中国证券登记结算有限责任公司 CA 认证业务技术文档

中国结算 CA 系统准入测试方案

中国证券登记结算有限责任公司

二〇一三年四月

目　录

1 概述

1.1 术语定义

1.1.1 CSDCCA

中国证券登记结算有限责任公司（以下简称：中国结算）CA 系统，简称：CSDCCA。

1.1.2 证书服务代理机构

通过 CSDCCA 准入测试，并经中国结算同意，某特定机构或单位可以申请成为证书服务代理机构，负责审核和办理证书申请、更新、冻结、解冻、作废、查询等证书服务。

1.1.3 证书接入系统

证书服务代理机构用于连接 CSDCCA 系统的应用软件、服务器及其它硬件设备统称之为证书接入系统，由证书服务代理机构负责开发和建设。证书接入系统可以是单独的应用系统或其它应用系统的功能模块，也可以由相关硬件设备来实现，它与 CSDCCA 系统的接口定义详见《中国结算 CA 系统对外服务接口规范》。

1.1.4 数字证书

数字证书（Certificate），也称电子证书（以下简称证书），是一种由特定机构（CA）数字签名的，包含公开密钥以及公开密钥拥有者信息的电子文档，证书格式及证书内容遵循 X.509 标准。数字证书如同现实生活中公安机关颁发的居民身份证一样，数字证书是网络环境中的一种身份证，用于证明某一实体（如人、PC 服务器等）的身份。从证书的一般用途来看，数字证书分为签名证书和加密证书，签名证书主要用于对用户信息进行签名，以保证信息的不可否认性；加密证

书主要用于对用户在网络上传送的信息进行加密，以保证信息的机密性、真实性和完整性。

1.1.5 订户

订户，又称证书订户，即证书持有人，是指从 CSDCCA 接受证书的实体。包括已经申请并拥有 CSDCCA 签发的数字证书的自然人投资者、法人投资者及其它个人、企业、机构等各类主体或实体。CSDCCA 提供不同类型的证书，订户应决定何种证书适合于自己的需要，并同意如遇危及私钥安全的状况时及时通知发证机构及相关方。

1.1.6 唯一甄别名

唯一甄别名（Distinguished Name，简称 DN），是用来在数字证书的主体名称域中，唯一标识证书用户的名称，体现用户的唯一性。例如，可以用户名、证书类型、RA 名称、CA 名称以及国家名称等一定规则的组合作为数字证书 DN，标识证书用户。

1.1.7 CA 中心

CA（Certificate Authority）中心，是采用公开密钥基础技术，专门提供网络身份认证服务，负责签发和管理数字证书，且具有权威性和公正性的第三方信任机构。CA 是 PKI 体系的核心组成部分，本文通称为认证中心。

1.1.8 KMC

KMC，即密钥管理中心，是 PKI 体系的一个重要组成部分，负责为 CA 中心提供密钥的生成、保存、备份、更新、恢复、查询等密钥服务。

1.1.9 证书审核注册中心

证书审核注册中心（Registration Authority，简称 RA），是 PKI

体系中的注册审批系统，是 CA 的组成部分和向用户的延伸，负责向 CSDCCA 提交各种证书请求，接收来自 CSDCCA 的处理结果，并为 RA 系统使用人提供证书管理服务。

1.1.10 公钥和私钥

根据非对称密码学的原理，每个数字证书持有人都持有一对密钥，即公钥（Public Key）和私钥（Private Key），公钥与私钥作数据的互为加解密使用。公钥通常以数字证书的形式公开发布，私钥由证书持有者在本地生成，只能由证书持有者秘密掌握，证书持有者应当妥善保管并注意保密，不能在网上传输。

1.1.11 数字签名

在进行数字签名过程中，发信者使用自己的私钥，通过非对称密码算法，对待发数据的数字摘要（哈希值）进行加密，从而得到一段信息称为数字签名（Sign）。这就是签名的过程。

