DV证书自主检测工具

**亚数信息科技（上海）有限公司**

目录

[DV证书自主检测工具 1](#_Toc502239238)

[1. 简介 3](#_Toc502239239)

[2. 工具介绍 3](#_Toc502239240)

[2.1 验证流程图 4](#_Toc502239241)

[2.2 模块详解 4](#_Toc502239242)

[2.2.1 CAA检测 4](#_Toc502239243)

[2.2.2 验证结果检测 5](#_Toc502239244)

[3. 解决方案 6](#_Toc502239245)

[3.1 DNS验证方式 6](#_Toc502239246)

[3.2 File验证方式 9](#_Toc502239247)

[4. 附录 11](#_Toc502239248)

[4.1 DNS验证规则 11](#_Toc502239249)

[4.2 FILE 验证规则 12](#_Toc502239250)

## 简介

申请Domain Validation（DV）类型的SSL证书时，Certificate Authority（CA）机构只验证域名所有权，不会人工介入审核验证。这一特性使DV证书颁发十分方便快捷，但也导致在系统审核的过程中产生很多验证限制，例如安全审核，DNS验证失败等，影响证书的正常颁发。

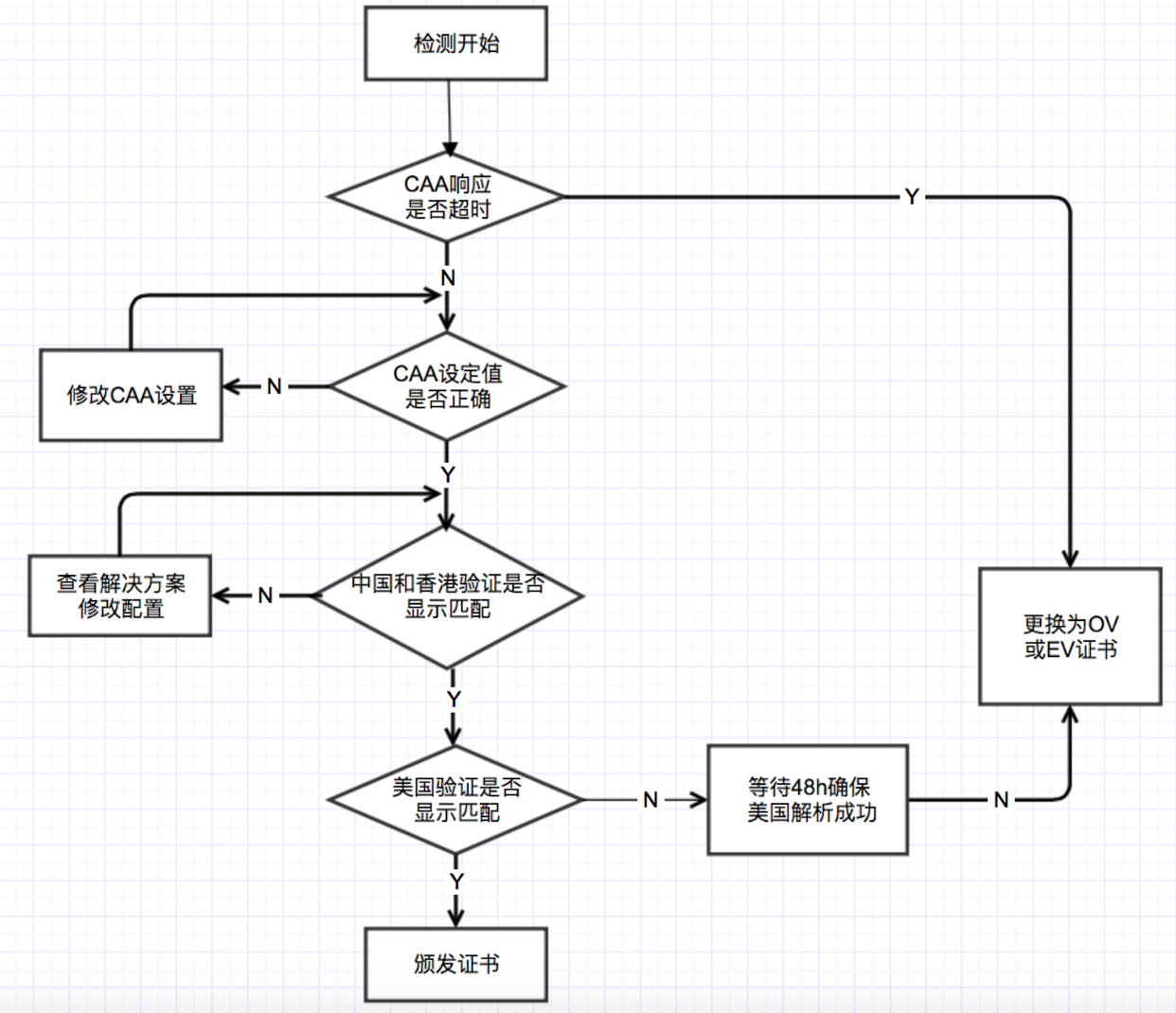
为了使用户能够自主定位问题，查询原因，调整配置，提高DV证书的的颁发效率，我司提供《DV证书自主检测工具》（以下简称“工具”）。

