ZJCA 通用证书策略(CP1)

V4.0

发布日期：2020 年 10 月 12 日

生效日期：2020 年 10 月 12 日

浙江省数字安全证书管理有限公司

修订记录

版本号	状态	修订说明	审核/批准人	生效日期
V1.0	版本发布	新版本发布	公司安全策略委员会	2009 年 5 月
V2.0	版本发布	内容修订更新	公司安全策略委员会	2017 年 5 月
V3.0	版本发布	内容修订更新	公司安全策略委员会	2018 年 8 月
V4.0	版本发布	内容修订更新	公司安全策略委员会	2020 年 10 月

版权声明

本证书策略的最新版本请参见本公司网站（www.zjca.com.cn），或者联系浙江省数字安全证书管理有限公司。

地址：浙江省杭州市中山北路 631 号晶晖商务大厦 22 层

邮编：310014

电话：86-571-85800770（总机）

传真：86-571-85800770-116

电子邮件：zjca@zjca.com.cn

公司网站：www.zjca.com.cn

本策略如有改动，对特定对象不再另行通知。

目　录

1.引言

1.1 概述

浙江省数字安全证书管理有限公司(Zhejiang Digital Certificate Authority Co. Ltd.，简称ZJCA或浙江CA)是依法面向社会提供电子认证服务的权威、公正的第三方机构。ZJCA严格按照《中华人民共和国电子签名法》和《电子认证服务管理办法》的要求，以及相关管理规定，提供数字证书签发、更新、变更、吊销和管理等服务，并通过以PKI技术、数字证书应用技术为核心的应用安全解决方案，为电子政务、电子商务、企业信息化构建安全可靠的信任环境。

证书策略（CP，Certification Policy）是关于证书认证机构（CA，Certification Authority）制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

本《ZJCA通用证书策略（CP1)》(以下简称《通用证书策略》）满足互联网标准组织制定的RFC3647《互联网X.509 公钥基础设施-证书策略和证书业务声明框架》，以及中华人民共和国标准GB/T 26855-2011《信息安全技术公钥基础设施证书策略与认证业务声明框架》的框架和内容要求。本《通用证书策略》适用范围为ZJCA发放的通用证书，包括个人证书、机构证书、设备证书和代码签名证书。具体设定了证书策略、生命周期、使用、依赖和管理的角色、责任与要求，以及各相关主体的职责。为批准、签发、管理和使用证书和相关的可信服务制定业务，提供技术、策略和法律上的要求和规范。

1.2 文档名称与标识

本文档的名称是《ZJCA通用证书策略（CP1)》，又称《通用证书策略》。

本证书策略是ZJCA发布的第4个版本，版本号4.0，将通过ZJCA网站（www.zjca.com.cn）面向社会公开发布，并提供更新说明和最新版本。

1.3PKI参与者

本文中所包含的电子认证活动参与者有：证书认证机构、注册机构、订户、依赖方以及其它参与者，下面将分别进行描述。

1.3.1 证书认证机构

证书认证机构（Certificate Authority，简称 CA）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。

ZJCA 是受用户信任的、权威的证书认证机构、负责颁发和分配公钥证书，是颁发证书的实体。

1.3.2 注册机构

注册机构（Registration Authority Center，简称 RA）是受理数字证书的申请、变更、恢复和吊销等业务的实体。

ZJCA 可以授权下属机构或委托外部机构作为注册机构,负责提供证书业务办理、身份鉴别与审核等服务。

ZJCA 授权外部机构作为注册机构，应在与外部机构签署的合同中，明确双方的权利与义务，以及承担的法律责任。

注册机构有责任依照《中华人民共和国电子签名法》和本《电子认证业务规则》妥善保存证书申请者的材料和数据,不允许将证书申请者的材料和数据透露给与证书业务无关的任何单位或个人,亦不允许将证书申请者的材料和数据用作任何商业利益方面的用途。

1.3.3 订户

是指接受 ZJCA 的依赖方协议、向 ZJCA 申请数字证书，并接受 ZJCA 提供服务的实体。

订户应能对证书对应的私钥的使用负有法律责任。

1.3.4 依赖方

是指接受 ZJCA 的依赖方协议,独立地判断证书的安全性是否满足其应用的安全需要，并验证证书和相应签名的实体。

1.3.5 其他参与者

其他参与者，即为 ZJCA 证书服务体系提供相关服务的其他实体。参与 ZJCA 证书服务体系的其他主要实体有:

1) 审核受理点（LRA）

审核受理点负责审核受理订户的证书申请信息,包括订户的名称、可以表明身份的号码和联系方法（通信地址、电子邮件、电话）等。受理点根据这些信息为订户提

供证书申请服务，或根据订户的要求，提供订户自行申请的技术支持。一个受理点可以开设几个受理窗口来完成证书申请注册功能，受理点对受理窗口的证书受理过程负有责任。受理窗口的设置、合并、撤销与受理点的设置、合并、撤销相联系。当受理窗口不符合本《电子认证业务规则》时，ZJCA 有权关闭其所属的受理点。

2) 证书垫付商

证书垫付商，是指能够为其所属或所服务的订户或潜在订户群体承担所有证书服务费用的团体或组织。证书垫付商根据本《通用证书策略》的规定、ZJCA《电子认证业务规则》及相关法律法规的要求，有权要求取缔由其支付费用的证书持有者的全部或部分证书服务，包括但不限于对持有者证书的吊销。垫付商必须根据与 ZJCA 签署的协议，事先预订证书种类、数量并缴纳相应的费用，必须承担其代付费用的全部证书持有者身份真实性的责任。

1.4 证书应用

1.4.1 适用的证书应用

ZJCA 签发的数字证书适合应用于企业信息化、电子政务和电子商务等领域，用于订户在网络环境中所进行的身份认证和电子签名、以及数据加密等服务。

ZJCA 签发的通用型证书包含个人证书、机构证书、设备证书和代码签名证书等，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种类。具体说明如下：

- 个人证书

个人证书，包括个人用户证书和机构员工证书，用于区分、标识和鉴别个人身份的场景，适用于个人身份认证和电子签名、以及数据加密保护等服务。

- 机构证书

机构证书，包括机构单位证书和机构法人证书，用于需要区分、标识和鉴别机构身份的场景，适用于机构身份认证和电子签名、以及数据加密保护等服务。

- 设备证书

设备证书，包括各种应用服务器证书和 Web 服务器证书（域名证书），用于标识各种服务器设备身份，实现设备身份认证以及交互数据的加解密，保证传输数据的完整性和安全性等。

- 代码签名证书

代码签名证书，用于对软件代码的数字签名，以此来标识软件来源以及软件开发

者的真实身份,保证代码在签名之后不被恶意篡改。申请代码签名证书的可以是个人、也可以是机构。

1.4.2 限制的证书应用

ZJCA 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己承担。

对于通用证书，限制的证书应用包括:

1) 任何与国家或地方法律、法规规定相违背的应用系统;
2) ZJCA 不认可的证书应用系统;
3) 证书不涉及用于、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，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

1.5.1 策略文档管理机构

ZJCA 安全策略委员会是本《通用证书策略》的管理机构和最高决策机构，负责本《通用证书策略》的制定、发布和更新等事宜。

本《通用证书策略》由浙江省数字安全证书管理有限公司拥有完全版权。

1.5.2 联系人

ZJCA 对本《通用证书策略》进行严格的版本控制，并由 ZJCA 指定的专门机构负责解释。

联 系 人: 浙江省数字安全证书管理有限公司安全管理小组

电　　话: 86-571-85800770（总机）

传　　真: 86-571-85800770-116

地　　址: 浙江省杭州市下城区中山北路 631 号晶晖商务大厦 22 层

邮　　编: 310014

电子邮件: zjca@zjca.com.cn

网站地址: www.zjca.com.cn

1.5.3 决定 CP 符合策略的机构

ZJCA 安全策略委员会是 CP 的最高决策机构，负责本《通用证书策略》的制定、

发布和更新等事宜。

1.5.4 CP 批准程序

本《通用证书策略》由 ZJCA 安全策略委员会组织编写小组进行编写。编写小组完成 CP 草案的编写后，由 ZJCA 安全策略委员会组织对 CP 草案进行初步评审。初步评审后，将 CP 评审稿提交给 ZJCA 安全策略委员会审批。经 ZJCA 安全策略委员会审批通过后，在 ZJCA 的网站对外公布。

本《通用证书策略》经 ZJCA 安全策略委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

本《通用证书策略》的发布不对其他实体单独通知。

1.6 定义和缩写

以下定义是用于本《通用证书策略》:

1) 公开密钥基础设施（PKI）Public Key Infrastructure

支持公开密钥体制的安全基础设施，提供身份鉴别、加密、完整性和不可否认性服务。

2) 私钥 Private Key

非对称密码算法中只能由拥有者使用的不公开的密钥。

3) 公钥 Public Key

非对称密码算法中可以公开的密钥。

4) 电子认证服务机构（CA）Certificate Authority

ZJCA 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。

ZJCA 是受用户信任的、负责创建和分配公钥证书的权威机构，是签发数字证书的实体。

5) 注册机构（RA）: Registration Authority

注册机构是受理数字证书的申请、更新、变更和吊销等业务的实体。

ZJCA 可以授权下属机构或委托外部机构、依赖方作为注册机构，负责提供证书业务办理、身份鉴别与审核等服务。

ZJCA 授权外部机构、依赖方作为注册机构，应在与外部机构、依赖方签署的合同中，明确双方的权利与义务，以及承担法律责任。

6) 电子认证业务规则（CPS）Certification Practice Statement

关于电子认证服务机构在全部证书服务生命周期中的业务实践（如签发、管理、吊销、更新证书或密钥等）所遵循的规则的详细描述和声明，提供其它业务、法律和技术方面的细节。《ZJCA 电子认证业务规则》是 ZJCA 证书相关业务和系统的运行规则。

7) 证书策略（CP）Certification Policy

关于认证机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

8) 证书吊销列表（CRL）Certificate revocation list

认证机构的失效证书列表。证书吊销可能由于证书过期、私钥失窃或者其他原因产生。

9) 在线证书状态协议服务（OCSP 服务）Online Certificate Status Protocol

在线的证书状态查询服务，该服务的主要对象是依赖方。

10) 数字证书（证书）Certificate

也称公钥证书，由点子认证服务机构（CA）签名的、包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

11) 电子签名人

指持有 ZJCA 数字证书并以本人身份或者以其所代表的名义实施电子签名的实体。

12) 电子签名依赖方

指基于对 ZJCA 数字证书或者电子签名的信赖而从事有关活动的实体。

2.信息发布与信息管理

2.1 信息库

ZJCA 信息库是一个对外公开的信息库，面向订户及依赖方提供信息服务。提供信息服务包括但不限于以下内容：CP、CPS、协议、证书以及 CRL 等。

2.2 认证信息的发布

订户证书签发后，ZJCA 将证书和 CRL 发布到信息库，订户及依赖方可以通过访问该信息库查询和获取证书。

证书状态可以通过 ZJCA 提供的 OCSP 或 CRL 获得。

本《电子认证业务规则》和 CP 发布在 ZJCA 网站（www.zjca.com.cn），供相关方下载和查阅。

2.3 发布的时间或频率

本《通用证书策略》一经 ZJCA 网站发布，即时生效。对数字证书的订户及证书申请人均具备约束力。

通用型证书签发时，ZJCA 通过信息库自动将该证书发布。

证书吊销列表（CRL）每 24 小时发布一次。

2.4 信息库访问控制

对于公开发布的 CP、CPS 和协议等信息，ZJCA 允许公众自行通过公司网站进行查询和访问。对于订户的证书和证书状态等信息，订户和依赖方可通过 ZJCA 的信息库进行查询。

