
教育网域名安全证书服务流程说明

(CFCA 证书)

CFCA 全球信任 SSL 证书办理过程，申请机构必须提供真实的材料，以证明机构的真实身份、申请人的真实身份、机构对域名的所有权等。CFCA 将对机构提供的材料进行严格审查。

1. 申请材料说明

申请机构需要向 CFCA 提供如下材料：

1、全球信任服务器证书申请表，需加盖公章（单位公章或带单位名称的部门章即可）；文件参考[附录一](#)



全球信任服务器证书申请表2020.xlsx

2、证书请求文件 CSR（生成方式请访问 <https://ssl.cfca.com.cn/Web/tool>）。

3、域名所属机构的身份证件复印件（如事业单位法人证书，无需盖章）；

4、经办人身份证件复印件（如身份证，无需盖章）；

5、根据自身情况选择域名验证方式以完成域名验证。CFCA 域名验证支持邮件验证、DNS 验证、文件验证及域名证书（盖章）四种方式。详细区别及操作方法参考以下文档或[附录二](#)



域名验证指南-V1.2.pdf

6、公网 IP 的证明（一般为网络运营商出具，用于证明 IP 所有权，仅申请 IP 形式的 OV SSL 证书时需要提供）；

IP 使用权证明示例如下：

公网 IP 证明函

中金金融认证中心有限公司：

运营商：_____（运营商名称）

证明以下公网 IP 地址：

IP1:

IP2:

IP3:

为我司分配给_____（证书申请单位名称）使用！

运营商：_____（公章）

时间： 年 月 日

所盖公章为单位公章，可使用部门章，公章（部门章）的名称要与单位名称一致。

申请机构需要将上述所有材料的电子版提供给赛尔网络，申请机构必须保证所提供材料的真实性，赛尔网络将协助申请机构办理证书。

2. 审核说明

赛尔网络业务部门将对申请机构提供的材料进行审查，主要内容包括：

- 1、检查证书申请表中机构信息与提供的机构身份证件是否相符。
- 2、检查证书申请表中申请人信息与提供的申请人身份证件是否相符。
- 3、检查证书申请表中域名与提供的域名证明是否相符。如域名非申请机构所有，则需要申请机构提供该域名所有者出具的唯一使用该域名的授权证明材料。如使用公网 IP，需提供网络运营商出具的 IP 使用权证明。

4、CSR 文件，DN 规则要求符合如下规范：

- (1) DN 中各项顺序依次为：CN、OU、O、L、ST、C；
- (2) CN 项是域名或者 IP，与证书申请表中域名一致；
- (3) O 项必须是真实的、完整的机构名称，与证书申请表中机构名称一致；
- (4) L 项、ST 项、C 项是必须是机构注册地，与机构身份证件中的注册地区一致。