1.1.12 加密

加密是通过数学变换将明文转变成密文的过程，也就是对明文进行各种伪装从而使其真实内容完全隐藏的过程。加密的方法很多，主要是通过数学运算、位移、替换等方法来实现。解密是加密的逆过程，通过数学的方法将密文还原成明文。在加密解密过程中要使用密钥，只有密钥的持有人才能解密，恢复数据的原貌，从而保证了信息传输过程中的保密性。

1.1.13 证书撤销列表

证书撤销列表（Certificate Revocation List，简称 CRL），是一种包含撤销证书列表的签名数据结构。CRL 是证书撤销状态的公布形式，CRL 就像信用卡的黑名单，它通知其他证书用户某些电子证书不再

有效。

1.1.14 LDAP

即轻量级目录访问协议，用于查询、下载数字证书以及数字证书废止列表（CRL）。

1.1.15 中华人民共和国电子签名法

《中华人民共和国电子签名法》于 2004 年 8 月 28 日第十届全国人民代表大会常务委员会第十一次会议审议并通过，自 2005 年 4 月 1 日起施行，共计五章三十六条。该法通过确立电子签名的法律效力、规范电子签名行为、维护有关各方合法权益，在法律制度上保障了网上交易安全。

1.2 CSDCCA 系统架构

CSDCCA 是由根 CA、KMC、运营 CA（也称二级 CA）、RA 组成的多级运行体系，其中根 CA 是运营 CA 的根结点，负责向国内外顶级电子认证领域扩展信用范围；KMC 负责密钥的生成、保存、备份等服务；运营 CA 负责发放证书；RA 负责向运营 CA 提交各种证书操作请求，接收来自运营 CA 的处理结果；LDAP 服务器负责发布证书废止列表（CRL）。

CSDCCA 体系架构如下图所示:

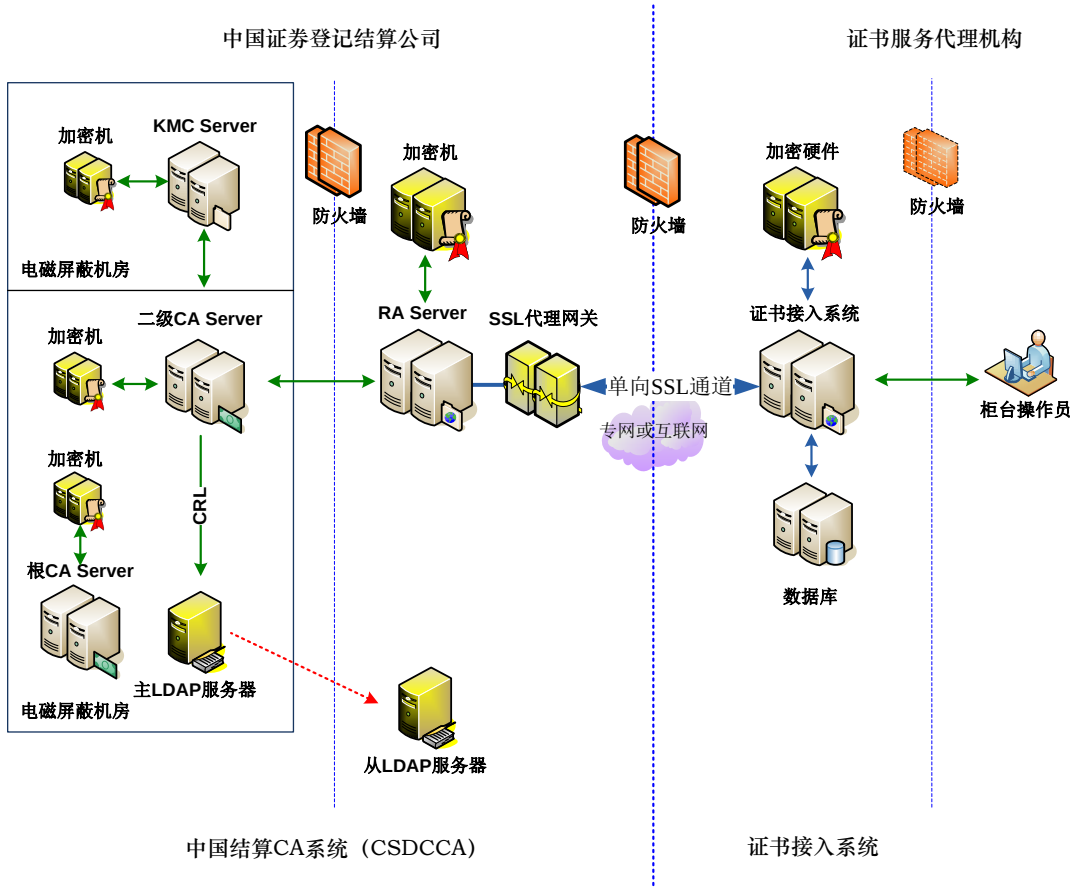

图 1 CSDCCA 系统架构示意图

证书服务代理机构需根据《中国结算 CA 系统对外服务接口规范》开发证书接入系统，并使用加密机或其它加密硬件设备存储证书服务代理机构接入证书和私钥，接入 CSDCCA 系统。

1.3 证书类型

按照证书的功能及申请证书的订户类型，CSDCCA 提供以下证书类型：

个人证书—面向境内、外自然人投资者及其它个人订户，在网上信息传递过程中提供身份验证、数字签名和信息加密等功能。

企业证书—面向境内、外法人投资者及其它企业订户，在网上信息传递过程中提供身份验证、数字签名和信息加密等功能。

企业员工证书—面向证书服务代理机构及其它企业内部员工订户，在网上信息传递过程中提供身份验证、数字签名和信息加密等功能。

证书服务代理机构接入证书—面向证书服务代理机构订户，是证书服务代理机构证书接入系统连接 CSDCCA 系统的电子凭证，在信息传递过程中提供身份验证和数字签名等功能。

其它类型—包括但不限于服务器证书、移动终端设备证书、手机号码证书等，目前不包含在本次测试范围内，不对其加以阐述。

根据安全级别不同的需求，针对个人证书、企业证书和企业员工证书分别提供普通证书和高级证书（暂不提供）两种类别，其中对于普通证书，只使用一套密钥对，即签名/验签密钥对。为保证签名私钥的安全性和唯一性，订户的签名/验签密钥对由订户在订户端生成，并在私钥丢失或怀疑泄露后及时申请密钥更新；对于高级证书，使用两套密钥对，即加密/解密密钥对，签名/验签密钥对。订户的加密/解密密钥对由 CSDCCA 密钥管理中心生成，而签名/验签密钥对则由订户在订户端生成。

1.4 证书发放流程

投资者证书及其它企业、企业员工证书是其作为网上开户及其它业务应用的身份认证工具，证书服务代理机构需在确认订户身份真实性的基础上发放。

对于订户临柜或见证申请，证书服务代理机构代其下载的方式，证书发放流程如下图所示:

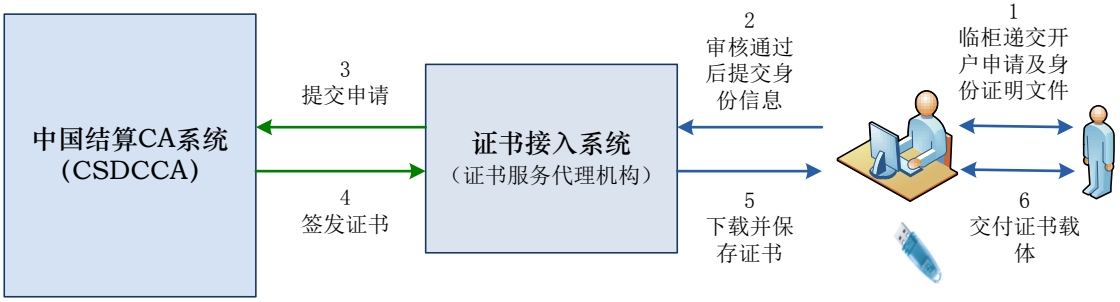

图 2 临柜或见证方式证书发放流程

对于订户临柜或见证申请，自主远程下载的方式，证书发放流程如下图所示:

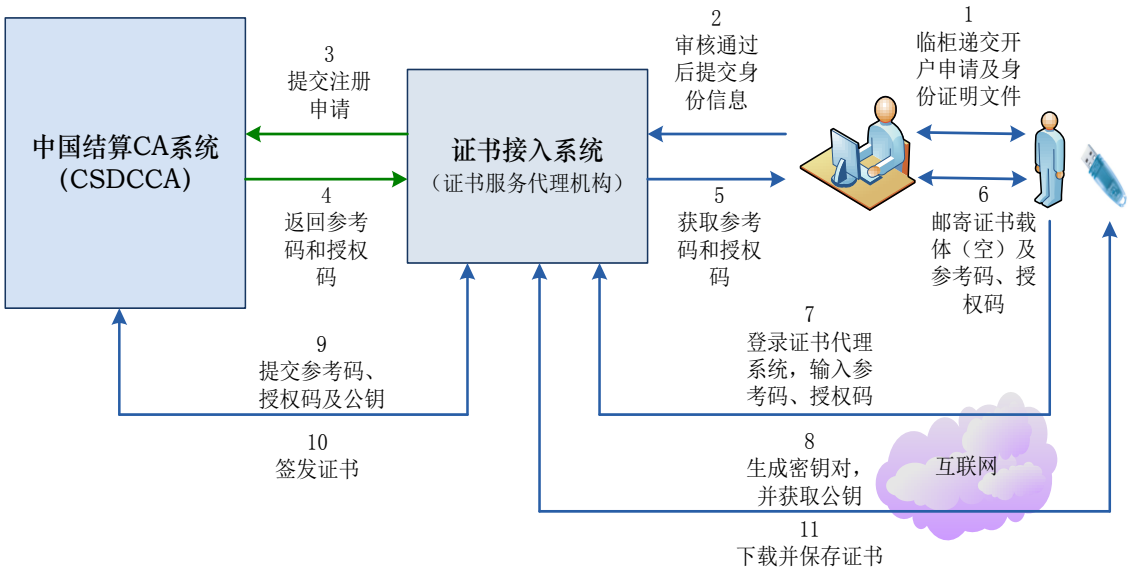

图 3 远程方式证书发放流程

1.5 CSDCCA 系统接入模式

证书服务代理机构接入 CSDCCA 系统前，需开发证书接入系统或在已有技术系统中实现证书接入系统有关功能，通过证书接入系统连接 CSDCCA，连接模式如下图所示。