ZJCA 的安全访问控制机制确保只有经过授权的人员才能编写和修改信息库中的信息，但不限制对这些信息的阅读权。ZJCA 在必要时可自主选择是否实行信息的权限管理，以确保 ZJCA 相关实体的实际权益。

3.标识与鉴别

3.1 命名

3.1.1 名称类型

ZJCA 生成或签发的证书命名符合 X.500 甄别名规定，遵循 X.509 标准。其通用名包含于每张证书的主题中，唯一标识证书订户的身份。各类证书命名方式不同，但是所有证书订户名都需要严格审查，命名符合 X.500 甄别名规定。

3.1.2 对名称意义化的要求

订户的甄别名(DN)必须具有一定的代表意义。

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

3.1.3 订户的匿名或假名

ZJCA 通用证书订户应该使用真实名称。对于测试订户,其 DN 项中必须包括“测试”或者“test”标记。

在 ZJCA 证书服务体系中，订户不宜使用匿名和假名。

3.1.4 理解不同名称形式的规则

ZJCA 签发的通用证书,其甄别名(DN)的内容各是符合 X.500 Distinguished Name（DN）的命名方式。

下面是一般识别名称的命名规则:

识别名称（DN）	说明	内容（示例）
Country(C)	机构所在国家名称	C=CN
Organization(O)	机构名称	O=ZJCA
Organization Unit(OU)	单位或部门名称	OU=技术中心
Common Name(CN)	证书持有者的一般通用名称	CN=张三

详细的 DN 选用说明可参考本《通用证书策略》中 “7.1.4 名称形式”中的选项的说明。

3.1.5 名称的唯一性

ZJCA 所有证书持有者的主题甄别名，要求必须是唯一的，ZJCA 根据该主题甄

别名有效的鉴别证书持有者。对同一订户，可以使用其主题名为其签发多种证书，但证书扩展项不同。

3.1.6 商标的承认、鉴别和角色

当订户或证书申请者的名称包含商标时，应向 ZJCA 提供商标注册方所有权的文件证明。

当订户或者申请者的名称，经有关主管部门的合法文件证明为其他订户或者申请者所有时，该订户必须承担因此产生的法律责任。验证订户或者申请者使用该名称的合法性，并不在 ZJCA 的业务职责范围。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

证书订户向 ZJCA 申请证书时，需提交该用户的证书请求（CSR），证书请求内包含订户的真实信息、订户公钥和订户私钥对该证书请求的签名信息。

ZJCA 通过使用订户的公钥验证该证书请求中的签名信息，以此来判断订户拥有私钥。

3.2.2 组织机构身份的鉴别

在组织机构申请者身份的鉴别流程中，ZJCA 将按照证书类型的要求进行不同的验证。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盖章或签字。

机构订户在向 ZJCA 或其注册机构、受理点等服务机构申请机构证书时必须递交组织机构身份证明文件，包括但不限于工商营业执照副本、统一社会信用代码证、事业单位登记证等；如申请者需要申请设备证书，须向 ZJCA 提供设备真实存在的有效证明，包括但不限于设备域名或 IP 归属性文件等；如申请者需要申请机构代码签名证书，申请者须承诺该代码证书不被用于任何恶意或者非法的用途。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。

ZJCA 或其注册机构、受理点在进行法律规定的有限审查后，不承担对申请者身份证明文件（如身份证等）进行合法性甄别的义务。ZJCA 或其注册机构、受理点将根据审查结果进行批准申请或拒绝申请的操作。

3.2.3 个人身份的鉴别

在个人申请者身份的鉴别流程中，ZJCA 可以按照证书类型相应的要求进行不同

验证。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盖章或签字。

个人订户在向 ZJCA 或其注册机构、受理点等服务机构申请个人证书时必须递交个人身份证明文件，包括但不限于身份证、护照、户口簿、港澳台居民身份证、军官证等。如申请者需要申请设备类型证书，须提交域名或 IP 使用权证明材料；如申请个人代码签名证书，申请者须承诺该代码证书不被用于任何恶意或者非法的用途。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。

ZJCA 或其注册机构、受理点在进行法律规定的有限审查后，不承担对申请者身份证明文件（如身份证等）进行合法性甄别的义务。ZJCA 或其注册机构、受理点将根据审查结果进行批准申请或拒绝申请的操作。

对于包括邮寄、传真、电子邮件等非现场方式进行的身份鉴别，ZJCA 或其注册机构、受理点可要求申请者提供额外的身份鉴别资料和证明，并选择认为合理的方式辅助进行鉴别。

3.2.4 没有验证的订户信息

订户提交的鉴别文件中，除签发证书所必需的身份信息外，其他不属于鉴别范围内的信息，为没有验证的订户信息。

对于没有验证的订户信息，ZJCA 或授权的注册机构、受理点将以书面或电子形式进行归档，但不承诺这类信息的真实性，也不承担由于这类信息的不真实、不完整等所引起的任何责任与解决纠纷的义务。

3.2.5 授权确认

ZJCA 或授权的注册机构、受理点、依赖方将要求被授权的经办人递交相应的申请者授权证明，并对其递交的材料作真实性声明，承担相应的法律责任。个人订户在数字证书申请表上写明经办人的身份信息并签名确认后，则证明本人对经办人的授权确认；机构订户在数字证书申请表上写明经办人的身份信息并经经办人签名、组织机构加盖机构公章后，则证明本组织机构对经办人的授权确认。

ZJCA 或授权的注册机构、受理点、依赖方会按照本《通用证书策略》的规定，对材料进行鉴别，也可能采取附加的或者额外的方式进行这种鉴别。如果经办人拒绝 ZJCA 或授权的注册机构、受理点、依赖方的身份与授权鉴别要求，那么就被视作放弃对证书的申请。同时 ZJCA 声明，ZJCA 或授权的注册机构、受理点、依赖方可以拒绝任何申请请求，并且没有对此说明原因的义务。

3.2.6 互操作准则

ZJCA 数字证书服务体系暂不涉及互操作。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

通用证书的常规密钥更新中，通过订户使用原有私钥对更新请求进行签名，ZJCA 将会对订户的签名和公钥、更新请求内包含的订户信息进行正确行、合法性、唯一性的验证和鉴别。

国家主管部门对密钥的管理、更新等有规定的，ZJCA 将严格予以执行。

3.3.2 吊销后密钥更新的标识与鉴别

通用证书吊销后密钥更新中对身份标识和鉴别的要求，使用原始身份验证相同的流程，详见“3.2.2 组织机构身份的鉴别”和“3.2.3 个人身份的鉴别”。

3.4 吊销请求的标识与鉴别

通用证书订户本人吊销时的请求标识和鉴别使用原始身份验证相同的流程，详见“3.2.2 组织机构身份的鉴别”和“3.2.3 个人身份的鉴别”。

如果是因为订户没有履行本《通用证书策略》和《ZJCA 电子认证业务规则》所规定的义务，由 ZJCA 或授权的注册机构、受理点等服务机构申请吊销订户的证书时，不需要对订户身份进行标识和鉴别。

4 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

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

4.1.2 申请过程与责任

通用证书订户按照本《通用证书策略》、《电子认证业务规则》以及相关协议所规定的要求，填写证书申请表，并准备相关的身份证明材料。ZJCA 或授权的注册机构、受理点等服务机构依据身份鉴别规范对订户的身份进行鉴别，并决定是否受理申请。

申请过程中，各方的责任说明如下:

1) 订户责任:

- 订户要按照本《通用证书策略》3.2 节所述的要求提供有效身份证明材料，并确保材料真实准确。
- 配合 ZJCA 或授权的注册机构、受理点、依赖方等服务机构完成对身份信息的采集、记录和审核。

2) ZJCA 责任:

- ZJCA 参照本《通用证书策略》3.2 节所述的要求，对订户的身份信息进行采集、记录和审核。
- 审核通过后，ZJCA 向订户签发通用型数字证书。
- 如果用户身份信息的鉴别是由授权的注册机构、受理点或依赖方完成的，ZJCA 有权对授权的注册机构、受理点或依赖方进行监督管理和审计。
- ZJCA 保证整个 CA 系统安全可靠的运行，但不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担赔偿责任。

3) 授权的注册机构、受理点或依赖方的责任:

- 注册机构、受理点或依赖方应参照本《通用证书策略》3.2 节所述的要求，对订户的身份信息进行采集、记录和审核。
- 审核通过后，向 ZJCA 提交证书申请，由 ZJCA 向订户签发证书。
- 注册机构、受理点或依赖方必须接受 ZJCA 和国家相关机构的监督管理和审计。

- 注册机构、受理点或依赖方应当按照 ZJCA 的要求，向 ZJCA 提交身份鉴别材料或自行妥善保管。
- 对于快捷型证书，授权的依赖方需经订户同意和授权，才能为该订户申请证书和保管证书与密钥，同时需确保订户密钥的存储安全和使用安全。

根据《中华人民共和国电子签名法》的规定，订户未向 ZJCA 或授权的注册机构、受理点、依赖方提供真实、完整和准确的信息，或者有其他过错，给 ZJCA 或授权的注册机构、受理点、依赖方造成损失的，应承担相应的法律责任和经济赔偿。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

当认证机构、注册机构接收到订户的证书申请后，须按照以下规定对订户的申领材料进行审查：

机构订户：参照本《通用证书策略》3.2.2 节的规定。

个人订户：参照本《通用证书策略》3.2.3 节的规定。

4.2.2 证书申请批准和拒绝

ZJCA 或授权的注册机构、受理点等机构按照本《通用证书策略》所规定的身份鉴别流程对证书申请人提交的申领信息及身份信息进行鉴别后，根据鉴别结果决定批准或拒绝证书申请。

证书申请人通过身份鉴别流程且鉴别结果为合格的，将批准证书申请，ZJCA 为证书申请人制作并颁发数字证书。

证书申请人未能通过身份鉴别，ZJCA 或授权的注册机构、受理点将拒绝申请人的证书申请，并通知申请人鉴别失败，同时以适当的方式、在合适的时间内通知申请人(法律禁止的除外)。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.3 处理证书申请的时间

注册机构在接受所有必须的用户申请信息后，将在 5 个工作日内对证书申请人提交的信息进行鉴别和审核，并做出批准或者拒绝的决定。

ZJCA 或授权的注册机构、受理点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 ZJCA 的管理要求。

4.3 证书签发

4.3.1 证书签发期间电子认证服务机构的行为

ZJCA 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。

4.3.2 订户证书签发的通知

无论是拒绝还是批准订户的证书申领，ZJCA 或授权的注册机构、受理点须通过适当的方式通知订户。如果证书申领获得批准并签发，注册机构或受理点应通过适当的方式告诉订户如何获取证书。

ZJCA 的证书签发系统签发证书后，将证书签发的信息通过适当的方式通知注册机构或受理点。

4.4 证书接受

4.4.1 构成接受证书的行为

当通用型证书订户填写证书申请表、同意相关订户协议、提供了真实准确的身份信息,并经注册机构审核通过后、接受了载有证书的介质即视为订户已经接受此证书。如订户对证书有异议，应在 5 个工作日之内提出。

