依赖方必须参照本 CPS 及相应 CP 的规定，决定对证书的使用和信任。

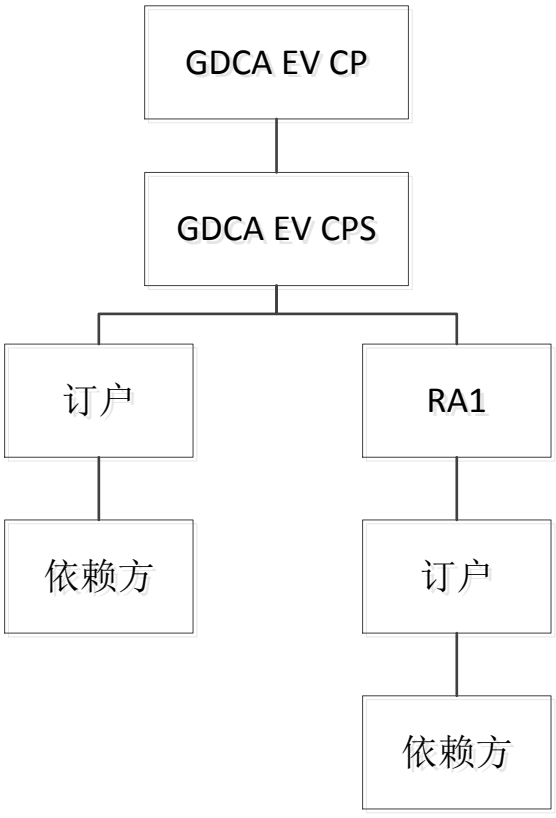
GDCA 遵循 WebTrust 国际标准（Trust Service Principles and Criteria for


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

Certification Authorities）及 CA/浏览器论坛（CA/Browser Forum）发布的扩展验证证书签发和管理指南（Guidelines for the Issuance And Management of Extended Validation Certificates）、扩展验证代码签名证书签发和管理指南（Guidelines for the Issuance And Management of Extended Validation Code Signing Certificates）的最新版本要求进行签发和管理 EV 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。

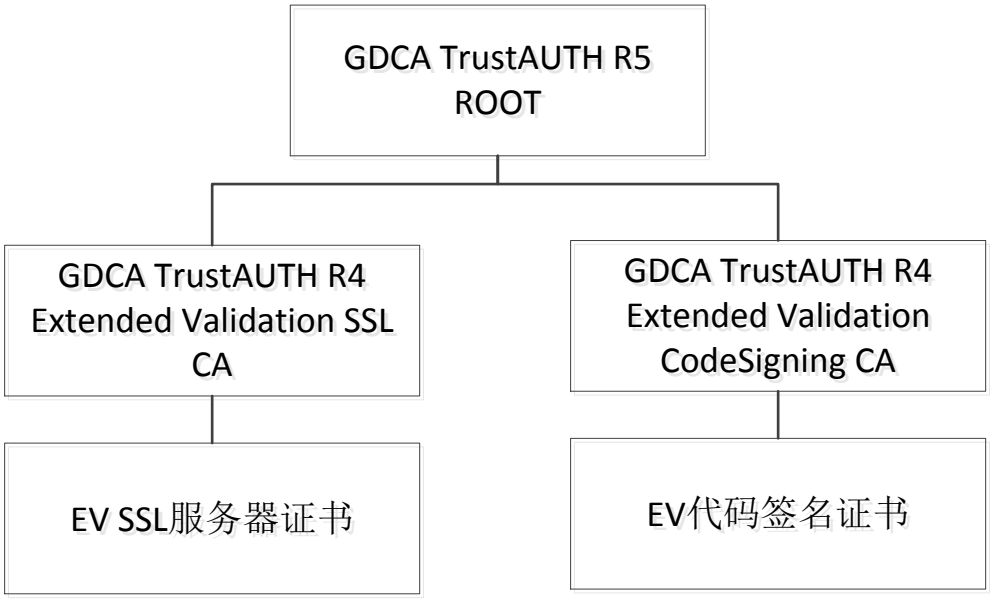
## 1.2 GDCA 架构

本 CPS 按照 GDCA EV CP 制定，GDCA 按照本 CPS 进行证书服务申请鉴别，订户、依赖方及其他相关实体按照本 CPS 及 EV CP 决定对证书的使用、信任并履行相关的义务。