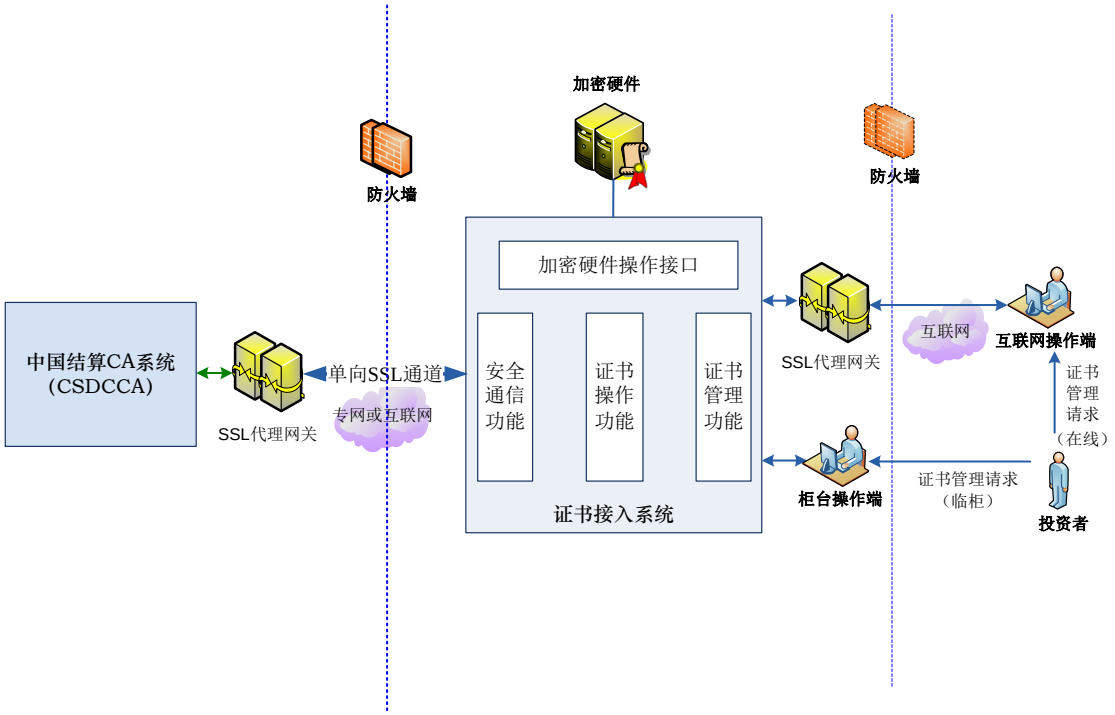

图 4 证书服务代理机构接入 CSDCCA 模式

证书接入系统负责连接到 CSDCCA 系统，完成证书操作相关功能，需实现以下功能:

（1）证书操作功能：承担证书申请、资料审核、证书制作及发放等工作，并将相关证书操作请求（如证书的申请、下载、冻结、解冻、作废、更新、查询等）提交给 CSDCCA 系统，接收和处理请求返还结果，实现《中国结算 CA 系统对外服务接口规范》;

（2）证书管理功能：存储和管理证书订户相关信息和证书信息;

（3）安全通信功能：使用证书服务代理机构接入证书对证书接入系统和 CSDCCA 之间交换的数据进行数据签名和验证数据签名，切实保障证书接入系统与 CSDCCA 之间数据交换的完整性和真实性;

（4）其它功能：实现对证书服务代理机构接入证书及私钥的安全存储，建议采用加密机或其它加密硬件设备实现该功能。

2 测试目的

本次测试主要目的在于测试证书代理服务机构的证书接入系统功能与数据接口是否与本公司《中国结算 CA 系统对外服务接口规范》完全符合，系统操作流程是否符合本公司有关业务规则要求。

注：本方案中涉及的证书、CSDCCA－证书服务代理机构关系、证书服务代理机构－证券账户开户代理机构、中国证券登记结算公司-证券公司、中国证券登记结算公司-投资者等关系纯属虚构，其他数据也仅仅为了测试而编制，并不代表真实情况。

3 测试系统环境

3.1 CA 测试系统

为更好地开展 CSDCCA 准入测试，中国结算提供了 CA 测试系统，证书服务代理机构的证书接入系统可以基于互联网采用 Https 协议访问中国结算 CA 测试系统（简称：CSDCCATest），完成证书操作相关测试。