3. 证书签发

CFCA 最终审核通过后，将由赛尔网络证书管理员签发证书。证书公钥及证书链将发送到证书申请表中的申请人邮箱。

4. 证书更新、延期、吊销

使用证书过程中，如果出现证书遗失、损坏、密钥泄露等问题，需要重新签发证书，机构应重新提供材料办理证书。证书有效期内 CFCA 免费进行证书操作。

证书到期前三个月内，赛尔网络会主动提醒机构申请联系人办理证书延期，机构应重新提供材料办理证书延期。

机构如果不再使用证书，可以联系赛尔网络办理证书吊销，并将该证书从网站服务器上移除。

附录一、CFCA 全球信任证书申请表

申请表

CFCA 全球信任服务器证书申请表							
证书申请信息	申请日期		证书数量		证书期限		
	业务类型	<input type="checkbox"/> 新申请 <input type="checkbox"/> 更新 <input type="checkbox"/> 吊销					
	证书类型	OV证书	<input type="checkbox"/> 单域名OV服务器证书		<input type="checkbox"/> 通配符OV服务器证书		
			<input type="checkbox"/> 多域名OV服务器证书				
	EV证书	<input type="checkbox"/> 单域名EV服务器证书					
		<input type="checkbox"/> 多域名EV服务器证书					
	域名						
	注： 1、多域名证书，默认以CSR中填写的域名为证书主域名，其他作为备用域名 2、通配符证书，适用以*开头的域名，例如*.domain.com 3、IP类型只限于申请公网IP，且只可申请OV单域名或者多域名（多个IP）证书 4、该处直接填写域名即可，不需要添加http://或者https//						
域名验证方式	<input type="checkbox"/> 邮箱验证	<input type="checkbox"/> DNS验证	<input type="checkbox"/> 文件验证	<input type="checkbox"/> 域名证书（盖章文件）			
	注： 1、采用邮箱验证方式时，请确保whois隐私保护关闭，whois中管理员邮箱可用（若开启隐私保护，我方无法查询明确的管理员邮箱，则默认向admin、administrator、webmaster、hostmaster、postmaster开头的域名邮箱发送验证邮件，例如admin@domain.com形式，请确认上述邮箱可正常回复邮件后，再选择此种验证方式） 2、采用DNS或文件验证方式时，需要域名管理员在域名解析服务商处的域名管理系统操作，记录值或文件CFCA会发送至本表格中经办人邮箱，按照邮件提示操作						
申请企业/机构信息区（以下信息全部填写，不可留白）							
机构信息	机构名称（中文全称）						
	机构证件类型	<input type="checkbox"/> 企业营业执照 <input type="checkbox"/> 组织机构代码证 <input checked="" type="checkbox"/> 其它，请注明： 统一社会信用代码					
	机构证件号码			联系电话			
	联系地址			邮政编码			
申请经办人	姓名	职务		电子邮件			
	证件类型	证件号		联系电话			
申请确认人	姓名	职务		电子邮件			
	证件类型	证件号		联系电话			
申请声明	本人/机构授权本表格中经办人办理证书申请相关事宜，并承诺以上信息资料真实、有效。本人/机构已认真阅读并同意遵守中金金融认证中心有限公司（CFCA）网站（ http://www.cfca.com.cn ）发布的《数字证书服务协议》、《全球信任体系电子认证业务规则（CPS）》中规定的相关义务。						
	申请机构盖章				日期		
	备注						
申请材料说明： 1、申请表（加盖企业公章或带有公司名称字样的部门公章） * 2、CSR（CSR中信息需与申请表中一致，CSR生成地址： https://ssl.cfca.com.cn/Web/tool ） * 3、机构证件复印件 4、经办人身份证复印件 4、加盖公章的域名证书（若选择邮箱、DNS或者文件验证方式，此文件不需要提供） 5、公网IP证明函（仅当以公网IP申请时需要，运营商出具的加盖公章的公网IP分配证明文件） 6、如申请EV证书，需要额外提供律师函、律师证							

附录二、CFCA 域名验证方式

目前 CFCA 支持邮箱验证、DNS 验证、文件验证及域名证书（盖章）四种域名验证方式，本文介绍常用四种方法。

注意事项：域名验证记录值有效期为 48 小时，自生成时开始计算。请务必在 48 小时内完成配置，如超时未进行配置或验证未通过，请联系赛尔网络工作人员，重新申请域名验证记录值并配置。

方法一：DNS 验证

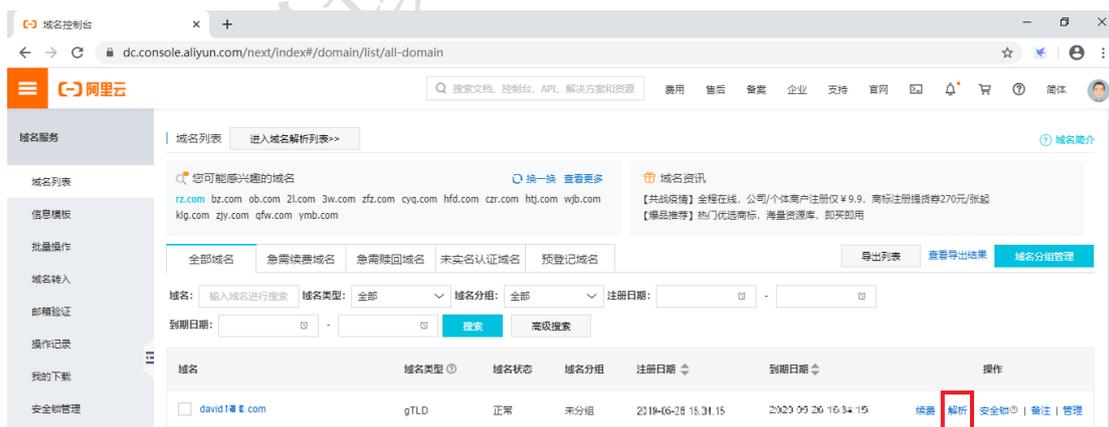
下文介绍 SSL 证书 DNS 验证在各主流域名注册商下的域名解析方法，仅供参考，具体以各注册商实际为准。赛尔网络会将 DNS 记录值发送到证书申请经办人邮箱，请留意查收。