### 1.2.1 GDCA EV 证书层次架构


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813




GDCA 有 1 个 EV 根证书 GDCA TrustAUTH R5 ROOT，其密钥长度为 4096-bit，下设 2 个子 CA 证书，其中：（1）GDCA TrustAUTH R4 Extended Validation SSL CA 证书，签发密钥长度为 2048-bit 的 EV SSL 服务器证书；（2）GDCA TrustAUTH R4 Extended Validation CodeSigning CA 证书，签发密钥长度为 2048-bit 的 EV 代码签名证书。

## 1.3 文档名称与标识

本文档称作《广东数字证书认证中心有限公司 EV 证书认证业务规则》（简称《GDCA EV CPS》）。

本 CPS 的对象标识符（OID）与《广东数字证书认证中心有限公司 EV 证书策略》（简称《GDCA EV CP》）中的对象标识符一致。

## 1.4 电子认证活动参与者

### 1.4.1 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 EV 数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 1.4.2 注册机构

注册机构（Registration Authority，简称 RA）代表 CA 建立起注册过程，确认 EV 证书申请者的身份，批准或拒绝 EV 证书申请者。

GDCA 作为 EV 证书的 CA 运营机构，自行担任 EV 证书 RA，不再另行设立 RA。

### 1.4.3 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。

本 CPS 中出现的订户，均指各类机构。GDCA 只对各类机构发放 EV 证书，不向自然人提供 EV 证书服务。

### 1.4.4 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。

### 1.4.5 其他参与者

其他参与者是指为 GDCA 的电子认证活动提供相关服务的其他实体。

## 1.5 证书应用

### 1.5.1 适合的证书应用

GDCA 签发的 EV 证书主要用于身份识别。

依据本 CPS 签发的 EV SSL 证书，可用来验证证书中标识的域名的身份，以及持有该域名的法人机构身份；依据本 CPS 签发的 EV CodeSigning 证书，可用来验证证书中标识的软件代码提供方或发布方的身份。凡是经过验证后确定是由 GDCA 签发的 EV 证书，均表明该证书中所包含的信息真实有效，并且已经通过了适当且可靠的身份鉴别程序。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

#### 1.5.1.1 EV SSL 服务器证书

EV SSL 服务器证书用于验证证书中标识的网络主机服务器或互联网域名的身份，以及持有该网络服务器或互联网域名的法人机构身份。GDCA 不签发通配符 SSL 服务器证书。

#### 1.5.1.2 EV 代码签名证书

EV 代码签名证书用于验证证书中标识的软件代码提供方或发布方的身份。

### 1.5.2 限制的证书应用

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

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

## 1.6 策略管理

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。

### 1.6.1 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 1.6.2 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

### 1.6.3 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。

### 1.6.4 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》的规定，从对外发布之日起的三十日之内向工业和信息化部备案。

### 1.6.5 CPS 修订

GDCA 根据国家的政策法规、技术要求、业务发展情况以及 CA/浏览器论坛（CA/Browser Forum）发布的扩展验证证书指南（Guidelines for Extended Validation Certificates）的最新要求及时修订本 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。

