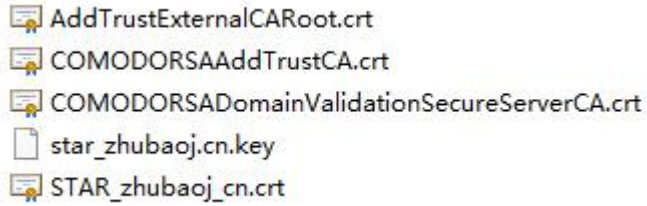


Sectigo 证书基本介绍及证书文件准备:

证书文件清单

Sectigo SSL 证书颁发下来为下列两种情况中的一种，请根据自己收到的文件做相应操作：

1、情况一，收到的证书由下方截图中的五个部分组成：



序号	文件名	文件描述
1	 AddTrustExternalCARoot.crt	根证书
2	 COMODORSAAddTrustCA.crt	中间证书 1
3	 COMODORSADomainValidationSecureServerCA.crt	中间证书 2
4	 star_zhubaoj.cn.key	私钥文件
5	 STAR_zhubaoj_cn.crt	网站证书文件

合并方法:

➤ 当配置 nginx 或 apache 文件时，需要将中间证书（文件序号 2,3）和网站证书文件（文件

序号 5）合并成一个，操作方法：

分别用文本编辑器打开三个文件，将文件 2 和文件 3 中内容依次复制粘贴到文件 5 的内容

之后保存即可。（根证书在合并时可以不放，也可以放在除了第一顺序的任何其他顺序，中

间不能出现空格或其他任意符号）


合并成功后参考下图：



```

-----BEGIN CERTIFICATE-----
MIIGSTCCBc2gAwIBAgIQBixII2gNhxTpU1QR4ruZezANBgkqhkiG9w0BAQsFADBl
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMTQwMgYDVQQDEyEaWdpQ2VydCBTSEYyIEV4dGVuZGVk
IFZhbG1kYXRpb24gU2VydMvYyIENBMB4XDTE4MDUyMTAwMDAwMFoXDTE5MDUyMTEy
jOpMbk3z5iD19iuLsjQAA7dfAiEAqEimqCFlnqGfcWFBCGmzEAmBfxyKHH0XBFJ1
MX8vZ9MwDQYJKoZIhvcNAQELBQADggEBAFL+hMkYzOGb50gFVCJhX+fjtMyGDQY0
aIg3c2uVYtThC7MpVeCp+vEwPieq17m9GRjzAl6QCLkNyD7LJLXHE3rYDKPAiauM
NJwooW4+fE9VmLdtOn05US8r5Uz0C4d3hlnCP7OR5it0W7pEC9cnP5Vyg38RLXST
cFimIxyq5yCVYTDfQ/qiyU7XDDBW/LuJlMQgP9k2Xpd+iE04QsyD/qVhWz9TvfzZ
eAAILAPB4TwRVIOFSVfnMjVsSSwp95jy4Dxvpylwrpamq720qNiJ3ldqVWWuJR41
bv8/lvOICyznJqrYULXcB5Szz1f1/8La3bnNmVMrWwEy/tpoHHEKacg=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEtjCCA56gAwIBAgIQDhmpRLCMEZUgkmFf4msdggzANBgkqhkiG9w0BAQsFADBs
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSswKQYDVQQDEyJEaWdpQ2VydCBIAWdoIEFzc3V5YW5j
ZSBFVjB5b290IENBMB4XDTE4MDUyMTAwMDAwMFoXDTE4MDUyMTAwMDAwMzFowdTEL
MAkGA1UEBhMCVVMxFTATBgNVBAoTDERpZ21lD2XJ0IEluYzEZMBcGA1UECmQ3d3
4xRjJcKx6HQGkyhE6Vt9VypAdP3THYUYUN9XR3WhfVUGLk3UHkMf4Ib0mKPLQNa
2sPIoc4sUqIAY+tzunHISScj12SFnjgOrWNoPLpSgVh5oywM395t6zHyuqB8bPEs
1OG9d4Q3A84ytciaGRpKkk47RppqF/oOi+Z6Mo8wNXrM9zwR4jxQUezKcxwCmXMS1
oVWNW1ZopCJwqjyBcdmqeU79OX2olHdx3ti6G8MdOu42vi/hw15UJGQmxg7kVkn
8TUoE6smftX3eg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEtjCCA56gAwIBAgIQDhmpRLCMEZUgkmFf4msdggzANBgkqhkiG9w0BAQsFADBs
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSswKQYDVQQDEyJEaWdpQ2VydCBIAWdoIEFzc3V5YW5j
SIB3DQEBAQUAA4IBDwAwggEKAoIBAQDT+SWFFi+hkNfP2g1RprVPUxKVGLk8m+92
jOpMbk3z5iD19iuLsjQAA7dfAiEAqEimqCFlnqGfcWFBCGmzEAmBfxyKHH0XBFJ1
MX8vZ9MwDQYJKoZIhvcNAQELBQADggEBAFL+hMkYzOGb50gFVCJhX+fjtMyGDQY0
aIg3c2uVYtThC7MpVeCp+vEwPieq17m9GRjzAl6QCLkNyD7LJLXHE3rYDKPAiauM
NJwooW4+fE9VmLdtOn05US8r5Uz0C4d3hlnCP7OR5it0W7pEC9cnP5Vyg38RLXST
cFimIxyq5yCVYTDfQ/qiyU7XDDBW/LuJlMQgP9k2Xpd+iE04QsyD/qVhWz9TvfzZ
eAAILAPB4TwRVIOFSVfnMjVsSSwp95jy4Dxvpylwrpamq720qNiJ3ldqVWWuJR41
bv8/lvOICyznJqrYULXcB5Szz1f1/8La3bnNmVMrWwEy/1OG9d4Q3A84ytciaGRp
Kkk47RppqF/oOi+Z6Mo8wNXrM9zwR4jxQUezKcxwCmXMS1oVWNW1ZopCJwqjyBcdm