DNS 验证注意事项：

当申请的域名不为主域名（如：domain.com），为二级域名时（如：www.domain.com），主机记录值需更新为：“_cfcachallenge.host.二级域名前缀”，即：_cfcachallenge.host.www

阿里云操作示例：

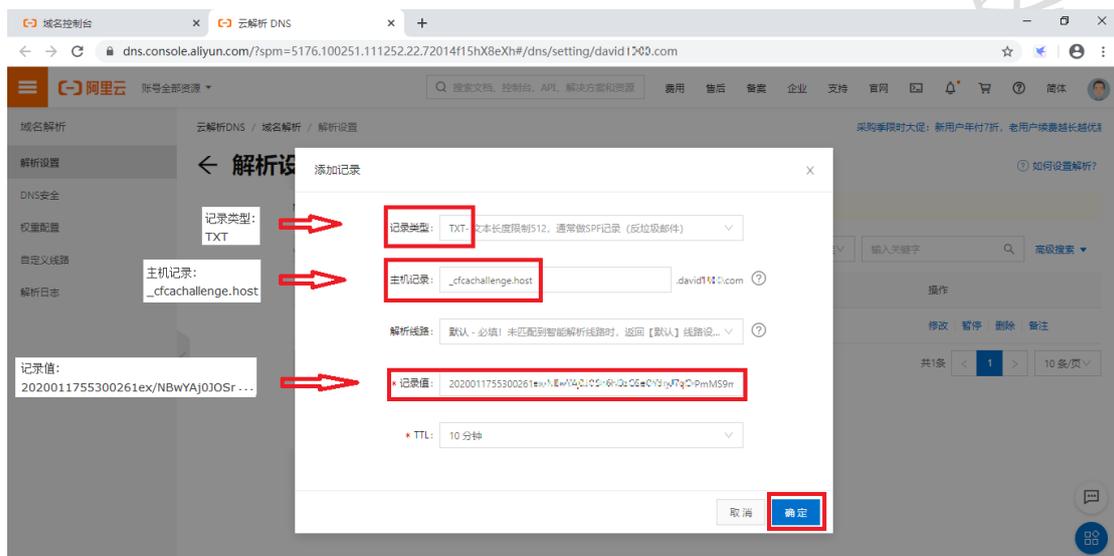
（1）登陆域名管理控制台，查看【域名列表】，单击操作栏的【解析】，进入域名解析页面：