## 1.7 定义和缩写

### 1.7.1 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 |


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

| | |
|---|---|
| | 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。 |

### 1.7.2 缩略语及其含义一览表

| | | |
|---|---|---|
| GDCA | Guang Dong Certificate Authority | 广东省数字证书认证中心 |
| CA | Certificate Authority | 电子认证服务机构 |
| KM | Key Management Center | 密钥管理中心 |
| RA | Registration Authority | 注册审核服务机构 |
| LRA | Local Registration Authority | 本地注册受理点 |
| LDAP | Lightweight Directory Access Protocol | 轻型目录访问协议 |
| CPS | Certification Practice Statement | 电子认证业务规则 |
| CRL | Certificate Rovoke List | 证书撤消列表 |


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

| | | |
|---|---|---|
| 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：510010 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：510010 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：510010　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 签发的 EV 数字证书符合 X.509 标准，分配给证书持有者的主体甄别名，采用 X.500 命名方式。

EV SSL 证书和 EV 代码签名证书命名规则和要求必须被记录在按照 CP 制定的本 CPS 中，并且符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第九部分的要求。EV SSL 证书和 EV 代码签名证书的甄别名必须包含通用名（common name，CN=）内容，经过验证的通用名中应当包含域名、机构电子邮件地址、机构的合法名称等。

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： |


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

| | |
|---|---|
| | ● 对于有确定机构的订户，是订户所在机构名称；<br>● 对于没有确定机构的订户，是 GDCA。 |
| 机构部门（OU） | 可以包含以下一个或多个内容：<br>● 订户所在机构的具体部门；<br>● 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 |

EV Root 证书甄别名命名规则

| 属性 | 值 |
|---|---|
| 国家（C） | CN |
| 机构（O） | GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. |
| 通用名（CN） | GDCA TrustAUTH R5 ROOT |

EV SSL CA 证书甄别名命名规则

| 属性 | 值 |
|---|---|
| 国家（C） | CN |
| 机构（O） | GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. |
| 通用名（CN） | GDCA TrustAUTH R4 Extended Validation SSL CA |

EV CodeSigning CA 证书甄别名命名规则

| 属性 | 值 |
|---|---|
| 国家（C） | CN |
| 机构（O） | GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. |
| 通用名（CN） | GDCA TrustAUTH R4 Extended Validation CodeSigning CA |


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 3.1.2 对名称意义化的要求

订户证书所包含的命名应具有一定的代表性意义。订户证书中包含的主体识别名称，应当能够明确确定证书持有机构以及所要标识的网络主机服务器、互联网域名或软件发布者的身份，并且可以被依赖方识别。主体识别名称应当符合法律法规等相关规定的要求。

### 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。

## 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）


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

等。

### 3.2.2 机构身份的鉴别

GDCA 仅向机构用户提供 EV 证书申请服务，机构在申请证书时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、主管人、经办人有效身份证件的原件和复印件以及其他证明文件。

对机构身份的鉴别和审核符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南的要求。同时，当证书申请中包含国际化域名（internationalized domain names，IDNs）时，GDCA 对域名持有人的身份进行验证以检测是否存在 IDNs 的同形异义欺骗（homographic spoofing）行为。