```

2、情况二：收到的证书由下方截图中的二个部分组成：

 241-156.ca-bundle	2018/11/2 星期...	CA-BUNDLE 文件	5 KB
 241-156.crt	2019/6/19 星期...	安全证书	7 KB

序号	文件名	文件描述
1	 241-156.ca-bundle	中间证书包 (中间证书 1 和中间证书 2 合并包)
2	 241-156.crt	网站证书文件

合并方法：

- 当配置 nginx 或 apache 文件时，需要将中间证书包和网站证书文件合并成一个，
- 操作方法：

分别用文本编辑器打开两个文件，将 Bundle 文件中的内容复制粘贴到网站证书文件的内容之后保存即可。

证书格式转换：

当客户的 web 服务是 IIS 或者是 tomcat 等时，需要对证书格式进行转换才能导入

方法一：用户可以使用 OPENSSSL 工具在命令行下进行转换（具体命令网上可以查询）；

crt 转 pfx:

```
openssl pkcs12 -export -out domain.pfx -inkey domain.key -in domain.crt -certfile
```

```
ca_bundle.crt
```

crt 转 jks:

网上搜索可以查到

方法二：使用转换工具：<https://www.chinassl.net/ssltools/convert-ssl.html>

如图所示，根据提示上传相应文件，即可转换。（原格式选择 pem）

选择文件和转换参数	
源格式: *	<input checked="" type="radio"/> PEM <input type="radio"/> PFX <input type="radio"/> DER
目标格式: *	<input type="radio"/> DER <input type="radio"/> P7B <input checked="" type="radio"/> PFX <input type="radio"/> JKS <input type="radio"/> PEM
证书文件: *	上传 ▾ <input type="button" value="选择文件"/> 未选择任何文件 ← 证书文件
私钥文件: *	上传 ▾ <input type="button" value="选择文件"/> 未选择任何文件 ← key文件
PFX证书密码: *	<input type="text" value="请设置6位以上密码。请记住输入的密码，非常重要"/>
证书别名:	<input type="text" value="默认值为证书域名，支持自定义别名，不支持中文"/>
根证书文件:	上传 ▾ <input type="button" value="选择文件"/> 未选择任何文件 ← root证书
证书链文件1:	上传 ▾ <input type="button" value="选择文件"/> 未选择任何文件 ← ca证书
证书链文件2:	上传 ▾ <input type="button" value="选择文件"/> 未选择任何文件

是否需要合并证书/转化证书格式?

1. 当配置 nginx 或 apache 服务器时，需要将中间证书和初级证书合并成一个，再加上单独使用的 key 文件再进行安装。

合并方法:

打开文本编辑器 (txt)，将初级证书和中间证书按照 初级证书代码→中间证书代码的顺序复制到文本中，保存为 crt 文件。（根证书在合并时可以不放，也可以放在除了第一顺序的任何其他顺序）

2. 当配置 IIS 或 Tomcat 服务器时，需要其他格式的证书，例如 JKS,则不用合并证书，而是转换证书。

证书格式转换方法:

方法一：用户可以使用 OPENSSL 工具在命令行下进行转换（具体命令网上可以查询）；

crt 转 pfx:

```
openssl pkcs12 -export -out domain.pfx -inkey domain.key -in domain.crt -certfile  
ca_bundle.crt
```

crt 转 jks:

网上搜索可以查到。

用户除了可使用命令行作为工具转化；也可用以下转换工具：

<https://www.chinassl.net/ssltools/convert-ssl.html>

如图所示，根据提示上传相应文件，即可转换。（原格式选择 pem）

选择文件和转换参数

源格式: *	<input checked="" type="radio"/> PEM <input type="radio"/> PFX <input type="radio"/> DER
目标格式: *	<input type="radio"/> DER <input type="radio"/> P7B <input checked="" type="radio"/> PFX <input type="radio"/> JKS <input type="radio"/> PEM
证书文件: *	<input type="button" value="上传"/> <input type="button" value="选择文件"/> 未选择任何文件 ← 证书文件
私钥文件: *	<input type="button" value="上传"/> <input type="button" value="选择文件"/> 未选择任何文件 ← key文件
PFX证书密码: *	<input type="text" value="请设置6位以上密码, 请记住输入的密码, 非常重要"/>
证书别名:	<input type="text" value="默认值为证书域名, 支持自定义别名, 不支持中文"/>
根证书文件:	<input type="button" value="上传"/> <input type="button" value="选择文件"/> 未选择任何文件 ← root证书
证书链文件1:	<input type="button" value="上传"/> <input type="button" value="选择文件"/> 未选择任何文件 ← ca证书
证书链文件2:	<input type="button" value="上传"/> <input type="button" value="选择文件"/> 未选择任何文件