4.4.2 对证书的发布

ZJCA 在签发证书后定期将该证书发布到信息库上，并通过安全的机制向依赖方提供查询服务。

4.4.3 电子认证服务机构对其他实体的通告

ZJCA 不对其他实体进行通知，其他实体如有需要可在信息库上自行查询。

4.5 密钥对和证书的使用

密钥对和证书须用于其规定的、批准的用途。签名密钥对用于签名与签名验证，加密密钥用于加密解密。

密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用是不受保障的。

4.5.1 订户私钥和证书的使用

订户在提交了证书申请并接受了 ZJCA 所签发的证书后，均视为已经同意遵守与

ZJCA、依赖方有关的权利和义务的条款。订户在使用私钥和证书时须遵循以下约定:

1) 订户只能在规定的范围内（在本《通用证书策略》1.4 中定义）使用私钥和证书，并对使用行为承担责任;
2) 订户在使用证书时必须遵守相关的订户协议及本《通用证书策略》和 ZJCA《电子认证业务规则》的要求;
3) 订户只有在接受了相关证书之后才能使用对应的私钥，并且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) 订户应当妥善保存其私钥和证书，避免遗失、泄露、被篡改或者被盗用,避免他人未经授权而使用证书的情形发生。
5) 任何人使用证书时都必须检验证书的有效性。

4.5.2 依赖方公钥和证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等），在依赖方接受电子签名信息后可通过对方证书中的公钥验证对方电子签名的真实性。验证电子签名的真实性包括:

1) 获得电子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) 证书的用途适用于对应的签名;
4) 确认该电子签名生成时对应的证书在有效期内且未被吊销;
5) 使用证书上的公钥验证该电子签名;

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

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

4.6 证书更新

为保证证书及其密钥对的安全有效，ZJCA 会为签发的证书设置有效期，这是为了保证订户的权利。证书更新是在不改变证书中订户的公钥或其他任何信息的情况下，为订户签发一张新的证书，以便延长证书的有效期。

4.6.1 证书更新的情形

如果订户需要更新证书，ZJCA 要求订户在证书有效期到期前，前往注册机构办

理。证书过期后也能办理更新业务，但是由于订户未及时办理证书更新而导致原证书过期和无法使用，ZJCA 及授权的注册机构、受理点不承担任何责任。

当订户的证书有效期到期前，ZJCA 将做出合理的努力，在证书有效期满之前向证书订户或者证书经办人、垫付商等发送证书更新提示。合理的努力包括但不限于网站提示、系统提示、书面提示、E-mail 通知或者其它方式，但 ZJCA 采取了上述任意一项提示或者通知方式，均可被视作进行了合理的努力。

4.6.2 请求证书更新的实体

个人证书和机构证书的订户为证书更新实体。

设备证书和代码签名证书不支持证书更新，可按初次申请的流程申请新的证书以延长其有效期。

4.6.3 证书更新请求的处理

处理证书更新请求的过程，包括申请鉴别、签发证书。对申请的鉴别须基于以下几个方面：

- 申请对应的原证书存在并且由 ZJCA 签发；
- 基于原注册信息对订户进行当面或线上的身份鉴别；

在以上鉴别通过后才可签发更新后的证书。

4.6.4 通知订户新证书签发

同 4.3.2。

4.6.5 构成接受证书更新的行为

同 4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

同 4.4.2。

4.6.7 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4.7 证书密钥更新

证书密钥更新是指订户需要生成新密钥并申请为新密钥签发新证书。

4.7.1 证书密钥更新的情形

如果出现下列情形，订户必须选择证书密钥更新或者重新申请证书：

1) 当订户证书即将到期或已经到期；

2) 当订户证书密钥遭到破坏时；

3) 当订户证实或怀疑其证书密钥不安全时；

4) 当订户证书被吊销后需要重新获得证书；

5) 其他可能导致密钥更新的情况。

4.7.2 请求证书密钥更新的实体

订户可以请求证书密钥变更。订户包括持有 ZJCA 签发的个人、机构、设备及代码签名等各类证书的证书持有人。

4.7.3 证书密钥更新请求的处理

当订户需要进行证书密钥更新时，订户可向 ZJCA 或授权的注册机构、受理点提交密钥更新申请。ZJCA 或授权的注册机构、受理点将对订户的请求和身份进行鉴别，鉴别通过之后将使用新的密钥签发新的证书。

订户证书密钥更新请求的鉴别流程和要求同初次申请的情形，具体见 3.2.2。同时，需要满足以下两个条件：

- 订户原证书由 ZJCA 签发
- 订户原注册信息与本次申请提交的信息一致

在以上鉴别通过后才能为订户使用新的密钥签发新的证书。

4.7.4 订户密钥更新后新证书签发的通知

同 4.3.2。

4.7.5 构成接受密钥更新后新证书的行为

同 4.4.1。

4.7.6 电子认证服务机构对密钥更新后的证书发布

同 4.4.2。

4.7.7 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4.8 证书变更

4.8.1 证书变更的情形

在证书有效期内，当证书信息发生变化，订户可以选择证书变更，申请签发新的证书，原证书做吊销处理。

4.8.2 请求证书变更的订户实体

订户可以请求证书变更。订户包括持有 ZJCA 签发的个人、机构、设备及代码签名等各类证书的证书持有人。

4.8.3 证书变更请求的处理

当订户需要进行证书变更时，订户可向 ZJCA 或授权的注册机构、受理点提交证书变更申请。ZJCA 或授权的注册机构、受理点将对订户的请求和身份进行鉴别，鉴别通过之后将为订户签发新的证书。

订户证书变更请求的鉴别流程和要求同初次申请的情形，具体见 3.2.2。同时，需要满足以下两个条件:

- ◆ 订户原证书由 ZJCA 签发
- ◆ 除本次申请变更的内容外，订户原注册信息与本次申请提交的信息一致

在以上鉴别通过后才能为订户签发新的证书。

4.8.4 订户新证书签发的通知

同 4.3.2。

4.8.5 构成变更证书接受的行为

同 4.4.1。

4.8.6 电子认证服务机构对变更证书的发布

同 4.4.2。

4.8.7 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

1) 证书有效期内，如果出现下列情况（包括但不限于下列情况），ZJCA 可以直

接将证书予以吊销:

a) 由于证书管理系统的不适用或者证书系统的整合需要;
b) 由于证书订户未能履行与 ZJCA 之间的协议（如未缴纳费用等）而被这些有权力主张吊销的实体提出;
c) 由于证书的不当使用而违反国家的法律法规、本《通用证书策略》或 ZJCA《电子认证业务规则》规定的主要和重要义务;
d) 政府主管机构或者法院依照正式合法的程序提出申请;
e) 订户（或其授权的经办人）请求吊销证书，一旦确定请求吊销者是订户本人的;
f) 订户申请证书服务时，提供不真实或者欺骗性材料的;
g) 电子认证服务机构因运营问题，导致 ZJCA 内部重要数据或 ZJCA 根密钥失密等原因的;
h) 证书的私钥丢失、被盗、被篡改、被未经授权泄露或被损害;
i) 发现并证明某证书没有根据本《通用证书策略》或 ZJCA《电子认证业务规则》要求的程序而签发;
j) 由于不可抗力、自然灾害、计算机或通信故障、法律法规的修改、政府行为（包括但不限于出口控制管理部门的限制行为）或其它超出人力合理控制的原因，造成其它人的信息受到严重威胁或危及其安全，从而拖延或阻止了订户责任的执行。

2) 证书在有效期内，如果出现下列情况，订户必须提出吊销请求:
a) 与证书中的公钥相对应的私钥被泄密、被窃取、被篡改或者其它原因产生对私钥的安全性顾虑;
b) 证书中的订户相关信息发生变更;
c) 由于证书不再需要用于原来的用途而要求终止;
d) 证书中的相关内容和提交申请进行注册时不一致;
e) 证书持有者已经不能履行或违反了本《通用证书策略》或 ZJCA《电子认证业务规则》或其它协议、法规及法律所规定的责任和义务。

3) 其它 ZJCA 认为可以进行吊销的理由。
4) ZJCA 没有义务一定要公开某一张证书被吊销的原因。

4.9.2 请求证书吊销的实体

根据不同的情况，订户、ZJCA、注册机构或授权的受理点可以请求吊销订户证书。

4.9.3 请求吊销的流程

订户吊销证书时可按以下流程进行:

订户（或其授权经办人）填写书面申请表并签名或盖章，同时提交相应的证明材料，向注册机构或受理点提出吊销证书请求。

ZJCA、注册机构或受理点在接到订户的吊销请求后，需通过可靠的方式确认请求确实来自订户。

4.9.4 吊销请求宽限期

订户一旦发现需要吊销证书,应在 8 小时之内向发放该证书的注册机构或关联过新应用的注册机构提出吊销请求。

4.9.5 电子认证服务机构处理吊销请求的时限

ZJCA 或其授权的注册机构、受理点从收到吊销请求到审核完成，做出吊销决定并将吊销证书发布到信息库。

对于通用型证书，处理吊销请求的全部工作应当在 24 小时内完成。订户在正式提出证书吊销申请后不得在交易中继续使用此证书，否则由此产生的后果，由订户自行承担。

4.9.6 依赖方检查证书吊销的要求

在具体应用中，依赖方必须使用以下两种功能之一进行所依赖证书的状态查询:

1) CRL 查询

利用证书中标识的 CRL 地址，通过信息库中的目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的检验。

依赖方需要验证 CRL 的可靠性和完整性，确保是经 ZJCA 发布并且签名的。

2) 在线证书状态查询(OCSP)

依赖方可通过 ZJCA 提供的在线证书状态查询服务实时查询订户证书状态。OCSP 服务系统接受证书状态查询请求，从信息库中查询证书的状态，查询结果经过签名后，返回给依赖方。

4.9.7CRL 发布频率

CRL 发布频率为 24 小时一次，在发布的同时对原有内容进行更新。

4.9.8CRL 发布的最大滞后时间

ZJCA 在生成 CRL 后会立即更新信息库，CRL 发布的最大滞后时间为 24 小时。

4.9.9 证书状态在线检查的可用性

ZJCA 提供 OCSP 证书状态查询服务，以供安全保障要求高的应用使用。

4.9.10 依赖方执行在线吊销状态查询的要求

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

4.9.11 吊销信息的其他可用传播途径

无其他途径。

4.9.12 密钥泄露的特殊要求

当订户发现、或有充足的理由发现其密钥遭受安全威胁时，应及时地提出证书吊销请求。

4.9.13 证书挂起的条件

当证书仍处于有效期，为了保留订户的证书使用权利，而不申请吊销该证书，当出现下列情况时，可以进行证书挂起：

1) 证书订户要求暂停使用该证书一段时间；
2) 订户未能履行与 ZJCA 签订的协议中应尽的义务，但向 ZJCA 提出申请并获得批准后；
3) 除证书订户（或者其授权的委托经办人）外的其它实体，如电子认证服务机构及其授权的服务机构、法院、政府主管部门及其他公共权利部门，向 ZJCA 提出挂起证书请求并获得批准。

4.9.14 请求证书挂起的实体

根据不同的情况，订户、ZJCA、注册机构或授权的受理点可以请求吊销订户证书。

4.9.15 请求挂起的过程

订户挂起证书时可按以下流程进行:

订户（或其授权的经办人）填写书面申请表并签名或盖章，同时提交相应的证明材料，向注册机构或受理点提出挂起证书请求。

ZJCA、注册机构或受理点在接到订户的挂起请求后，需通过可靠的方式确认请求确实来自订户。

4.9.16 证书挂起的最长时间

证书挂起的最长时间不超过 6 个月。

4.10 证书状态服务

4.10.1 操作特征

ZJCA 提供两种证书状态查询服务:

1) CRL 查询

CRL 通过信息库的目录服务器进行发布,其可信度及安全性由 ZJCA 及其授权的发证机构的 CA 证书的签名来保证。CRL 仅提供定期的证书状态查询，目前 ZJCA 每 24 小时发布一次 CRL。

订户和依赖方需要将 CRL 下载到本地后进行验证，包括 CRL 的合法性验证和检查 CRL 中是否包含待验证证书的序列号。

2) OCSP 查询

依赖方和订户可以通过 ZJCA 提供的 OCSP 服务在线查询证书状态，OCSP 提供实时的证书状态查询服务。

4.10.2 服务可用性

ZJCA 提供 7X24 小时的证书状态查询服务。即在网络允许的情况下，依赖方和订户能够实时获得证书状态查询服务。

4.10.3 其他可选特征

根据请求者的要求，在请求者支付相关费用后，ZJCA 可以提供以下通知服务:

- 提供证书同步服务，当订户的证书被签发、更新后，可将新发的证书同步给请求者;
- 提供通知服务，当指定的证书被吊销时，ZJCA 将通知请求该项服务的请求

者。

4.11 订购结束

以下二种情形将被视为订购结束:

1) 证书在有效期外，订户不再延长证书使用有效期或不再重新申请证书时，视为订购结束。
2) 证书在有效期内，证书吊销视为订购结束。

4.12 密钥托管和恢复

4.12.1.密钥托管和恢复的策略与实施

订户在向 ZJCA 申请证书时，订户的签名密钥对由订户的密码设备（如智能密码钥匙或智能 IC 卡)、或等同安全等级的密码模块生成，ZJCA 不对订户的签名密钥进行托管。

订户的加密密钥对由密钥管理中心生成,订户证书密钥恢复是指加密密钥的恢复。密钥恢复分为两类：订户密钥恢复和司法取证密钥恢复。

4.12.2.会话密钥的封装和恢复的策略与实施

ZJCA 使用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开并恢复会话密钥。

5 设施、管理和操作控制

5.1 物理控制

ZJCA 认证机构的物理场地满足以下安全要求并最有效地控制风险:

1) 防止物理非法进入

4 层物理结构及完善的安全管理体系保护 ZJCA 的运营设施和信息安全。

2) 防止未经过授权的物理访问

确保未经过授权的人或仅被授权访问有限物理区域的人员不得访问 ZJCA 认证机构内的受限区域。

3) 维护 CA 服务的完整性、可用性

针对环境的安全威胁，采用了一些有力的措施，例如 UPS 电源保障、数据线路、门禁系统、监控装置和屏蔽机房的建设等。保障提供 CA 服务的系统、设施不受到破坏，保证认证服务不被中断。

5.1.1 场地位置与建筑

ZJCA 认证业务的运营场地是按照以下国家相关部门制定规范进行构建的:

- GB 50174-93《电子计算机机房设计规范》
- GB 2887-89《计算站场地技术条件》
- GB 9361-88《计算站场地安全要求》
- GB 5054-95《低压配电装置及线路设计规范》
- GB 19-87《采暖通风与空气调节设计规范》
- GB 5157《建筑防雷设计规范》
- GBJ 79-85《工业企业通信接地设计规范》
- GB 50034-1992《工业企业照明设计标准》

运营场地的整体建筑由能够阻止物理穿透的材料建成。建筑物的外墙、地板和天花板都属于永久性建造，并互相联结，可以阻止未经过授权的进入、穿透。敏感区域及以上区域的墙壁，在其双层干饰面内墙之间，采用镀钢夹层。敏感区域只设置一个门作为的常规入口。根据消防要求置了消防紧急出口。敏感区域及以上区域没有窗口。

物理安全是基于物理层级的保护，每一物理层就是一个屏障，需要设置可以控制进出的门禁系统来控制每个人进出每一个区域。每一层区域必须有非常严格的控制方法防止未经授权的物理访问。而且要求每一个物理安全层在物理上必须能完全包含下

一个物理安全层，最外层的安全层应该是整个建筑物的外墙。

5.1.2 物理访问控制

ZJCA 的物理设施的访问控制系统是与控制各层门进出的门禁系统相结合的，并实现了以下安全功能：

- 进出每一道门都有记录作为审计依据；
- 每道门的进出采用身份识别卡或生物识别鉴定的控制方法；
- 授权人员进出每一道门都会有时间记录和相关信息提示；
- 关键区域的门都设有强行开门报警。
- 整套访问控制系统配有断电保护装置提供紧急用电；
- 与门禁系统配合使用的还有录像监控系统，所有的录像资料根据安全审计要求保留一段时间。

5.1.3 电力与空调

ZJCA 有安全、可靠的电力供电系统及电力备用系统，以确保系统 7×24 小时正常供电，及在供电系统出现供电中断时能够提供正常的服务。另外，ZJCA 认证机构还具有空调系统控制运营设施中的温度和湿度。

本系统建设的供配电系统达到以下效果：

- 完全根据各设备电负荷的大小，选用相应线径的供电电缆和不同容量的电源滤波器。
- 多处采用低泄漏电流的电源滤波器，达到插入衰减能力与屏蔽室综合效能一致的效果。
- 针对大容量的供电全部采取三相供电方式。
- 对于室内电缆沟或管线走线，按照实际要求位路配路电源插座。

根据《机房建设概算》和 GB50174-93《电子计算机机房设计规范》的有关规定，ZJCA 的机房使用独立的空调与冷却系统，机房的温湿度控制执行 B 级标准，即温度为 23℃±5℃，相对湿度为 55%±15%，空气洁净度为粒径≥0.5um，个数≤18000/dm3。通过设备照明、通风、人体体温及建筑热量的估算，24 小时稳定控制室温湿度。

5.1.4 水患防治

ZJCA 数据中心有专门的技术措施，防止漏水的出现，并能够在出现漏水时最大程度地减小漏水对认证系统的影响。

5.1.5 火灾预防和保护

5.1.5.1 结构防火

ZJCA 认证机构的运营中心耐火等级符合 GB50045-95《高层民用建筑设计防火规范》中规定的二级耐火等级，防护方法应符合当地管理部门或机构的安全要求。

5.1.5.2 火灾报警及消防设施

ZJCA 认证机构设施内设置火灾报警装置。在机房内、各物理区域内及易燃物附近部位设置烟、温感探测器。

敏感区及高敏区配置了独立的气体灭火装置。

5.1.5.3 紧急出口

根据国家的有关消防要求、规定和标准，在非敏感区及敏感区的办公区域内，设置了紧急出口，紧急出口设有消防门。紧急出口有监控设备进行实时监控，并保证紧急出口门随时可用。紧急出口门外部没有门开启的装置，且紧急出口门与门禁报警设备联动。非紧急避险状态下，紧急出口门不能被内部人员任意打开。

5.1.6 介质存储

ZJCA 认证机构对储存产品软件和数据、归档、审计或备份信息的介质保存在安全设施中,这些设施受到适当的物理和逻辑访问控制的保护,只允许授权人员的访问,并防止这些介质受到意外损坏（如水、火灾和电磁)。

5.1.7 废物处理

当 ZJCA 电子认证服务系统使用的硬件设备、存储设备、加密设备等废弃不用时，将按国家的有关规定进行报废处理，其中所涉及敏感性、机密性信息都将被安全、彻底的消除，保证其信息无法被恢复与读取。

当电子认证服务机构保存的相关数据已不再需要或存档的期限已满时，ZJCA 将完全销毁这些数据。

所有处理行为将由至少 2 名人员同时进行，相互监督，并将处理行为记录在案，并签字确认，以供审查的需要，所有销毁行为遵守我国的法律。

5.1.8 异地备份

ZJCA 认证机构对关键系统数据、审计日志数据和其他敏感信息进行日常备份，这些备份信息保存在 ZJCA 建筑物以外的安全的地方。

5.1.9 注册机构物理控制

ZJCA 注册机构的物理场地也需要有足够的安全措施，保证只有授权的人员才能进入，只有授权的人员才能接触系统进行证书管理。

5.2 过程控制

5.2.1 可信角色

ZJCA 的可信人员包括:

- 鉴证和客户服务人员
- 安全管理人员
- 密钥与密码设备管理人员
- 加密设备操作人员
- 系统管理员
- 人力资源管理人员
- 掌握 CA 密钥共享的人员
- 能够进入三层以上工作区域的人员

5.2.2 每项任务需要的人数

ZJCA 有严格策略和控制程序，以保障基于工作性质的职责分离。最敏感的操作要求多名可信人员共同参与完成。

1) 鉴别和签发证书，要求 2 个可信人员的参与

访问 CA 密钥离线生成室和 CA 密钥离线存放室，至少两名有访问权限的人员。

2) 掌管密钥共享，至少 5 人

操作存放有 CA 密钥的密码设备，包括密钥生成、分配、备份、销毁等，至少需要 3 个密钥共享持有人，一个密钥管理员，一个见证人。

5.2.3 每个角色的识别与鉴别

对于物理访问控制，ZJCA 通过门禁磁卡、指纹识别鉴别不同人员，并确定相应的权限。

对于进行证书生命周期管理的 ZJCA 及注册机构证书管理员，需使用相应的数字证书访问认证系统、注册机构系统，完成证书管理工作。

对于系统维护人员，需使用安全的身份鉴别机制进入认证系统进行维护工作。

5.2.4 需要职责分割的角色

所谓职责分割，是指限制某些岗位由同一组人员兼任的安全要求。ZJCA 对如下人员进行了职责分割:

- 密钥管理员
- 安全经理
- 证书申请鉴别人员
- 网络安全管理人员
- 财务管理人员
- 安全策略委员会主任

5.3 人员控制

5.3.1 资格、经历和无过失要求

在 ZJCA 中担任一定角色、执行一定功能、完成一定工作的人员，其所受教育、培训及工作经历应足够胜任其工作。

ZJCA 客户服务人员必须受过专门的客户服务技能培训，通过 PKI 及相关应用基本知识培训，熟悉有关证书业务，考试通过后方能进行有关工作。这些培训和考试由 ZJCA 负责。

ZJCA 安全管理人员必须熟悉、掌握有关的安全知识和安全管理，熟悉 ZJCA 安全要求，熟悉 ZJCA 安全与审计指南，有很强的责任感。为了达到此要求，ZJCA 将对安全管理人员进行培训。

ZJCA 密钥与密码设备管理人员必须熟悉 PKI 基本知识，熟悉 CA 证书和密钥相关的证书，如 CA 证书的产生、签发、更新、密钥更新等，熟悉有关密码设备操作使用。

ZJCA 所有的可信人员必须符合清白要求：没有伪造教育、工作经历，没有违法犯罪记录，工作中没有严重的不诚实行为。

5.3.2 背景审查程序

为了确保担任可信角色的人员能够胜任有关工作，ZJCA 将对雇佣的人员先进行背景调查。在成为 ZJCA 的可信人员前，有关人员必须提交相关材料，以证明他们能够胜任预期的工作。