#### 3.2.2.1鉴别要求

EV 证书只面向政府机关、企业单位、事业单位、社会团体以及其他机构提供，对于申请人必须进行以下鉴别和验证：

1. 必须依法存在
2. 证书申请人和与合法注册的机构名称一致
3. 证书申请经办人必须获得机构授权

#### 3.2.2.1鉴别方法

1. 机构身份确认

（1） 验证组织机构代码证、工商营业执照、社会团体登记证、事业单位登记证等相关证明文件

（2） 通过查询第三方数据库等方式验证机构名称、注册信息等与申请人提交的信息是否一致

（3） 验证机构经营地址或经营场所

（4） 验证电话号码等机构联系方式

2. 证书申请经办人身份确认

（1） 验证经办人身份证、护照等个人身份证明材料

（2） 验证银行卡、电话账单等证明材料


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

（3） 验证经办人的授权办理证明文件

（4） 通过电话、邮件等方式与机构人事部门联系，确认相关人员身份及授权

3. 域名确认

通过万网“Whois”查询方式验证域名持有人信息。

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

EV证书不接受个人申请。

### 3.2.4 没有验证的订户信息

EV 证书中所有包含的订户信息都应进行验证。

### 3.2.5 授权确认

当机构订户授权经办人办理证书业务时，应当进行如下验证：

1. 通过第三方身份证明服务或数据库、提交政府主管部门签发的文件等方式确认该机构存在；

2. 通过电话、有回执的邮政信函、雇佣证明或任何同等方式来验证该人属于上述机构以及其代表行为被该机构授权。

### 3.2.6 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

## 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

对于常规情况下的密钥更新，在 EV 证书到期前，订户应重新按照 CPS § 3.2 关于证明私钥拥有方法的规定提交证书申请。

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

EV 证书吊销后不能进行密钥更新。

## 3.4 吊销请求的标识与鉴别

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 节描述进行身份鉴别。

## 3.5 授权服务机构的标识和鉴别

GDCA 自行担任 EV 证书的 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：510010 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

## 4.1 证书申请

### 4.1.1 证书申请实体

证书申请实体是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

EV 证书注册操作符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南的要求。

申请者应事先了解订户协议、CP 及本 CPS 等文件约定的事项，特别是其中关于证书适用范围、权利、义务和担保的相关内容。

申请者应向 GDCA 递交 EV 证书申请表及相应证明文件，此行为即意味着申请者已经了解和接受上述内容。

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。

GDCA 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。

## 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 验证申请者提交的申请材料后，根据验证结果决定接受、拒绝该申请或要求申请者补充递交相关材料。

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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 4.2.2 证书申请批准和拒绝

完成 4.2.1 识别与鉴别的执行后，如果用户满足相应要求，则视为 GDCA 已经批准该证书请求，申请者即成为 GDCA 的 EV 证书订户；否则应拒绝证书申请。

如果法律法规明确禁止某个申请，或 GDCA 认为批准该申请具有高风险性，GDCA 应拒绝该申请，GDCA 根据反钓鱼联盟、防病毒厂商或相关联盟、负责网络安全事务的政府机构等第三方发布的名单，或公共媒体公开报道中披露的信息，建立和维护 EV 证书高风险申请人列表，在接受证书申请时将会查询该列表信息。对于列表中出现的申请人，GDCA 将直接拒绝其申请。

对于已签发的 EV 证书，也将会定期根据列表予以复核，一旦发现证书持有人出现在列表中，GDCA 有权撤销该证书或采取适当机制进行谨慎处理。

对于法律法规、国家政府部门、行业监管部门或当地政府明确禁止从事商业活动或其它公开活动的机构，GDCA 有权拒绝为其签发 EV 证书。此外，如果证书申请相关人员受到法律法规、国家或地方政府的相关限制，GDCA 可不予受理由其参与的 EV 证书申请事宜。

#### 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，GDCA 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；


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

#### 4.2.3 处理证书申请的时间

GDCA 应在合理的期限内完成证书申请处理。

## 4.3 证书签发

#### 4.3.1 电子认证服务机构（CA）的行为

CA 将在证书申请被批准后生成并签发证书。CA 为申请人生成和签发的证书基于其在证书申请中被批准的信息。签发证书的操作符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 12 部分的要求。

#### 4.3.2 CA 通知订户证书的签发

GDCA 的证书签发系统签发证书后，将通知订户证书已被签发，并向订户提供可以获得证书的方式，可通过面对面、网络下载等方式，或者通过其它与订户约定的方式告知订户如何获得证书。

## 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，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、订户反对证书或者证书内容的操作失败。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

#### 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 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。

订户应保护其私钥避免未经授权的使用，并且不再使用过期或被撤销的证书。私钥不得进行归档。

对于 EV 代码签名证书，不存在一个证书对应多个软件对象。

#### 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

当依赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密。依赖方应将加密证书连同加密信息一起发送给接受方。