（2）单击【添加记录】



(3) 添加记录类型为 TXT 的 DNS 记录，单击【确定】完成添加

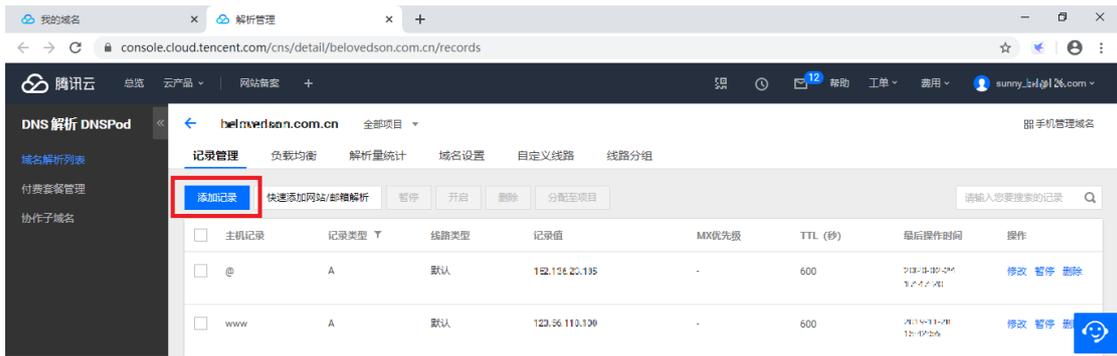


腾讯云操作示例：

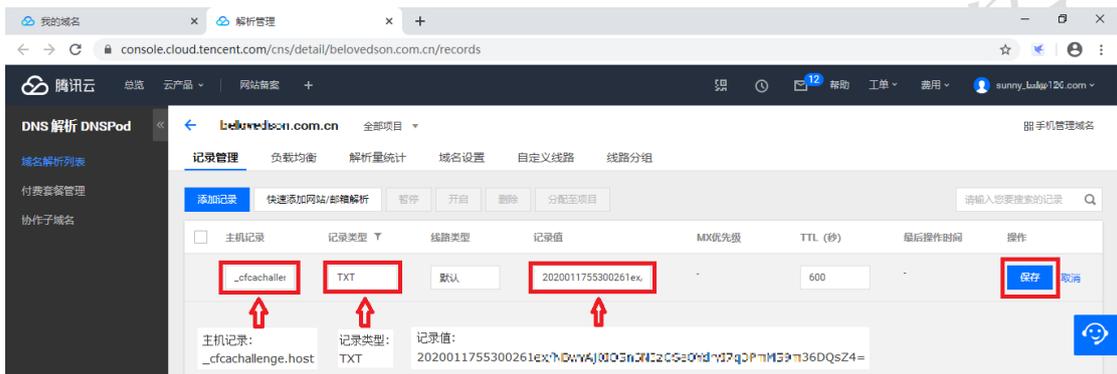
(1) 登陆域名管理控制台，查看【我的域名】，单击操作栏的【解析】，进入域名解析页面：



(2) 单击【添加记录】



(3) 添加记录类型为 TXT 的 DNS 记录，单击【保存】完成添加



新网操作示例：

将记录类型选择为 TXT 记录，在主机记录中输入邮件中提供的主机记录字段信息，不包括网址信息，在记录值中输入邮件中的记录值字段信息，点击添加



方法二：文件验证

选择文件方式验证后，赛尔网络会发送记录值至证书申请经办人邮箱：

操作步骤

1、创建文件：

本地创建名称为“**cfcafileauth.txt**”的TXT文件，将邮件中“文件内容”字段，

复制到上述文件，保存（请不要增加空格等其他多余信息）；

2、创建目录：

在站点根目录下创建 `/.well-known/pki-validation` 子目录，然后将 `cfcafileauth.txt` 文件上传至该目录；

注：

(1) 第一层目录是带点的隐藏目录，Windows 下命令为：`mkdir .well-known`

```
Microsoft Windows [版本 10.0.17134.1099]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\thinkpad>cd C:\inetpub\wwwroot
C:\inetpub\wwwroot>mkdir .well-known
```