ZJCA 依据有关材料进行背景调查，在调查过程中，ZJCA 将为有关人员保密，

保护其隐私。背景调查时如果出现提交材料与事实不符或证明提交材料为捏造时，ZJCA 将拒绝可信职位候选人获得有关职位或取消其可信人员的资格。

5.3.3 培训要求

为了使有关人员能胜任其承担的工作，ZJCA 对所有入职员工制定有专门的培训计划，培训内容包括：

- 本人工作职责
- 安全管理要求及制度
- 事故和安全威胁的报告和处理

对于销售、服务和支持还包括：

- PKI 及应用。
- ZJCA 的产品与服务。
- 客户服务流程与要求（客户服务）。
- 安全操作流程（系统、密钥）。

5.3.4 再培训周期和要求

ZJCA 根据业务需要安排。

5.3.5 工作岗位轮换周期和顺序

内部安排。

5.3.6 未授权行为的处罚

ZJCA 对于未授权行为或其他违反公司安全策略和程序的行为制定有相应的处罚措施，包括警告、罚款直至辞退，情节严重的将依法追究刑事责任。

5.3.7 独立合约人的要求

在有限制的情况下，独立合约人或顾问可以担任可信职位。任何合约人或顾问在某一职务的职能和安全标准应与相应职位的内部雇员一样。

担任可信角色的独立合约人和顾问需要通过本《通用证书策略》5.3.2 中所述的背景调查程序，否则，他们不能担任可信角色，当进入敏感区时，只能在认证机构人员的陪同和直接监督下访问认证机构的安全设施，完成有关的工作。

5.3.8 提供给员工的文档

提供给员工的文档通常包括员工培训资料及员工工作手册，这些资料通常是不公

开的。

5.4 审计日志程序

5.4.1 记录事件的类型

ZJCA 对如下几类事件进行记录:

1) CA 密钥生命周期内的管理事件，包括:

- 密钥生成，备份，存储，恢复，归档和销毁。
- 密码设备生命周期的管理事件，例如接收、使用、卸载和弃用。

这些记录都是由相关人员完成的纸质或电子记录。

2) CA 和订户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。
- 成功或失败的证书操作。

这些记录由认证系统自动记录，保存在数据库。

3) 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 系统的非授权访问及访问企图。
- 系统崩溃，硬件故障和其他异常。
- 防火墙和 IDS 记录的安全事件。

这些记录由操作系统自动完成，ZJCA 的系统维护人员会定期检查系统日志。

4) ZJCA 物理设施的访问，包括:

- 授权人员进出。
- 非授权人员进出及陪同人。
- 安全存储设施（离线密钥）的访问。

授权人员进出物理设施由 ZJCA 物理场地的访问控制系统自动记录。非授权人员进出由陪同人员作纸质记录。

5) 日志记录，包括:

- 每个日志记录的日期和时间。
- 对于自动日志记录，登记的序列号或序号。
- 记录日志的实体的身份。
- 日志记录的种类。

- 日志记录的种类。

6）可信人员管理记录，包括且不限于：

- 认证服务系统的操作员、管理员等账号申请、变更、权限分配记录。
- 人员情况变化记录。

5.4.2 处理日志的周期

对于 CA 和订户证书生命周期内的管理事件日志，ZJCA 将一个月进行一次内部检查、审计。

系统安全事件和系统操作事件日志，ZJCA 将每周进行一次检查、处理。

ZJCA 物理设施的访问日志，ZJCA 将每月进行一次检查、处理。

5.4.3 审计日志保存期限

与证书相关的审计日志，在证书失效后至少保留 5 年。

5.4.4 审计日志的保护

ZJCA 采取了物理和逻辑的访问控制方法，防止未经授权而浏览、修改、删除或其他方式篡改电子或纸质审计日志文件。

5.4.5 审计日志备份程序

对于认证系统的日志，ZJCA 定期进行备份。

5.4.6 审计收集系统

对于电子审计信息，ZJCA 设置了专门的审计信息存储系统，自动或人工完成审计信息的收集。对于纸质的审计信息，则有专门的文件管理柜来实现审计信息的收集。

5.4.7 对导致事件主体的通知

当审计记录报告一个事件时，ZJCA 会立即通知引起该事件的个人、组织机构。

5.4.8 脆弱性评估

根据审计记录，ZJCA 定期进行系统、物理场地、运营管理、人事管理等方面的安全脆弱性评估，并根据评估报告采取措施。

5.5 记录归档

5.5.1 归档记录的类型

ZJCA 归档下列信息：

- 审计记录的归档依据本《通用证书策略》5.4.1 要求
- 证书申请信息
- 证书签发过程中的支持文档
- 证书生命周期的相关信息

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。

对订户证书生命周期内的管理事件的归档，证书失效后保留时间不少于 5 年。

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。

订户证书的归档保留期限不少于证书失效后 5 年。

CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，额外保留 5 年。

5.5.3 归档文件的保护

ZJCA 对各种电子、磁带、纸质形式的归档文件，都有安全的物理和逻辑保护措施和严格的管理程序，确保归档了的文件不会被损坏，防止非授权的访问、修改、删除或其它的篡改行为。

5.5.4 归档文件的备份程序

所有归档的文件和数据除了保存在 ZJCA 的主要存储库，对于认为必要的资料，还将在异地保存其备份。归档的数据库一般采用物理或逻辑隔离的方式，与外界不发生信息交互。只有授权的工作人员才能在监督的情况下，对档案进行读取操作。ZJCA 在安全机制上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

ZJCA 对每项日志有时间记录。对于纸质记录，有操作人员手工记录；对于电子记录，由系统自动增加时间或采用时间戳技术。

5.5.6 归档收集系统

ZJCA 认证服务系统的归档信息，全部由 ZJCA 内部的工作人员或具有安全控制措施的内部系统、按照人工和自动操作两部分进行产生和收集，并且由具备相关权限的人进行管理和分类。

5.5.7 获得和检验归档信息的程序

只有可信人员才可以查看和获得归档信息，这些信息被归还时必须得到验证。

5.6 CA 密钥变更

当 CA 密钥对的累计寿命超过本《通用证书策略》6.3.2 中规定的最大生命期，ZJCA 将启动密钥更新流程，替换已经过期的 CA 密钥对。ZJCA 密钥变更按如下方式进行：

1) 一个上级 CA 将在其私钥到期时间小于下级 CA 的生命期之前停止签发新的下级 CA 证书（“停止签发日期”）；
2) 产生新的密钥对，签发新的上级 CA 证书；
3) 在“停止签发证书的日期”之后，对于批准的下级 CA（或订户）的证书请求，将采用新的 CA 密钥签发证书；
4) 上级 CA 继续利用原来的 CA 私钥签发 CRL 直到利用原私钥签发的最后的证书过期为止。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

ZJCA 已制定各种应急处理方案，规定了相应的事故和损害处理程序，这些应急处理方案有：

- 认证系统应急方案
- 电力系统应急方案
- 消防应急方案
- 网络与信息系统应急方案
- 安全事故应急处理方案等。

5.7.2 计算机资源、软件和/或数据的损坏

ZJCA 对业务系统及其他重要系统的资源、软件和/或数据进行了备份，并制定了相应的应急处理流程，当出现计算机资源、软件和/或数据的损坏时在最短的时间内恢复被损害的资源、软件和/或数据。

5.7.3 实体私钥损害处理程序

对于实体私钥的损害，ZJCA 有如下处理要求和程序：

1）当证书订户发现实体证书私钥损害时，订户必须立即停止使用其私钥，并立即通过电话的方式通知 ZJCA 或注册机构吊销其证书。

2）当 ZJCA 或注册机构发现证书订户的实体私钥受到损害时，ZJCA 或注册机构将立即吊销证书，并通知证书订户，订户必须立即停止使用其私钥。发布证书吊销信息。

3）当 ZJCA 或注册机构的 CA 证书出现私钥损害时，ZJCA 将立即吊销 CA 证书并及时通过广达的途径通知依赖方，然后生成新的 CA 密钥对、签发新的 CA 证书。

5.7.4 灾难后的业务存续能力

ZJCA 异地保存了系统数据备份系统，在物理场地或系统数据出现重大灾难时，能够根据需要尽快恢复其业务。

5.8 电子认证服务机构或注册机构的终止

当 ZJCA 及其注册机构需要停止其业务时，将会严格按照《中华人民共和国电子签名法》及相关法规中对认证机构中止业务的规定要求进行有关工作。

6 技术安全控制

6.1 密钥对的产生和安装

6.1.1 密钥对的产生

6.1.1.1 电子认证服务机构的密钥的生成

对于 ZJCA 的密钥的生成，ZJCA 专门的密钥管理员及若干名接受过相关培训的可信雇员在 ZJCA 安全设施中的密钥生成室，按照 ZJCA 的密钥管理策略中规定的密钥生成规程进行产生。ZJCA 的密钥生成规程规定了 CA 密钥产生的流程控制及参加人员。ZJCA 的密钥对采用密码硬件实现，所使用的生成及保存的密码模块（含密钥生成算法芯片）符合国家密码主管部门的要求，并通过国家密码主管部门的鉴定。

6.1.1.2 订户密钥的生成

订户的签名密钥由订户的密码设备（如智能密码钥匙或 IC 卡）、或等同安全等级的密码模块生成，加密密钥对由密钥管理中心生成。

6.1.2 私钥传送给订户

订户的签名密钥对由自己的密码设备或密码模块生成并保管。加密密钥对由密钥管理中心产生，以密钥信封的密文形式、通过安全通道安装到订户的密码设备或密码模块中。

6.1.3 提交公钥给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到 CA。

从注册机构到 CA、以及从密码管理中到 CA 的传递过程中，采用国家密码管理部门许可的通信协议及密码算法，保证了传输中数据的安全。

6.1.4 传送电子认证服务机构公钥给依赖方

对于 ZJCA 的主 CA 公钥，通过如下方式之一传输给依赖方：

1）依赖方访问 ZJCA 的证书服务站点下载 CA 证书，该站点受到服务器证书的保护；

2）依赖方访问 ZJCA 的信息库；

3）ZJCA、注册机构或其合作伙伴到依赖方业务系统现场将 CA 证书安装到业务系统中；

4）ZJCA、注册机构或其合作伙伴通过签名电子邮件将CA证书传输给依赖方；

5）ZJCA、注册机构或其合作伙伴分发给依赖方的软件中绑定、包含有CA证书。

对于ZJCA的其他CA公钥，除了上面所述的方式传输给依赖方外，当证书订户获取证书时ZJCA通过PKCS#7格式将除根证书外的证书链传递给订户。

6.1.5 密钥的长度

密钥算法和长度符合国家密码主管部门的规定。

6.1.6 公钥参数的生成和质量检查

符合国家密码管理部门的要求。

6.1.7 密钥使用目的

主CA的密钥用于签发运营CA的证书及CRL，运营CA的密钥用于签发订户证书。

订户证书的使用目的需满足本《通用证书策略》的要求。

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

ZJCA使用国家密码管理部门认可、批准的硬件密码模块生成主CA、证书签发CA和其他CA密钥对和存储CA私钥。ZJCA制定有专门密码管理策略，在从运送、验收、初始化、离线存放、在线使用到销毁的整个密码设备生命周期内，对密码模块进行管理和控制。CA密码模块离线存放在CA密钥离线存放区中，CA密码模块在线放置在屏蔽机房或机柜中。CA密码设备的操作遵从多人在场、多人控制的原则。