## 4.6 证书更新

### 4.6.1 证书更新的情形

GDCA 不提供 EV 证书更新服务。

### 4.6.2 请求证书更新的实体

不适用。

### 4.6.3 证书更新请求的处理

不适用。

### 4.6.4 颁发新证书时对订户的通告

不适用。

### 4.6.5 构成接受更新证书的行为

不适用。

### 4.6.6 电子认证服务机构对更新证书的发布

不适用。

### 4.6.7 电子认证服务机构对其他实体的通告

不适用。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

## 4.7 证书密钥更新

### 4.7.1 证书密钥更新的情形

GDCA 的证书密钥更新包括但不限于以下情形：

1） 证书到期。

2） 证书密钥到期。

3） 基于技术、政策安全原因，GDCA 要求证书密钥更新。

### 4.7.2 请求证书密钥更新的实体

请求证书密钥更新的实体为证书订户。

### 4.7.3 证书密钥更新请求的处理

参照 CPS § 3.3 的规定对证书密钥更新进行用户身份鉴别和识别。

参照 CPS § 4.3 的规定对证书进行签发。

### 4.7.4 颁发新证书时对订户的通告

同本 CPS § 4.3.2。

### 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

同本 CPS § 4.4.2。

### 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

## 4.8 证书变更

GDCA 不提供EV 证书变更服务，如证书中包含的信息发生变更时应按照本CPS §4.9 的规定吊销该证书，订户应按照本 CP §4.1、§4.2、§4.3、§4.4 的规定重新申请签发证书。

### 4.8.1 证书变更的情形

不适用。

### 4.8.2 请求证书变更的实体

不适用。

### 4.8.3 证书变更请求的处理

不适用。

### 4.8.4 颁发新证书时对订户的通告

不适用。

### 4.8.5 构成接受变更证书的行为

不适用。

### 4.8.6 电子认证服务机构对变更证书的发布

不适用。

### 4.8.7 电子认证服务机构对其他实体的通告

不适用。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

## 4.9 证书吊销和挂起

证书撤销和状态查询操作符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 13 部分的要求。

### 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) 订户违反了本 CPS 规定的重要职责；
3) 订户主动提出吊销请求；
4) GDCA 发现订户在申请时提供的证明材料不真实；
5) 订户未能履行订户协议中应尽的责任，如订户未按期缴纳证书服务费；
6) 订户 EV SSL 证书里的信息做了实质性的更改；
7) 证书申请是未得到授权或不能追溯到授权行为；
8) GDCA 终止营运并且尚未安排另外的 EV 证书签发机构来提供 EV 证书的撤销支持服务；或者 GDCA 不再具备签发 EV SSL 证书的权利或资质；
9) 继续使用证书将会对 GDCA 产生损害；
10) GDCA EV 根证书或 EV 子 CA 证书相对应的私钥出现安全风险，或 GDCA 不再具备签发 EV 证书的权利或资质，或 GDCA 发现签发证书时未遵循 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南的要求或 GDCA 的 EV 证书政策；
11) 由于技术或标准演变可能导致依赖方或应用软件提供方产生不可能接受的风险；
12) 司法机构的判决导致证书可信度被削弱或被无法被信任，或法律法规直接或间接的规定和要求；
13) 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 4.9.2 请求证书吊销的实体

请求证书吊销实体为订户、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) 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；
2) 订户向 GDCA 提交吊销申请表和身份证明材料，同时说明吊销原因；
3) GDCA 按照本 CP § 3.4 的规定进行证书吊销请求的鉴别；
4) 鉴别完成后，GDCA 在 24 小时内对吊销请求进行调查；
5) GDCA 在接到吊销请求后的 2 个工作日内完成证书吊销；
6) GDCA 完成吊销后及时将其发布到证书吊销列表；
7) GDCA 通过电话、邮件、传真等适当方式，通知订户证书被吊销及被吊销的理由。