CSDCCATest 的拓扑图如下图所示：

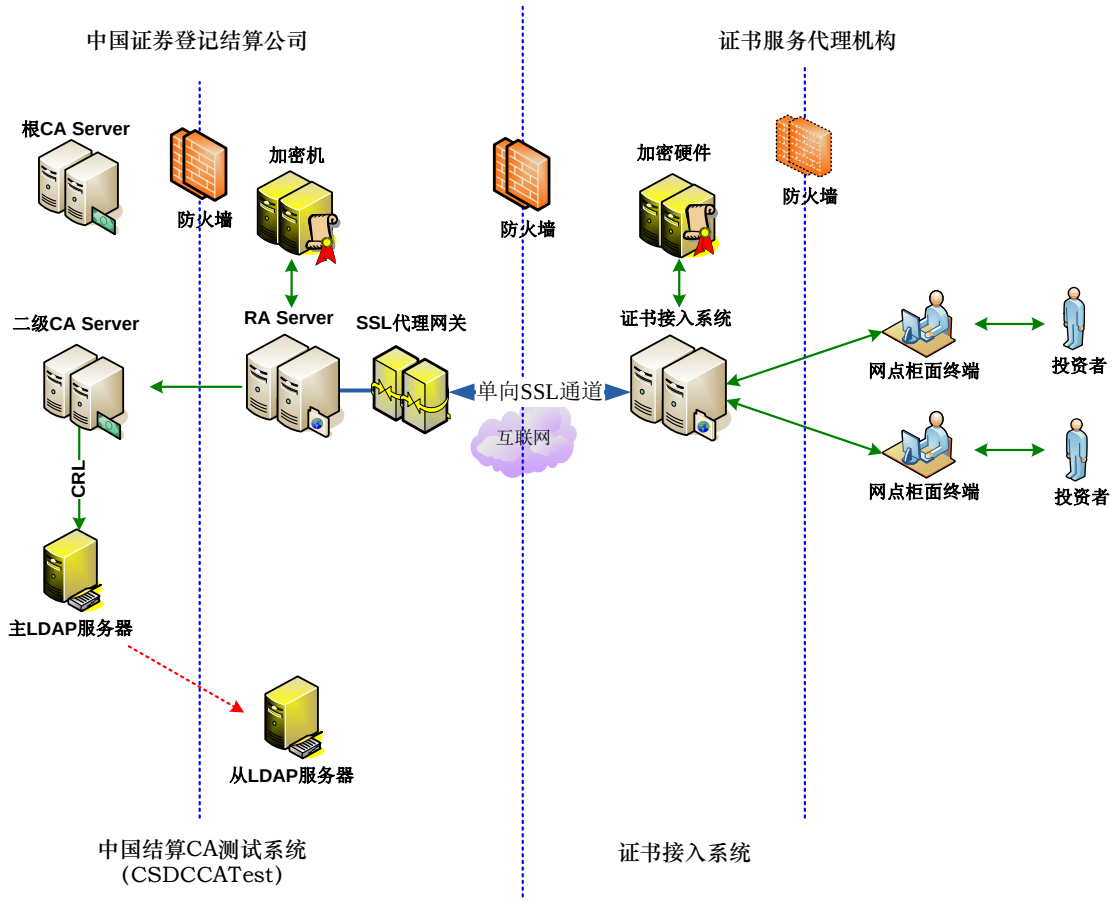

图 5 中国结算 CA 测试系统

CSDCCAtest 提供的对外测试接口约定如下:

- 接口提供方: 中国结算 CA 测试系统
- 连接方式: 单向 HTTPS 协议
- 接口协议: WebService
- 消息内容: 以 WebService 的方式进行相互之间通信, XML 遵循 1.0 标准规范, 使用 UTF-8 对 XML 文档进行编码, 具体内容详见《中国结算 CA 系统对外服务接口规范》
- 接口地址:

  https://ip:port?raGateway/WebServiceInterface.do?wsdl

- 其它：证书服务代理机构提交的所有证书操作请求均需使用证书服务代理机构接入证书进行签名，签名方式采用裸签（即只带签名，不带证书）方式

3.2 测试方式

证书服务代理机构的证书接入系统负责连接到CSDCCATest系统完成证书操作相关功能测试。测试前，证书接入系统需实现的功能详见1.5节。

3.3 网络连接参数

为保障CA测试系统网络安全，具体的网络连接参数将在接收到测试申请后，通过邮件方式发送至测试申请单位。

4 测试步骤

4.1 测试申请

证书服务代理机构成为中国结算授权的证书服务代理机构，接入CSDCCA生产系统之前，需向中国结算提交加盖公章的中国结算CA系统准入测试申请书面材料（含测试申请及证书服务代理机构接入测试证书申请，详见附件 1）及其电子版，并根据中国结算安排，连接CSDCCATest系统进行准入测试。

证书服务代理机构接入测试证书作为证书服务代理机构连接CSDCCATest系统的电子凭证，其具体申请和签发流程如下：

（1）证书服务代理机构向中国结算提交书面的测试证书申请材料（详见附件1），由中国结算对申请信息进行审核；

（2）证书服务代理机构在加密机或其它加密硬件设备内部生成密钥，产生证书请求RSA 2048位CSR（即证书请求文件），并

将证书请求文件通过电子邮件方式发送至中国结算，邮件主题或内容需写明申请单位名称和办理人员联系方式;

（3）中国结算收到证书请求后，生成测试证书，并通过电子邮件返回给证书服务代理机构;