ZJCA要求通用型证书的订户采用符合国家密码管理部门认可的、符合安全要求的硬件设备（如：智能密码钥匙、IC卡）或密码模块来存放证书和密钥。

6.2.2 私钥多人控制

ZJCA的各类CA私钥存放在符合安全要求的加密机中，该加密机启动的密钥被分割保存在5个智能密码钥匙或IC卡中（称为密钥共享），这5个智能密码钥匙或IC卡由ZJCA的5名可信雇员持有（称为密钥分管者），保存ZJCA内部保险盒中。当要操作使用CA私钥时（离线），需要3名密钥管理者持有密钥共享智能密码钥匙或IC卡才能启动加密卡。

订户的私钥由订户通过密码设备或密码模块的密码、口令来单独控制。

6.2.3 私钥托管

ZJCA 所有 CA（包括主 CA 和运营 CA）的私钥均未托管。

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。订户加密证书对应的私钥由密钥管理中心托管，密钥管理中心严格保证订户密钥对的安全，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。

6.2.4 私钥备份

6.2.4.1 电子认证服务机构私钥的备份

ZJCA 对 CA 私钥通过专门的备份加密卡进行备份，这些备份分别作为本地常规备份和异地灾难恢复备份。

6.2.4.2 订户私钥备份

ZJCA 的密钥管理中心对订户的加密私钥进行备份存储，备份数据以密文形式存在。

6.2.5 私钥归档

当 ZJCA 的 CA 密钥对超过使用期后，这些 CA 密钥对将归档保存至少 5 年。归档 CA 密钥对保存在本《通用证书策略》6.2.1 所述的硬件密码模块中，并且 ZJCA 的密钥管理策略和流程阻止归档 CA 密钥对返回到产品系统中。对归档私钥到了归档保存期，ZJCA 将对其进行销毁。

订户的私钥不作归档处理。

6.2.6 私钥导入、导出密码模块

ZJCA 的 CA 密钥对在硬件密码模块上生成，保存和使用。此外，为了常规恢复和灾难恢复，ZJCA 对 CA 密钥进行复制。当 CA 密钥对从一个硬件密码模块复制到另一个硬件密码模块上时，被复制的密钥对以加密的形式在模块之间传送，并且在传递前要进行模块间的相互身份鉴别。另外 ZJCA 还有严格的密钥管理流程对 CA 密钥对复制进行控制。所有这些有效防止了 CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

订户的签名私钥由订户使用符合安全要求的密码设备或密码模块生成，保存和使用，无法导出。订户的加密私钥按 ZJCA 的业务流程、以密钥信封的密文形式安全导入到订户的密码设备或密码模块中，导入后无法从密码模块中导出。

6.2.7 私钥在密码模块中的存储

私钥以加密的形式存放在符合安全要求的密码硬件或密码模块中,并只能在该密码硬件或密码模块中使用。

6.2.8 激活私钥的方法

ZJCA 的 CA 私钥激活，需要具有激活私钥权限的管理员使用含有自己的身份的智能密码钥匙或 IC 卡登录，启动密钥管理程序，进行激活私钥的操作，需要 3 名管理员以上同时在场。

订户的证书私钥存放在符合安全要求的密码设备或密码模块中,采用 PIN 码(口令）进行激活。

6.2.9 解除私钥激活状态的方法

对于 ZJCA 的 CA 私钥，当存放私钥的硬件密码模块断电,私钥进入非激活状态。

订户的私钥可通过密码介质断电、或退出密码模块等方法解除激活状态。

6.2.10 销毁私钥的方法

ZJCA 的 CA 私钥在生命周期结束后,ZJCA 将 CA 私钥继续保存在一个备份硬件密码模块中，并进行归档，其他的 CA 私钥备份被安全销毁。归档的 CA 私钥在其归档期限结束后,需在多名可信人员参与的情况下安全销毁。CA 私钥的销毁将确保 CA 私钥从硬件密码模块中彻底删除，不留有任何残余信息。

订户的证书私钥，在其生命周期结束后，订户应按照存储私钥的密码设备或密码模块的说明完成销毁。订户在销毁私钥前，须自行确认是否还有信息需要加密私钥进行解密。由于订户销毁私钥导致的原有信息无法解密的后果，需由订户自行承担，ZJCA 不承担任何责任。

6.2.11 密码模块安全要求

ZJCA 使用服务器密码机，均具有国家密码主管部门颁发的商用密码产品认证证书，符合国家有关标准。

ZJCA 要求订户采用具有国家密码主管部门颁发的商用密码产品认证证书的密码设备（如：智能密码钥匙）和密码模块来存放证书和密钥，以确保其密钥的安全性。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

对于生命周期外的 CA 和订户证书，ZJCA 将进行归档，归档的证书存放在指定数据库中。

6.3.2 证书操作期和密钥对使用期限

对于通用型证书，订户密钥对的使用期限与证书有效期保持一致。

6.4 激活数据

6.4.1 激活数据的产生和安装

存放有 ZJCA 的 CA 私钥的设备的激活信息（密钥共享），其产生按 ZJCA 密钥生成规程中的规定进行。所有密钥共享的创建和分发有相应的记录，包括产生时间、持有人等信息。ZJCA 的 CA 私钥的激活数据由硬件设备内部产生，并分割保存在 5 个智能密码钥匙或 IC 卡中，需通过专门的读卡设备和软件读取。

订户证书和密钥存储在密码设备（如：智能密码钥匙）或密码模块中，激活数据为 PIN 码（口令），由订户在初始化密码设备或密码模块时自行设置。ZJCA 要求订户设置的 PIN 码（口令）长度不少于 6 位字符（英文字母或数字）。

6.4.2 激活数据的保护

ZJCA 的 CA 私钥激活数据存放在 5 个智能密码钥匙或 IC 卡中，由 5 个不同的可信人员持有，而且持有人员必须符合职责分割的要求，签署协议确认他们知悉密钥分管者责任。密钥共享必须存放在保险盒中。

证书订户使用 PIN 码（口令）激活和保护私钥，订户应妥善保管好其 PIN 码（口令），防止泄露或窃取。

6.4.3 激活数据的其他方面

6.4.3.1 激活数据的传送

保存 ZJCA 的 CA 私钥激活数据的智能密码钥匙或 IC 卡，通常保存在 ZJCA 的安全设施中，不能携带外出或传送。如因某种特殊情况确实需要传送时，其传送过程需在 ZJCA 安全管理人员和密钥管理人员的监督下进行。

当订户证书私钥的激活数据需要进行传送时，订户应保护它们在传送过程中免于

丢失、偷窃、修改、非授权泄露、或非授权使用。

6.4.3.2 激活数据的销毁

保存 ZJCA 的 CA 私钥激活数据的智能密码钥匙或 IC 卡，其销毁所采取的方法包括将智能密码钥匙初始化，或者彻底销毁智能密码钥匙或 IC 卡，无论采取何种方式，都将保证不会残留有任何密钥信息。CA 私钥激活数据的销毁是在 ZJCA 安全管理人员和密钥管理人员的监督下进行。

当订户证书私钥的激活数据不需要时应该销毁，订户应该确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部，比如记录有 PIN 码（口令）的纸张必须粉碎。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

ZJCA 的证书认证系统主机实现了自主访问控制（DAC），进行了安全漏洞扫描和安全优化，安装了防病毒系统，确保了包含 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。此外，认证机构只允许有工作需求的必要人员访问产品服务器，一般的应用用户在产品服务器上没有账户。

认证机构的生产系统网络与其它部分逻辑分离，并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，只有认证机构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直接访问认证系统数据库。

6.5.2 计算机安全评估

ZJCA 的 CA 系统及其运营环境符合国家密码管理局的安全保障要求。

6.6 生命周期技术控制

6.6.1 系统开发控制

ZJCA 通过内部流程来控制证书认证系统的研发工作，并确保该系统安装的可靠性。

6.6.2 安全管理控制

ZJCA 已制定了各种安全策略、管理制度与流程对 CA 运营系统进行安全管理。

6.6.3 生命期的安全控制

ZJCA 的证书认证系统在系统设计过程中充分进行了安全性考虑，完全依据国家有关标准进行严格设计，使用的算法和密码设备均通过了主管部门鉴定。在开发过程中有严格的流程进行代码安全管理，在开发完成后进行了严格的安全测试，在正式使用前通过了国家有关部门的系统安全性审查。在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。

6.7 网络的安全控制

ZJCA 证书认证系统网络进行安全漏洞扫描和安全优化，部署了防火墙、入侵检测系统，并在系统通信过程中使用加密和电子签名进行保护。

6.8 时间戳

ZJCA 根据系统安全管理和控制的要求，会决定是否使用时间戳。根据不同数据对时间的敏感性、严密性和逻辑关系的要求，ZJCA 将会确定时间戳服务的有关规定和策略。

7. 证书、CRL 和 OCSP

7.1 证书

ZJCA 签发的证书均符合 X.509 V3 证书格式，遵循 RFC3280 标准。

7.1.1 版本号

ZJCA 签发的证书符合 X.509 V3 标准。

7.1.2 证书扩展项

根据具体的应用需求，ZJCA 签发的证书除使用 IETF RFC 3280 中定义的证书扩展项外，还支持私有（非关键）扩展项，不能识别私有（非关键）扩展项的应用、依赖方可以忽略该扩展项。

ZJCA 采用的 IETF RFC 3280 中定义的证书扩展项：

- 颁发机构密钥标识符 Authority Key Identifier
- 主体密钥标识符 Subject Key Identifier
- 密钥用法 Key Usage
- 扩展密钥用途 Extended Key Usage
- 私有密钥使用期 Private Key Usage Period
- 主体可选替换名称 Subject Alternative Name
- 基本限制 Basic Constraints
- 证书吊销列表分发点 CRL Distribution Points

私有扩展项可支持以下类型：

- 个人身份证号码 Identify Card Number
- 营业执照（统一社会信用代码）IC Registration Number

7.1.3 算法对象标识符

ZJCA 签发的证书中使用的对象标识符，符合国家密码主管部门批准的算法对象标识符。

7.1.4 名称形式

ZJCA 数字证书中的主体 Subject 的 X.500DN 是 C=CN 命名空间下的 X.500 目录唯一名字，各属性的编码一律使用 UTF8 编码。

主体 Subject 的 X.500DN 支持多级 O 和 OU，其格式如下：

C=CN;

O=XX

O=XX

OU=XX;

OU=XX;

CN=XX

- C（Country）应为 CN，表示中国。
- O（Organization）中的内容分为两种：

a) 代表证书持有者所在的组织机构；

b) 代表证书签发机构。

- OU（Organization Unit）中的内容根据 O 中的内容分为两种：

a) O 采用其 a)中所述内容时，OU 代表证书持有者所在的部门；

b) O 采用其 b)中所述内容时，OU 代表签发机构中的部门或服务类（如 CN Individual Comsumer Service Center）。

- CN（Common Name）中的内容分为 4 种：

a) 个人证书中应为证书主体的姓名；

b) 机构证书中应为证书主体单位的标准全称或标准简称；

c) 设备证书中应为证书主体设备的域名或者 IP 地址或者设备编码；

d) 代码签名证书中应为负责人的姓名，或所属单位的标准全称或简称。

- Email 仅在邮件证书中的 DN 中存在，应为证书主体的有效电子邮件地址。

7.1.5 证书策略对象标识符

当 ZJCA 签发的通用证书中包含了证书策略扩展项时，该扩展项中的对象标识符与本《通用证书策略》的对象标识符相对应。

7.1.6 关键证书策略扩展项的处理规则

当 ZJCA 签发的通用证书中标记为“关键”的扩展项不能识别时，依赖方理应拒绝处理该证书，并告知 ZJCA 或授权的注册机构、受理点等服务机构。

7.2 证书吊销列表

7.2.1 版本号

ZJCA 定期签发 CRL（证书废除列表），其所签发的 CRL 遵循 RFC3280 标准。采用 X.509 V2 格式。

7.2.2CRL 和 CRL 条目扩展项

CRL 扩展项：颁发机构密钥标识符 Authority Key Identifier。

CRL 条目扩展项：不使用 CRL 条目扩展项。

7.3 在线证书状态协议

7.3.1 版本号

使用 OCSP 版本 1（OCSP v1）。

7.3.2OCSP 扩展项

ZJCA OCSP 不支持扩展项。

8 一致性审计和其他评估

8.1 评估的频率或情形

审计是为了检查和监督 ZJCA 及其下属机构或其它授权的关联机构，是否依据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《通用证书策略》和《ZJCA 电子认证业务规则》的要求，依法开展电子认证服务业务，以及在开展业务过程中，是否存在违反其它法律法规与 ZJCA 的业务规范、管理制度、安全策略等情况，以达到规避经营风险、提高服务质量、保障客户权益的目的。