#### 4.9.3.2 订户被强制吊销证书

1) 当 GDCA 有充分的理由确信出现本 CPS §4.9.1 中的情况时，须经过 GDCA 安全策略委员会批准后方可进行；
2) 在 GDCA EV Root 证书或 EV 子 CA 证书相对应的私钥出现安全风险时，经国家电子认证服务主管部门批准后可直接进行证书撤销；
3) 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。

GDCA 提供 7*24 小时的 EV 证书问题报告和处理机制。

#### 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 4.9.4 问题和报告处理机制

订户应在证书对应的私钥出现或疑似泄漏、被破解或被滥用时，应立即告知 GDCA，最长不超过 24 小时。GDCA 在接到订户报告后应在 24 小时内，对已经接受报告的证书进行调查和决定是否撤销或采取其他适当的行动处理机制。

GDCA 建立并保持 7*24 小时的 EV 证书问题报告和受理机制，任何订户、依赖方、应用软件供应商或其他第三方发现证书可能存在问题、私钥出现或怀疑出现泄漏、证书滥用、或其他与 EV 证书相关的舞弊、泄漏、滥用或不正当行为时，均可向 GDCA 进行报告或投诉。报告方式如下：

- 电话号码：020-83487228
- 传真号码：020-83486610
- E-mail:report@gdca.com.cn

在接受报告或投诉后，GDCA 在 24 小时内对已经接受报告的证书进行鉴别和调查，并根据调查结果决定是否采取撤销或其他适当的方式进行处理。鉴别和调查主要包括但不限于以下内容：

1) 报告人的身份识别
2) 问题的性质和产生原因
3) 相应问题的出现次数和频率
4) 证书签发等相关业务流程的重新审视及认定结果
5) CP/CPS 和订户协议等相关规范的遵循
6) 有关法律法规的遵循

### 4.9.5 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。

### 4.9.6 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 4.9.7 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。

### 4.9.8 CRL 发布频率

GDCA 须定时发布最新的证书吊销列表。对于订户证书，证书吊销列表更新的时间间隔不能超过 24 小时。对于子 CA 证书，至少每 3 个月签发和公布一次，对于根 CA 证书，必须每年公布一次。

CRL 签发频率符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第 13 部分的要求。

### 4.9.9 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。

### 4.9.10 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（OCSP）。OCSP 的可用性符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 13 部分的要求。

### 4.9.11 在线状态查询要求

对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，依赖方在依赖一个证书前必须通过证书状态在线查询检查该证书的状态。

### 4.9.12 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。

### 4.9.13 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。如果 CA 的密钥（根 CA 或子


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

CA 密钥）安全被损害或者怀疑被损害，应该在合理的时间内用合式的方式及时通知订户和依赖方。

#### 4.9.14 证书挂起的情形

不适用。

#### 4.9.15 请求证书挂起的实体

不适用。

#### 4.9.16 挂起请求的流程

不适用。

#### 4.9.17 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。

#### 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。

证书状态服务的可用性符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第 13 部分的要求。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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） 证书到期后没有进行更新；

2） 证书到期前被吊销。

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 密钥托管与恢复

4.12.1 密钥托管与恢复的策略与行为

GDCA 不得托管任何 EV 证书订户的私钥，因此也不提供密钥恢复服务。

4.12.2 会话密钥的封装与恢复的策略和行为

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：510010 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：510010 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：510010 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：510010 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：510010 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

人员控制符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 14.1 部分的要求。

### 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

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。根据考察的结果作出相应的安排。

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；


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

- 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等。

此外，对于证书操作员和审核员，GDCA 定期开展工作职责所需要的培训，包括岗位职责、事件和损坏的报告处理流程、灾难恢复和业务连续性管理流程等。在新系统上线或认证系统的重要更新或升级时，对操作人员和审核人员也需进行相应的培训。

