**360浏览器根证书预置申请表**

申请加入360浏览器根信任库的CA机构必须

1. 遵守360浏览器根认证策略的规定（[链接](http://caprogram.360.cn)）
2. 填写并提交本表格（发邮件至caprogram@360.cn）

**CA机构的基本信息**

|  |  |
| --- | --- |
| CA公司名称 |  |
| 公司网址 |  |
| 企业类型 | 指CA机构由何种类型企业运营：私营企业、公有企业、政府机关、国际机构、学术机构、财团或非营利组织等等。注意：某些情况下CA机构可以为混合制企业，如政府成立的公司。对于政府CA，这里必须说明该政府的层级（如：国家、地方、州级、省级或市级）。 |
| 主要市场/客户群 | CA将服务于何种客户群？CA是否仅为某一国家或地区提供服务？ |
| 对360用户的影响 | 为什么CA需要将根证书内置到360根信任库中而不仅通过请求360信任库已有的其他根证书为其签发可信任的中级根？详细介绍哪些用户需要倚仗该根证书浏览网站（https访问） |
| 其他浏览器中的内置情况 | 用于申请内置的根证书是否已内置于别的浏览器中？若有，请列举。 |
| CA机构的首选联系方式（POC） | 首选联系email邮箱：Email邮箱别名：CA机构电话号码：CA机构的代表人必须亲自提交和（或者）参与根内置申请。根据360根证书计划策略：为了将CA机构的根证书预置在360根信任库中，CA机构必须向360提出申请，并请发邮件至caprogram@360.cn。该申请必须由主体CA机构授权的代表作出。 |

**根证书和子证书的技术参数**

|  |  |
| --- | --- |
| 根证书名称 | 用户适当的名称，展示证书信息。 |
| 证书序列号 |  |
| 颁发者字段 | 颁发者信息中的机构名称和通用名字段必须有足够的CA机构信息。 |
|  |  |
| 指纹 |  |
| 有效期开始于 |  |
| 有效期结束于 |  |
| 证书版本 |  |
| 证书签名算法 |  |
| 签名密钥参数 | RSA密钥长度，如：2048/4096bit；或ECC算法，如：NIST Curve P-256、P-384或P-512. |

**终端用户证书简况**

|  |  |
| --- | --- |
| 主体 | 指示字段 |
| 颁发者 | 指示字段和内容 |
| 持续时间 | 比如，一年 |
| 证书版本 |  |
| 证书签名算法 |  |
| 签名密钥参数 | RSA密钥长度，如：2048/4096bit；或ECC算法，如：NIST Curve P-256、P-384或P-512. |
| CRL URL | CRL链接 |
| OCSP URL  | OCSP链接 |
| 策略OID(s) |  |

**CA机构每个根证书的层级信息**

|  |  |
| --- | --- |
| CA层级 | 列举、描述和（或）以图表的方式列出根证书签发的所有中级根。指明哪些是内部运营子CA，哪些是外部运营子CA。 |
| 外部运营的子CA | 如果根证书下有子CA根证书是有第三方机构运营的，则必须提供这些信息：子CA公司名称；子CA网址；子CA证书下载地址；安装有链接到子CA证书的测试网站的链接（若允许子CA签发SSL证书）；子CA下的证书层级；子CA的CP/CPS链接；其CP或CPS中的相关章节的章节号，该章节内容规定合理的验证域名所有权的方法。 |
| 交叉签名 | 列出所有该根证书为其他根证书签发的交叉根证书；列出其他根证书为该根证书签发的交叉根证书；若存在此类交叉签名，注明该CA是否有预置到360的根证书库中。 |

**验证策略和操作**

|  |  |
| --- | --- |
| 策略文件 | 以下文件的链接：CP：CPS：依赖方协议： |
| 审计 | 审计类型：审计机构：审计机构网站：审计报告和管理声明的URL： |
| 测试证书网站 | 正常(good)： 过期(expired)： 吊销(Revoked)：  |
| 《基本要求》（SSL） | BR的审计报表的URL： |
| EV | EV审计报表的链接 |
| 网络安全 | 适当文档的链接 |