审计分为外部审计与内部审计:

外部审计是由法律规定的主管部门、主管部门委托的第三方机构或 ZJCA 委托的第三方机构对自身的电子认证服务业务进行审计与评估。审计内容、评估标准及审计评估结果是否公开由主管部门确定。

外部审计原则上每年执行一次。

内部审计是指 ZJCA 自行组织人员对机构内部、下属机构等进行审计评估，审计结果供 ZJCA 内部用以完善管理、改进服务，不需对外公开。

内部审计按 ZJCA 自身需求确定其频率。

8.2 评估者的资质

内部审计人员的资质要求:

- 具备认证机构、信息安全审计的相关知识。
- 具有两年以上的相关经验，并熟悉本《通用证书策略》和 ZJCA《电子认证业务规则》的相关规范。
- 具备计算机、网络、信息安全等方面的知识和实际工作经验。

外部审计的审计人员的资质，由主管部门或第三方确定。

8.3 评估者与被评估者的关系

评估者应是与被评估者无任何业务、财务往来或其他足以影响评估客观性的利害关系的机构或组织。

8.4 评估内容

评估内容包括：CA 物理环境和控制、CA 基础控制、密钥管理操作、证书生命

周期管理、CA 业务规则、CPS 执行情况。

8.5 对问题与不足采取的措施

ZJCA 管理层将对审计报告进行评估，对于在审计中发现的重大以外或不作为采取行动。根据审计中发现的意外或不作为对证书体系的安全或完整性的危险程度制定相应的改动计划，必须在 30 天内制定改正行动计划，并在合理的期限内执行它。

8.6 评估结果的传达与发布

除非法律明确要求，ZJCA 一般不公开审计结果。

在必要的情况下，向 ZJCA 关联单位（例如垫付商、注册机构、审核受理点）通知审计结果的具体规定将在 ZJCA 和关联单位的协议中写明。

9 业务和法律事务

9.1 费用

9.1.1 证书签发和更新费用

ZJCA 对通用证书的服务收取费用，其价格由 ZJCA 与依赖方或订户的协议、合同确定。

9.1.2 证书查询费用

依赖方和订户使用公开的方式查询资料库，暂不收取查询费用。

如依赖方或订户需要定制化的证书查询服务，由 ZJCA 和依赖方或订户在协议中约定。

9.1.3 吊销或状态信息查询费用

通过 CRL 查询证书是否吊销，ZJCA 暂不收取信息访问费用。

对于在线证书状态查询(OCSP)，由 ZJCA 与依赖方或订户在协议中约定。

9.1.4 其他服务的费用

ZJCA 如提供证书恢复、密钥恢复、签名验证以及各类通知等相关服务，需要收取服务费用，ZJCA 将通过但并不限于网站、《电子认证业务规则》或订户协议及依赖方协议等方式予以告知。

如依赖方或订户需要 ZJCA 出具电子签名验证报告等材料，其费用在签订的协议中约定。

9.1.5 退款策略

在实施证书操作和签发证书的过程中，ZJCA 和授权的注册机构、受理点遵守并保持严格的操作程序和策略。一旦订户接受数字证书，ZJCA 将不办理退证、退款手续。

如果订户在证书服务期内退出数字证书服务体系，ZJCA 将不退还剩余时间的服务费用。

9.2 财务责任

9.2.1 保险的范围

ZJCA 根据业务发展情况和国内保险公司的业务开展情况决定其投保策略。

9.2.2 其他资产

无规定。

9.2.3 保险或担保对最终实体的覆盖

根据《中华人民共和国电子签名法》的规定，订户在此同意：由于 ZJCA 的责任给订户造成的直接损失，ZJCA 将根据使用证书的种类，承诺赔偿订户一定金额的直接损失。具体的情况及赔付额度，参见本《通用证书策略》的 9.9 之规定。

9.3 保密信息

9.3.1 保密信息范围

系统方面：认证系统结构、配置，包括系统、网络、数据库等；认证系统安全策略和方案；系统操作、维护记录；各类系统操作口令。

运营管理方面：物理安全策略与实施方案，包括场地、访问控制、入侵检测等实施方案；密钥管理策略与操作记录；CA 或 RA 批准或拒绝的申请纪录；可信人员名单；内部安全管理策略与制度。

客户信息：客户的注册信息；客户系统、应用访问 CRL 的记录（时间、频度）；客户与认证机构、注册机构签订的协议；

9.3.2 不属于保密的信息

证书策略、认证业务声明、依赖方协议、订户协议等。

订户证书的相关信息可以通过 ZJCA 的信息库等方式对外公布。

9.3.3 保护保密信息的责任

ZJCA 通过有效的技术手段和管理程序，保护商业的和客户的保密信息。ZJCA 的每个员工都要接收信息保密方面的培训。

当 ZJCA 在任何法律、法规或规章的要求下，或在法院的要求下必须提供本《通用证书策略》或 ZJCA《电子认证业务规则》中具有保密性质的信息时，ZJCA 应按照要求向执法部门公布相关的保密信息，ZJCA 无须承担任何责任，这种提供不被视为违反了保密的要求和义务。

9.4 个人隐私保密

9.4.1 隐私保密计划

认证机构应制定隐私保密计划对证书订户的个人信息保密。隐私保密计划遵守现行的法律和法规。

9.4.2 作为隐私处理的信息

作为隐私处理的信息包括，订户注册申请证书中提交的信息，包括联系电话、地址等；个人与 ZJCA 或授权的注册机构、受理点和依赖方签订的协议。

9.4.3 不被认为隐私的信息

出现在证书中的信息；证书及证书状态。

9.4.4 保护隐私的责任

ZJCA 和授权的注册机构、受理点和依赖方在没有获得客户授权的情况下，不得将客户隐私信息透露给第三方。但在法律法规或公共权力部门通过合法程序要求下，ZJCA 可以向特定的对象公布隐私信息，ZJCA 无需承担由此造成的任何责任。

9.4.5 使用隐私信息的告知与同意

ZJCA 和授权的注册机构、受理点和依赖方如果需要将客户隐私信息用于业务范围内，无论是否涉及到隐私，ZJCA 均可以不用告知订户；但在用于双方约定的用途以外的目的，则需要事先告知客户并获得客户同意和授权，而且这种同意和授权是要用可归档的方式（如传真、信函、电子邮件等）。

9.4.6 依法律或行政程序的信息披露

由于法律执行、法律授权的行政执行的需要，ZJCA 和授权的注册机构、受理点和依赖方将有关信息在客户知晓或不知晓的情况下提供有关执法机关、行政执行机关是允许的，即使这样，ZJCA 和授权的注册机构、受理点和依赖方也应尽可能地保护客户隐私信息。

9.4.7 其他信息披露情形

ZJCA、订户、注册机构、依赖方等机构或个人都有义务按照本《通用证书策略》的规定，承担相应的保护隐私责任。ZJCA、订户、注册机构、依赖方等机构或个人对其他信息的披露受制于法律、订户协议。

9.5 知识产权

9.5.1 证书和吊销信息中的知识产权

ZJCA 对它签发的证书、证书吊销列表及其中信息的拥有知识产权。

9.5.2 CP 中的知识产权

ZJCA 对本《通用证书策略》拥有知识产权。

9.5.3 命名中的知识产权

证书订户对证书注册信息及签发给他的证书中包含的商标、服务标志或商品名和甄别名拥有知识产权。

9.5.4 密钥和密钥材料的知识产权

证书中的密钥对是证书中主题对应实体或实体拥有者的知识产权。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

订户同意订户协议是作为订户注册申请的一个条件，依赖方同意依赖方协议作为接收证书及状态信息的一个条件。同样地，ZJCA 必须按要求使用订户协议和依赖方协议。ZJCA 不负责评估证书是否被恰当使用，订户和依赖方必须依订户协议和依赖方协议确保证书用于允许使的目的。ZJCA 和订户之间的担保、免责和有限责任由他们之间的协议规定和约束。

ZJCA 在提供电子认证服务活动过程中对订户做出的承诺如下:

1) ZJCA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受工业和信息化部的领导，对签发的数字证书承担相应的法律责任;
2) ZJCA 保证使用的系统及密码符合国家政策与标准，保证其 ZJCA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定;
3) ZJCA 签发给订户的证书符合本《通用证书策略》的所有实质性的要求;
4) 吊销服务和信息库的使用在所有方面符合本《通用证书策略》的要求;
5) 证书中不存在批准证书申请或签发证书的实体已知的对事实的实质性错误描述，或来自于这些实体的错误信息;
6) 在管理证书申请或制造证书时，批准证书申请或签发证书的实体不会因为工

作疏忽将错误信息包含到了证书中。

ZJCA 在提供电子认证服务活动过程中对依赖方做出的承诺如下:

1) 除了未经鉴别的订户信息外，包含在证书中的所有信息都是准确的;
2) 在 ZJCA 信息库中发布的证书已经签发给了个人或组织机构（它们的名字包含在证书中），订户已经根据接收了该证书;
3) 批准证书申请或签发证书的实体签发证书时完全遵守了本《通用证书策略》的规定。

9.6.2 注册机构的陈述与担保

ZJCA 授权的注册机构、受理点、依赖方在参与电子认证服务过程中的承诺如下:

1) 提供给证书订户的注册过程完全符合 ZJCA 的《电子认证业务规则》的所有实质性要求;
2) 在 ZJCA 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人的信息不一致;
3) 注册机构将按 ZJCA 的《电子认证业务规则》的规定，及时向 ZJCA 提交证书申请、吊销、更新等服务请求;
4) 授权的注册机构、受理点、依赖方有义务通知订户阅读本《通用证书策略》和 ZJCA《电子认证业务规则》以及相关用户协议。

9.6.3 订户的陈述与担保

订户一旦接受 ZJCA 签发的证书，就被视为向 ZJCA 和授权的注册机构、受理点、依赖方做出如下承诺:

1) 订户需熟悉本《通用证书策略》、ZJCA《电子认证业务规则》以及订户协议，还需遵守本《通用证书策略》对证书使用方面的有关限制;
2) 订户在证书申请表上填写的所有声明和信息必须是完整的、真实的和正确的，可供 ZJCA 和授权的注册机构、受理点、依赖方检查和核实;
3) 订户应当妥善保护好自己的私钥，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的发生;
4) 私钥仅为订户自身访问和使用，订户对使用私钥的行为负责;
5) 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄露以及其他情况，订户应立刻通知 ZJCA 和授权的注册机构、受理点、依赖方，申请