### 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

司法机构处理等措施。

### 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

GDCA 有权决定是否对导致事件的实体进行通告。

#### 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

## 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

划和措施，每季度进行数据灾难恢复演练。

### 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

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。

业务连续性的实施符合和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16 部分的要求。

在发生自然灾害或其他灾变，以致于无法在 24 小时内恢复证书状态服务时，将启用异地备份机房的设施，并于启用后 24 小时内恢复提供证书状态服务。

## 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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. 处理和存储敏感文档；
12. 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。

## 5.10 数据安全

数据安全符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16 部分的要求。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 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

CA 密钥对由国家密码主管部门批准和许可的设备生成的。密钥的生成、管理、存储、备份和恢复应遵循 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 FIPS140-2 标准仅参照执行，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。

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。

### 6.1.2 私钥传送给订户

私钥由订户自行生成，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

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

CA 和最终订户密钥对至少是 2048 位 RSA。

密钥长度符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.5 部分的要求。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 6.1.6 公钥参数的生成和质量检查

公钥参数必须使用国家密码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。

### 6.1.7 密钥使用目的

GDCA 签发的 X.509v3 证书包含了密钥用法扩展项，其用法与 RFC 5280 标准 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002) 相符。如果 GDCA 在其签发证书的密钥用法扩展项内指明了用途，证书订户必须按照该指明的用途使用密钥。

## 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 6.2.3 私钥托管

GDCA 的私钥不允许托管，也不向订户提供私钥托管服务。

### 6.2.4 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。

### 6.2.5 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。

密钥到期后，GDCA 在 10 天内完成归档操作。

### 6.2.6 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，导入时必须必须三个证书载体同时导入，解密合并后才能导入。

### 6.2.7 私钥在密码模块的存储

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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

#### 6.2.8 激活私钥的方法

CA 的私钥存放于硬件密码模块中，其激活数据按照 CPS §6.2.2 进行分割，并且保存在 IC 卡等硬件介质中，必须由 3 名管理员同时在场，插入管理员卡并输入 PIN 码，才能激活私钥。

#### 6.2.9 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。

#### 6.2.10 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。

#### 6.2.11 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。

### 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。

密钥到期后，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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 6.3.3 证书操作期和密钥对使用期限

证书有效期符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.4 部分的要求相一致。

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。

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：

对于 4096 位 CA 证书，其密钥对的最长允许使用年限是 30 年

对于 2048 位 CA 证书，其密钥对的最长允许使用年限是 27 年

对于 2048 位订户证书，其密钥对的最长允许使用年限是 27 个月

## 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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
- 至少 12 位字符
- 至少包含一个数字和一个字母
- 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
- 至少 90 天修改一次密码
- 不能与前四次的密码相同
- 每 90 天检查一次账户名和密码
- 移除 90 天内非活跃账户
- 证书系统登录尝试 5 次失败后即锁定账户

### 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

## 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。

系统安全符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16.5 部分的要求。

### 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

## 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；
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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 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：510010 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 证书遵循 ITU-T X.509v3（1997）：信息技术-开放系统互连-目录：认证框架（1997 年 6 月）标准和 RFC 5280：Internet X.509 公钥基础设施证书和 CRL 结构（1999 年 1 月）。

EV 证书至少包含基本的 X.509 v1 域，其规定值或值的限制如下表所描述。

表-EV 证书结构的基本域

| 域 | 值或值的限制 |
|---|---|
| 版本 | 指明 X.509 证书的格式版本，值为 V3 |
| 序列号 | 证书的唯一标识符 |
| 签名算法 | 签发证书时所使用的签名算法（见 CP$7.1.3） |
| 签发者 DN | 签发者的甄别名 |
| 有效起始日期 | 基于国际通用时间(UTC)，和北京时间同步，按 RFC 5280 要求编码 |
| 有效终止日期 | 基于国际通用时间(UTC)，和北京时间同步，按 RFC 5280 要求编码。有效期限的设置符合本 CPS 规定的限制。 |
| 主题 DN | 证书持有者或实体的甄别名 |
| 公钥 | 根据 RFC 5280 编码，使用 CPS 中指定的算法，密钥长度满足 CPS 指定的要求 |