## 工具介绍

通过访问[https://myssl.com/dns\_check.html#ssl\_verify](https://myssl.com/dns_check.html" \l "ssl_verify)使用此工具。使用步骤如下图所示：



## 验证流程图



## 模块详解

## CAA检测

自2017年10月开始新增了CAA规则，DV证书的申请域名必须要通过 DigiCert的 CAA检查。CAA检测包含CAA超时和CAA设置检测，在其检测过程中，你可能遇到如下图所示的问题：

* CAA查询响应失败，时间超时



* CAA设置中未包含**symante.com**和**digicert.com**参数



## 验证结果检测

目前，此工具只针对TrustAsia和Let’s Encrpyt品牌的证书进行验证，验证方式会随CA的策略变化而变化。DV的验证方式分为**DNS验证**和**FILE验证**，任意一种验证方式都必须通过中国、香港和美国三方匹配。如下所示：



如遇到任一一方显示“验证失败”的提示，都表明匹配不成功。须查看本文中的**章节3解决方案**，根据实际情况进行修改后再次进行验证匹配。

## 解决方案

根据所选DV证书的验证方式，选择下面对应的问题及其解决方案，自行修改设置后再进行验证匹配。

## DNS验证方式

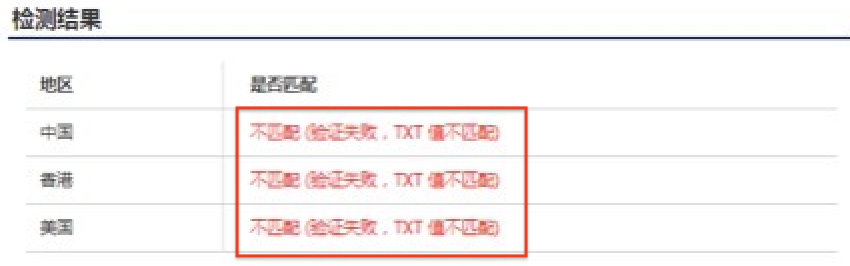
* 美国不匹配



**原因**：可能是DNS记录解析延迟导致

**解决方案**：耐心等待48小时后再查看。若之后还是显示“验证失败”提示，请更换申请Organization Validation (OV) 或者Extended Validation (EV) 类型证书。

* 三方都显示“不匹配（验证失败，TXT值不匹配）”

****

**常见原因**：1.订单中的验证值不正确

2.使用了非ANSI编码存储文件

**解决方案**：1.正确复制黏贴对应订单中的验证值；

2.使用ANSI编码存储文件。

* 三方都显示“不匹配（暂未查询到值）”



**原因**：没有配置TXT

**解决方案**：配置TXT解析。

* 显示“验证失败，DNS错误，查询XXX时域名错误”

**原因**：尚未使用该域名等

**解决方案**：购买或者申请该域名，并投入使用。

* 显示“验证失败，DNS错误，查询XXX时SERVFAIL”



