**1.接入范围和基本要求**

数字证书互信互认系统接入的范围为已取得电子政务电子认证服务资质的证书认证机构，已建证书认证系统但尚未取得电子政务电子认证服务资质的证书认证机构，应在取得资质后再行接入。要求接入的证书认证系统采用SM2算法，并遵从《GM/T 0015-2012 基于SM2密码算法的数字证书格式规范》，对接网络环境为国家电子政务外网。

**2.接入流程**

为确保接入注册的各级电子政务电子认证服务机构证书认证系统证书认证系统的合规性，各证书认证机构信息的全面性和准确性，以及证书认证机构证书验证信息CRL的实时性和有效性，证书互信互认系统接入检测遵循以下流程：

1. 计划接入的各电子政务电子认证服务机构线下提交《电子认证数字证书互信互认系统接入申请表》，并加盖机构单位公章，申请表参见附录2；
2. 计划接入的电子政务电子认证服务机构按接入要求提供相关信息和文件，并完成政务外网测试对接环境的准备工作，将测试环境相关信息上报系统管理员；
3. 系统管理员收到申请书并审核通过后，与计划接入的机构进行测试环境对接；
4. 测试环境对接成功后，系统管理员将相关机构正式注册至证书互信互认系统生产环境，完成系统对接。

**3.接入前检测内容**

遵从海南省CA互信互认接入检测标准、GM/T 0015-2012、GM/T 0034-2014、GM/T 0037-2014等要求，对接入证书认证机构进行检测，内容包括证书信任链检测、证书格式符合性检测、CRL格式符合性检测等。各电子政务电子认证服务机构，包括现有的第三方CA和行业CA，在接入前应将CA的相关基本信息、CA的证书验证相关信息上报给证书互信互认系统运行维护机构进行检测。具体包括：

1. CA注册基本信息：认证机构名称、省份、证书认证机构联系人、证书认证机构联系电话、证书认证机构的根证书、证书认证机构颁发的示例证书；
2. CA证书验证信息（CRL链接相关信息）：连接证书认证机构对外发布的LDAP主机IP、LDAP主机端口号、对应LDAP中过滤CRL证书链的条件、CRL证书存放的属性值、CRL的基准DN。

**4.信息注册**

应按海南省CA互信互认接入检测标准，通过接入检测后，互信互认管理平台注册不同证书认证体系的根证书、证书吊销验证信息以及示例证书。确保各证书认证机构注册信息的准确性，确保CA证书验证信息的实时性和有效性。

注册信息应包括CA基本信息和CA证书验证信息：

表 1 证书认证机构注册基本信息

|  |  |
| --- | --- |
| 项名称 | 描述 |
| 认证机构证件号 | 采用国家密码局审批的电子政务电子认证服务机构证件号作为接入证书互信互认系统的证书认证机构统一可识别标识 |
| 省份 | 证书认证系统所在机构的省份信息 |
| 联系人 | 证书认证系统所在机构维护人姓名 |
| 联系人电话 | 证书认证系统所在机构维护人联系电话 |
| CA根证书导入 | 证书认证系统根证书链信息，包括注册证书认证系统所在证书认证系统的完整根证书信息，包括证书签发系统、注册审核系统证书，并将所有证书转换为PEM编码格式后合为一份文件整体导入证书互信互认管理系统 |
| 示例证书 | 证书认证系统颁发的示例证书，用于该证书认证系统接入时的互信互认验证 |

CA证书验证信息应包括证书验证的CRL地址信息、CRL证书的属性信息等：

表 2 CA证书验证信息

|  |  |
| --- | --- |
| 项名称 | 描述 |
| LDAP主机地址 | 证书认证系统对外发布CRL文件的LDAP地址信息 |
| LDAP主机端口 | 证书认证系统对外发布CRL文件的LDAP端口信息(一般默认389) |
| CRL过滤Filter(过滤条件) | 通过LDAP获取证书认证系统对外发布CRL证书过滤条件(objectClass=cRLDistributionPoint,，一般是objectClass=xxxxx) |
| CRL文件存放的属性值 | 通过LDAP获取证书认证系统对外发布CRL文件存放的属性值，程序根据存放属性值取出CRL文件(列如：certificateRevocationList;binary)如果CRL存放属性是有多个，请使用逗号“,”分隔开填写 |
| CRL的基准DN | 通过LDAP获取证书认证系统对外发布CRL文件起始扫描节点DN信息 |

**6.日常管理**

接入数字证书互信互认系统的证书认证机构应定期组织安全检查，定期对运行状态进行检查，确保系统运行的稳定与安全，应重点关注和检查以下内容：

1. 数字证书发放的合规性，避免非法人员持有合法证书；
2. 定期检查LDAP系统CRL的更新，避免已注销的数字证书仍能够正常使用；
3. 无法实时进行线上与证书互信互认系统同步的LDAP系统，证书认证机构应定期将CRL文件上报至数字证书互信互认系统。