(2) 如果您的站点由于某种原因无法创建隐藏目录，请选择 DNS 验证方式

3、域名解析至服务器

4、配置检测：

配置好之后，可通过浏览器访问地址，如正常输出配置的记录值，则表示配置成功。

(1) HTTP 配置检测：`http://您的域名/.well-known/pki-validation/cfcafileauth.txt`

(2) HTTPS 配置检测：`https://您的域名/.well-known/pki-validation/cfcafileauth.txt`

若申请 `*.domain.com` 类型的通配符证书时，访问检测地址为：

(1) HTTP 配置检测：`http://domain.com/.well-known/pki-validation/cfcafileauth.txt`

(2) HTTPS 配置检测：`https://domain.com/.well-known/pki-validation/cfcafileauth.txt`

注意事项：

(1) HTTP、HTTPS 任选其一验证通过即可，HTTP 方式需使用 80 端口，HTTPS 方式需使用 443 端口；

(2) 文件验证需要直接响应 200 状态码和文件内容，不支持任何形式的跳转。

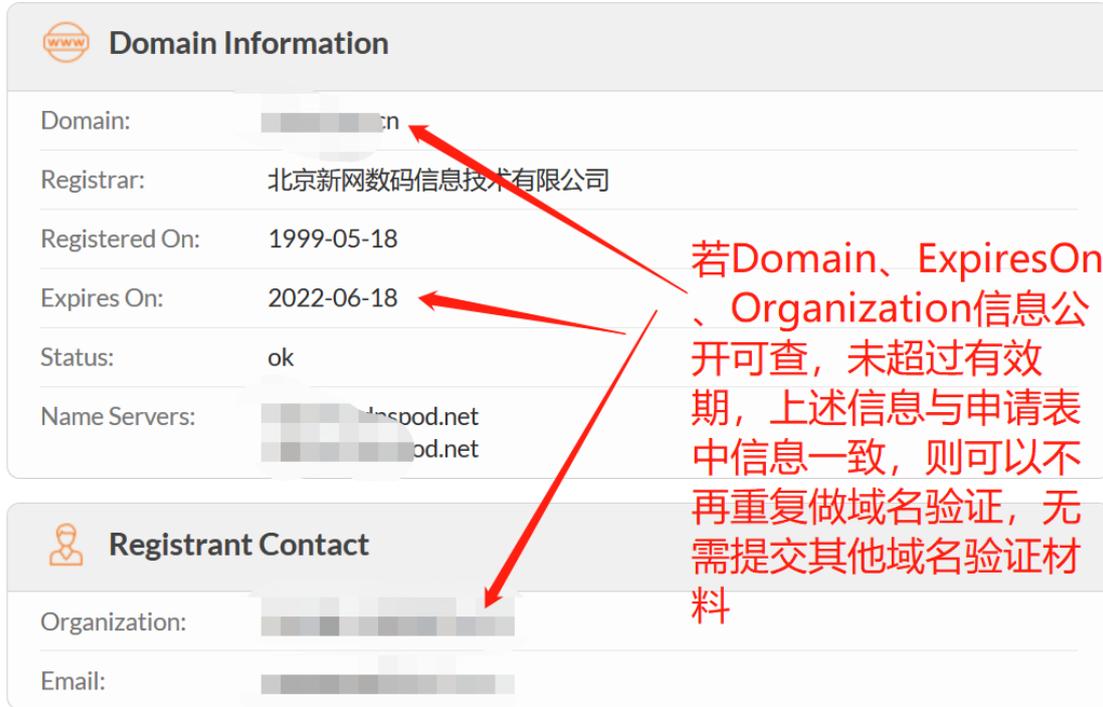
方法三：邮箱验证

邮箱验证，即通过 Whois 查询域名注册时预留的邮箱，赛尔网络向该注册邮箱发送 SSL 证书申请确认信息，若赛尔网络收到确认邮件，则可证明该邮箱被合法持有人控制，验证通过后可为其颁发服务器证书。

采用邮箱验证方式时，请确保 whois 隐私保护关闭，whois 中管理员邮箱可正常回复邮件（若开启隐私保护，我方无法查询明确的管理员邮箱，则默认向 `admin`、`administrator`、`webmaster`、`hostmaster`、`postmaster` 开头的域名邮箱发送验证邮件，例如 `admin@domain.com` 形式，请确认上述邮箱可正常回复邮件后，再选择此种验证方式。

Whois 邮箱查询地址:

<https://www.whois.com/whois/>



The screenshot shows a Whois domain information page. The top section is titled "Domain Information" and contains the following fields:

Domain:	████████.cn
Registrar:	北京新网数码信息技术有限公司
Registered On:	1999-05-18
Expires On:	2022-06-18
Status:	ok
Name Servers:	████████.nsod.net ████████.od.net

The bottom section is titled "Registrant Contact" and contains the following fields:

Organization:	████████████████████
Email:	████████████████████

Red arrows point from a red text box on the right to the Domain, Expires On, and Organization fields. The red text box contains the following text:

若Domain、ExpiresOn、Organization信息公开可查，未超过有效期，上述信息与申请表中信息一致，则可以不再重复做域名验证，无需提交其他域名验证材料

方法四：盖章的域名证书

如上述几种方式均不能验证，可以向 CFCA 提供注册域名时，域名注册机构发放的域名证书（提供盖章的电子版即可），CFCA 核实域名证书中信息与实际申请信息一致后，也可发放对应域名的服务器证书。