采取吊销等处理措施；

6) 订户已知其证书被冒用、破解或被其他人非法使用时，应及时通知 ZJCA 和授权的注册机构、受理点、依赖方吊销其证书。

9.6.4 依赖方的陈述与担保

在任何信赖行为发生之前，依赖方必须熟悉本《通用证书策略》、ZJCA《电子认证业务规则》的条款以及依赖方协议，独立评估证书使用于任何目的适当性，并确定证书将会被恰当使用于本《通用证书策略》所规定的目的。

依赖方在信赖订户的数字证书前，必须采取合理步骤，查证订户数字证书及数字签名的有效性。

所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解《通用证书策略》和 ZJCA《电子认证业务规则》的有关条款。

9.6.5 其他参入者的陈述与担保

其他参与者的陈述与担保同 9.6.4。

9.7 担保免责

有下列情况之一的，应当免除 ZJCA 之责任。

1) 由于证书申请人或订户故意提供或未按照要求提供不准确、不真实、不完整的信息而获得 ZJCA 签发的证书，订户在使用该证书时引起的责任；
2) ZJCA 不承担任何其他未经授权的人或组织以 ZJCA 名义编写、发表或散布的不可信赖的信息所引起的法律责任；
3) 由于非 ZJCA 原因造成的设备故障、网络中断导致证书报错、交易中断或其他事故造成的损失责任；
4) ZJCA 对各类证书的适用范围作了规定，若证书被超范围使用或被用于其他不被允许的用途，ZJCA 向任何相关方承担赔偿和/或补偿责任；
5) ZJCA 在法律许可的范围内，根据有关法律法规的要求，如实提供电子交易和网络交易中产生的电子签名的验证信息，但对此不承担法律或政策之外的责任；
6) ZJCA 与授权的外部注册机构、受理点或依赖方签署合同，合同条款中明确注册机构、受理点或依赖方承担订户身份核实责任。对于明显由于外部注册机构、受理点或依赖方的越权行为或其他过错行为所引发的违反约定义务而

对订户造成的损失，由授权的外部注册机构、受理点或依赖方承担；

7) 由于不可抗力因素导致ZJCA暂停、终止部分或全部证书服务，ZJCA不承担赔偿责任。

9.8 有限责任

在法律允许的范围内，ZJCA订户协议、依赖方协议和其他订户协议限制认证机构承担的责任。责任限制包括排除间接的、特殊意外造成的、偶然的和后续性的损失。

ZJCA在与订户和依赖方签订的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

9.9 赔偿

9.9.1 赔偿范围

在电子认证活动中产生的赔偿，都以本《通用证书策略》或ZJCA《电子认证业务规则》为处理依据，法律法规另有要求的除外。

1) ZJCA的赔偿责任

- 在签发证书时，如果未按照本《通用证书策略》的规定进行处理，或者违反法律法规的要求而造成证书订户损失的，ZJCA应承担赔偿责任。
- 因为操作人员恶意、故意或者疏忽，未按照本《通用证书策略》的规定签发、吊销等请求，而造成证书订户损失的，ZJCA应赔偿订户的损失。
- 因ZJCA的根密钥出现问题，造成订户证书出现问题的，ZJCA应赔偿相关的损失。
- 证书订户或者其他有权提出吊销证书的人，提出吊销请求后、到ZJCA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、或进行交易时产生纠纷的，如果ZJCA按照本《通用证书策略》的规范进行了有关操作，ZJCA不承担任何损害赔偿责任。
- 证书订户赔偿的追溯有效期限，按照有关法律法规的要求进行操作。

2) 注册机构（包括受理点、授权的依赖方）的赔偿责任

- 注册机构及其操作人员没有妥善保管订户的注册和身份验证的相关隐私信息，而造成订户信息泄露、被冒用、篡改或者任意使用导致产生损失的，注册机构应负担损害赔偿责任。
- 如果因为操作人员故意、恶意或者疏忽，未按照本《通用证书策略》的规定

办理证书注册，或者违反法律法规而造成证书订户损失的，注册机构应赔偿订户的直接损失，以及其他随之产生的附带损失和相关补偿。

- 因为注册机构的原因造成系统或软件错误，未能在本《通用证书策略》规定的时间内，将订户的证书申请、吊销、挂起等请求信息发送给 ZJCA，而导致订户或者依赖方损失的，注册机构应承担所有的损害赔偿责任。
- 该类赔偿的追溯有效期限，按照有关法律法规的要求进行操作。

3) 订户的赔偿责任

- 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 ZJCA 及其授权的证书服务机构或者第三方遭受损害的，订户应赔偿一切损害责任。
- 订户因故意或者过失造成其私钥泄露、遗失，明知私钥已经泄露、遗失而没有告知 ZJCA 及其授权的证书服务机构，以及不当交付他人使用造成 ZJCA 及其授权的证书服务机构、第三方遭受损害的，订户应赔偿一切损害责任。
- 订户使用证书或者依赖方信任证书的行为，有违反本《通用证书策略》及相关操作规范，或者将证书用于非本《通用证书策略》规定的业务范围的，订户或者依赖方应承担一切损害赔偿责任。
- 订户使用或信赖证书时，未能依照本《通用证书策略》、ZJCA《电子认证业务规则》等规范进行合理审核，导致 ZJCA 及其授权的证书服务机构、第三方遭受损害的，应由该用户承担一切损害赔偿责任。
- 证书订户或者其他有权提出吊销证书的实体，提出吊销请求后、到 ZJCA 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、或进行交易时产生纠纷的，如果 ZJCA 按照本《通用证书策略》的规范进行了有关操作，那么应该由该证书订户承担所有损害赔偿责任。
- ZJCA 与订户签署的协议另有赔偿规定的，参照其规定。

9.9.2 赔偿限额

ZJCA 及其授权的注册机构（包括受理点、授权的依赖方），对所有当事人（包括但不限于订户、申请者、接受者或依赖方）的合计责任不超过证书的使用的责任封顶金额。

对于一份证书产生的所有数字签名和交易处理的总计，ZJCA 及其授权的注册机构（包括受理点、授权的依赖方）对任何人有关该特定证书的合计责任应该限制在一

个不超出赔偿责任上限的范围内。这种赔偿的上限按照《消费者权益保护法》来执行，即：赔偿限额不超过合同约定的证书单价或服务单价的三倍，其赔偿金额不足五百元的，为五百元。

本条款限制适用于一定形式的损害，包括但不局限于任何人或实体（包括但不局限于订户、证书申请者、接收方或信赖方）由于信任或者使用 ZJCA 签发、管理、使用、吊销证书或已过期证书而导致的直接的、补偿性的、间接的、特别的、结果的、惩戒性的或意外的损害。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的赔偿均有限额而不考虑签名、交易处理或其他有关的索赔数量。当超过赔偿限额时，除非得到依法判决或仲裁，可用的赔偿限额将首先分配给最早得到索赔解决的一方。ZJCA 没有责任为每个证书支付高出赔偿限额总和的赔偿，而不管高出赔偿限额总和在索赔提出者之间是如何分配的。

9.10 期限与终止

9.10.1 有效期限

本《通用证书策略》自发布之日起正式生效。

本《通用证书策略》中将详细注明版本号及发布日期。

9.10.2 终止

当新版本的《通用证书策略》正式发布生效时，旧版本的《通用证书策略》自动终止。

当 ZJCA 中止电子认证业务时，本《通用证书策略》自动终止。

9.10.3 效力的终止与保留

本《通用证书策略》的某些条款在终止后急需有效，如知识产权承认和保密条款。另外，各参与方应返还保密信息到其拥有者。

当由于某种原因，如内容修改、与适用法律相冲突，本《通用证书策略》、《电子认证业务规则》、订户协议、依赖方协议和其他协议中的某些条款失效后，不影响文件中其他条款的法律效力。

9.11 对参入者个别通告及信息交互

ZJCA 在必要的情况下，如主动吊销订户证书、发现订户将证书用于规定外用途

及订户其他违反订户协议的行为，可通过适当方式，如电话、电邮、信函、传真等，个别通知订户、依赖方。

9.12 修订

9.12.1 修订程序

ZJCA 安全策略委员会每年至少审查一次本《通用证书策略》，确保其符合国家法律法规和主管部门的要求，符合认证业务开展的实际需要。

本《通用证书策略》的修订由安全策略委员会提出并组织修改，ZJCA 安全策略委员会审核并批准后才能予以发布。

9.12.2 通知机制与期限

本《通用证书策略》公司网站（www.zjca.com.cn）上发布。

版本更新时，最新版本的《通用证书策略》在公司网站上发布，对具体个人和依赖方不做另行通知。

9.12.3 必须修改 CP 的情形

当本《通用证书策略》描述的规则、流程和相关技术已经不能满足 ZJCA 电子认证业务要求或本《通用证书策略》依据的法律法规和部门规章变更时，ZJCA 将依照有关规定修改本《通用证书策略》的相关内容。

9.13 争议解决条款

当 ZJCA、授权的注册机构、订户和依赖方之间出现争议时，按照以下步骤解决：

1) 当事人首先通知 ZJCA，根据本《通用证书策略》和 ZJCA《电子认证业务规则》中的规定，明确责任方；
2) 由 ZJCA 相关部门负责与当事人协调；
3) 协调不成的，当事人因与 ZJCA 或授权机构在电子认证活动中产生的任何争端及/或对本《通用证书策略》和 ZJCA《电子认证业务规则》所产生的任何争议，均应提请杭州仲裁委员会按照其仲裁规则在杭州进行仲裁。仲裁裁决是终局的，对双方有约束力。

9.14 管辖法律

中华人民共和国法律、规则、规章、法令和政令将管辖 ZJCA 的业务活动。ZJCA

的任何业务活动必须受有关法律、法规的制约，任何业务和法律文件、合同的解释、执行不能同有关法律、法规相冲突。

9.15 符合适用法律

本《通用证书策略》接受《中华人民共和国电子签名法》和《电子认证服务管理办法》以及其它中华人民共和国法律法规的管辖和解释。

ZJCA 提供的电子认证服务遵循《电子认证服务密码管理办法》。

9.16 一般条款

9.16.1 完整协议

ZJCA《通用证书策略》、《快捷型证书策略》、《电子认证业务规则》、订户协议及依赖方协议及其补充协议将构成 PKI 参入者之间的完整协议。

9.16.2 让渡

ZJCA、订户及依赖方之间的责任、义务不能通过任何形式让渡给其他方。

9.16.3 分割性

在法律允许的范围内，ZJCA 的订户协议、依赖方协议和其他订户协议可以包含可分割性条款。一个协议中的可分割性条款防止协议中一个条款的无效影响协议中其他条款效力。

9.16.4 强制执行

在 ZJCA、订户和依赖方之间出现纠纷、诉讼时，胜诉方可以要求对方支付有关诉讼费作为对其补偿的一部分。免除一方对某次合同违约的赔偿不意味着免除对其他合同违约的赔偿。

9.16.5 不可抗拒力

在法律允许的范围内，ZJCA 的订户协议、依赖方协议和其他订户协议应该包括保护不可抗力条款，明确在出些哪些不可抗拒力情况下，ZJCA 可以免除或部分免除责任。一般地，自然灾害、战争属于不可抗拒力。

9.17 其他条款

ZJCA 对本《通用证书策略》拥有最终解释权。