（4）证书服务代理机构将测试证书存储到加密机或其它加密硬件设备中，完成测试证书申请流程。

4.2 测试过程

证书服务代理机构提交准入测试申请材料，并将 CSDCCATest 签发的测试证书存储到加密机或其它加密硬件设备后，应根据中国结算安排，严格按照《中国结算 CA 系统准入测试测试用例》对证书接入系统进行功能测试，并记录好测试过程中生成的数据文件及错误信息，测试完成后，如实填写《中国结算 CA 系统准入测试情况报告》(详见附件 2)，并将加盖公章的书面测试报告及电子版提交给中国结算。

5 测试内容

5.1 测试可覆盖功能

（1）证书申请;

（2）证书更新;

（3）证书补办;

（4）证书冻结;

（5）证书解冻;

（6）证书作废;

（7）证书查询;

（8）证书下载;

详见《中国结算 CA 系统对外服务接口规范》。

5.2 测试证书说明

测试证书由 CSDCCATest 为证书订户签发，CSDCCA 和 CSDCCTtest 不承担任何证书真实性的责任，仅供证书服务代理机构准入测试使用。

测试证书 DN 规则如下表所示。

表 1 测试证书 DN 规则

证书类型	证书用途	证书 DN 规则
个人普通软证书	面向境内、外自然人投资者及其它个人订户	CN=C@1@序列号, OU=Customers01, O=CSDC(1 个空格)Test,C=CN
个人普通硬证书		CN=C@2 @序列号 , OU=Customers01, O=CSDC (1 个空格)Test,C=CN
个人高级硬证书(双证，暂不开放)		CN=AC@3 @序列号, OU=AdvanceCustomers, O=CSDC(1 个空格)Test,C=CN
企业普通软证书	面向境内、外法人投资者及其它企业订户	CN=E@4@4 位机构号@序列号, OU=Enterprise, O=CSDC(1 个空格)Test,C=CN
企业普通硬证书		CN=E@5@4 位机构号@序列号, OU=Enterprise, O=CSDC(1 个空格)Test,C=CN
企业高级硬证书(双证，暂不开放)		CN=AE@6 @4 位机构号@序列号, OU= AdvanceEnterprise, O=CSDC(1 个空格)Test,C=CN
企业员工普通软证书	面向证书服务代理机构及其它企业内部员工订户	CN=P@7@4 位机构号@序列号, OU=Operator, O=CSDC(1 个空格)Test,C=CN
企业员工普通硬证书		CN=P@8 @4 位机构号@序列号, OU=Operator, O=CSDC(1 个空格)Test,C=CN
企业员工高级硬证书		CN=AP@9@4 位机构号@序列号, OU=AdvanceOperator,

(双证，暂不开放)		O=CSDC(1 个空格)Test,C=CN
证书服务代理机构接入证书	面向证书服务代理机构订户	CN=4 位机构编号@序列号, OU=Access, O=CSDC(1 个空格)Test,C=CN

注意：测试证书 DN 规则中，O=CSDC(1 个空格)Test，即为 CSDC Test ，表达的含义是 CSDC 和 Test 之间有一个空格分隔。

6 测试要求

1、各参测单位应做好详尽的 CSDCCA 准入测试计划，提交《中国结算 CA 系统准入测试申请表》，并指定专人负责联网测试工作。

2、各参测单位须建置较为独立的系统测试环境进行测试，不能因 CSDCCA 准入测试而影响到运行系统、其他业务和交易。

3、各参测单位须详细记载测试现象与结果，检查其正确性。如发现异常现象，及时向本公司报告。

4、各参测单位需认真研究本测试方案，并根据测试方案所提供的框架组织相应的测试案例，尽量覆盖正/反、常用/异常情况。

7 联系方式

中国证券登记结算公司

联系人：刘永红（负责测试）

联系电话：010-59378658

邮件：yhliu@chinaclear.com.cn

联系地址：北京西城区太平桥大街 17 号（邮编：100033）

联系人：王思远（负责测试）

联系电话：010-58598875

邮件：sywang@chinaclear.com.cn

联系地址：北京西城区太平桥大街 17 号（邮编：100033）

联系人：孙宏伟（负责接口规范）

联系电话：010-58598987

邮件：hwsun@chinaclear.com.cn

联系地址：北京西城区太平桥大街 17 号（邮编：100033）

附件 1 中国结算 CA 系统准入测试申请表

中国结算 CA 系统准入测试申请表

单位名称:

一、测试证书申请

申请单位名称: ----------

单位邮政地址: ----------邮政编码: □□□□□□

组织机构代码证号: □□□□□□□□-□

工商营业执照注册号: □□□□□□□□□□□□□□□

其他证件号: ---------- (可选)

办理人信息:

姓　　名: ---------- 身份证号码: ----------

联系电话: ---------- 传真: ---------- -

电子邮箱地址: ----------

二、系统基本情况

1、是否完全实现《中国结算 CA 系统对外服务接口规范》: 是□　否□

2、加密硬件名称 型号 厂商----------

3、是否有固定公网 IP 地址或地址段: 是□:测试系统服务器 IP 地址或地址段: ---------- ,如进行 NAT 转换,则转换后 IP 地址或地址段: ---------- 。否□

4、系统架构: □B/S 架构　□C/S 架构

5、测试系统服务器操作系统名称 版本----------(可选)

6、操作终端设备名称: □普通 PC　□平板电脑(如 IPAD) □其它-----(可选)

三、测试负责人

姓名: ----------　职务/职称: ----------

传真: ----------　联系电话: ----------

手机: ----------　电子邮件: ----------

通信地址: ----------　邮编: -------

四、其它建议
申请单位在此郑重申明：以上所填信息及相关证明材料完全真实有效，特申请中国结算 CA 系统准入测试，并接受据此颁发的证书服务代理机构接入测试证书。本单位全权委托上述办理人和测试负责人处理测试证书申请及准入测试的相关事宜。 申请单位盖章：_____ 日期:_____年____月_____日

注：在所选项目的“□”打“✓”，并填写所选项目对应要求的信息。

附件 2 准入测试报告模板

中国结算 CA 系统准入测试情况报告

填表日期:

单位名称:

一、测试用例通过情况

1、申请证书（含个人/企业/企业员工等证书类型）

1.1 申请返还两码

☐ 1.1.1 正常流程 ☐ 1.1.2 异常流程

1.2 申请下载证书

☐ 1.2.1 正常流程 ☐ 1.2.2 异常流程

2、更新证书（含个人/企业/企业员工等证书类型）

2.1 更新返回两码

☐ 2.1.1 正常流程 ☐ 2.1.2 异常流程

2.2 更新下载证书

☐ 2.2.1 正常流程 ☐ 2.2.2 异常流程

3、补办证书（含个人/企业/企业员工等证书类型）

3.1 补办返回两码

☐ 3.1.1 正常流程 ☐ 3.1.2 异常流程

3.2 补办下载证书

☐ 3.2.1 正常流程 ☐ 3.2.2 异常流程

4、冻结证书（含个人/企业/企业员工等证书类型）

☐ 4.1 正常流程 ☐ 4.2 异常流程

5、解冻证书（含个人/企业/企业员工等证书类型）

☐ 5.1 正常流程 ☐ 5.2 异常流程

6、作废证书（含个人/企业/企业员工等证书类型）

☐ 6.1 正常流程 ☐ 6.2 异常流程

7、查询证书（含个人/企业/企业员工等证书类型）

☐ 7.1 正常流程 ☐ 7.2 异常流程

8、证书下载（含个人/企业/企业员工等证书类型）

☐ 8.1 正常流程 ☐ 8.2 异常流程

注：如还使用其他测试用例，请将测试用例及测试结果作为附件提交。

二、测试结论

1、测试日期：_____年___月___日___时至_____年___月___日___时

2、测试用例完成情况　完全通过□　部分通过□
如果部分通过，系统改造还需_____时间，并列出未通过测试用例编号：

_____

3、其它：_____

三、异常情况

1、

2、

3、

4、

郑重申明：以上所填信息及相关证明材料完全真实有效，特申请中国结算 CA 系统准入测试情况报告。

测试负责人： **联系电话：**

注：在所选项目的“□”打“✓”。

中国证券登记结算有限责任公司　　_____公司
（盖章）　　（盖章）