**解决方案**：DNSSec导致失败，调整DNS配置。

* 显示“验证失败，DNS错误，查询XXX时数据错误”

**原因**：使用非常规DNS服务器，数据格式有问题

**解决方案**：更换DNS服务，如bind，server2016，腾讯云等。

## File验证方式

* 美国不匹配



**解决方案**: 直接更换申请OV或者EV类型证书。

* 显示“验证失败，请重试”



**解决方案**: 重新点击“检测”按钮。

* 显示“验证失败，验证中发生URL重定向”

**原因：**File验证链接响应状态为3xx

**解决方案**:重新设置，取消跳转等配置。

* 显示“验证失败，响应非2xx状态码”

**原因**：File验证方式没有设置为2xx响应，伴随出现404，页面不存在，50X服务器内不错等原因

**解决方案**:调整File验证配置来解决。

* 显示“验证失败，响应Content-Type错误”

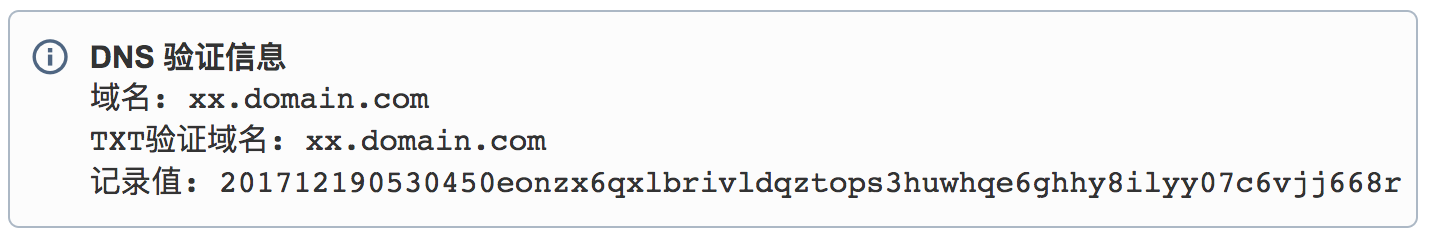


**解决方案**: Content-Type类型必须是text/html或者text/plain ，需到服务器上调整响应类型。

## 附录

## DNS验证规则

提交订单后，系统将返回如下验证信息



* 在域名的DNS系统中解析验证信息:    
  xx.domain.com  –>   TXT   –>  201712190530450eonzx6qxlbrivldqztops3huwhqe6ghhy8ilyy07c6vjj668r
* 若使用主域名下的 www 子域名申请证书，请直接对主域名解析验证信息，如：
  + 申请域名为*www.domain.com*，需用 domain.com来做 TXT域名验证解析。
  + 申请域名为*www.domain.com.cn，*需用domain.com.cn来做 TXT域名验证解析。
* 若做TXT验证解析的域名存在 CNAME记录，请在 域名前加一级 **\_dnsauth** 来做解析，避免CNAME冲突，如：
* xx.domain.com有CNAME记录存在，用 \_dnsauth.xx.domain.com 来做 TXT 验证解析。

## FILE 验证规则

提交订单后，系统将返回如下验证信息



* 在域名的指定路径下 /.well-known/pki-validation/fileauth.txt  设置指定内容：  
  201712190628231ynisv0fh7es467ttfsb59z0zag1ix6rfalphfa9rlodme9dw9
* 保证外网通过 HTTP 或 HTTPS 能够访问到指定内容。
* 内容结尾不能有任何回车或换行符。
* 内容响应状态码确保是 200 ，不支持任何形式跳转。
* 内容响应类型Content-Type必须是text/html或 text/plain ,不支持其他 Content-Type。
* FILE 验证内容的访问不能加UA限制，保证所有UA均可访问(Java/1.8.0\_xx)。
* 若使用主域名下的www子域名申请证书，请直接在主域名下放置验证文件，如：
  + 申请域名为*www.domain.com*，需在 domain.com下面的指定目录防止验证文件。
  + 申请域名为*www.domain.com.cn*，需在domain.com.cn下面的指定目录防止验证文件。