### 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，证书扩展项遵循 IETF RFC 5280 标准，并符合 Guidelines For The Issuance And Management Of Extended Validation Certificates 的要求。

1、证书标准项

- 证书版本号(Version)


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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

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）


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。
- 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

别名称。

### 7.1.6 证书策略对象标识符

GDCA 签发的 EV 证书应包含证书策略的对象标识符。

证书标识符符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.3 部分的要求。

### 7.1.7 策略限制扩展项的用法

无规定。

### 7.1.8 策略限定符的语法和语义

无规定。

### 7.1.9 关键证书策略扩展项的处理语义

与 X509 和 PKIX 规定一致。

## 7.2 证书吊销列表

GDCA 定期签发 CRL，供用户查询使用。

### 7.2.1 版本

GDCA 的证书吊销列表采用 X.509 v2 版的证书格式。

### 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。
- 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 7.3.1 版本号

RFC2560 定义的 OCSP V1 版本。

### 7.3.2 OCSP 扩展项

无规定。

### 7.3.3 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）


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

- 需要签名（sigRequired）
- 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：510010 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 应每年对物理控制、密钥管理、操作控制、鉴证执行等情况执行一次审计，以确定实际发生情况是否与预定的标准、要求一致，并根据审查结果采取行动；每季度内部进行一致性审计和运营评估，并每次抽取至少 3%数量的证书进行评估，以保证证书服务的可靠性、安全性和可控性。

审计操作应当明确记录在 CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 17 部分的要求相一致。

## 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

## 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：


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。

## 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 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：510010 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 其他财产

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：510010 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：510010 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。

## 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。

### 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

◆ 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。

◆ 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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对订户的承诺如下：

- 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。

### 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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。
- 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 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 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 GDCA 所承担的上限额度，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；
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；


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

### 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。

## 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。


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

## 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，并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。

### 9.12.4 对象标识符变更

当本 CPS 发生修订时，相对应的证书策略对象标识符不会进行变更，仅增加版本识别代码。

## 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。
- 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


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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：510010 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：510010 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 有 1 个 EV 根证书 GDCA TrustAUTH R5 ROOT，其密钥长度为 4096-bit，下设 2 个子 CA 证书，分别为（1）GDCA TrustAUTH R4 Extended Validation SSL CA 证书，签发密钥长度为 2048-bit 的 EV SSL 服务器证书；（2）GDCA TrustAUTH R4 Extended Validation CodeSigning CA 证书，签发密钥长度为 2048-bit 的 EV 代码签名证书。

**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 Extended Validation SSL CA**

国家=CN

组织= GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.

通用名= GDCA TrustAUTH R4 Extended Validation SSL CA

序列号= 35 8f 82 86 5c e6 2d b1

有效期：2014年11 月26日到 2030年12月31日

SHA1 摘要= 20 ec 59 23 96 51 de c2 37 0d fd d0 75 97 6d c8 8c 01 32 7b

**3、GDCA TrustAUTH R4 Extended Validation CodeSigning CA**

国家=CN

组织= GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.

通用名= GDCA TrustAUTH R4 Extended Validation CodeSigning CA

序列号= 21 bd 62 27 3f b8 01 a8

有效期：2014年11 月26日到 2030年12月31日

SHA1 摘要= ac e9 a0 22 fa 09 38 5a d3 a3 e7 9c af 34 fe 39 58 50 a4 82


地址：广州市越秀区东风中路 448 号成悦大厦第 23 楼 邮编：510010 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 EV 电子认证业务规则修订记录表

| 内容 / 序号 | 项目 | 1.0 版 | 1.1 版 |
|---|---|---|---|
| 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。 |
| 二 | $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：510010 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813