国密 SM2 证书 Apache 安装指南-Linux

沃通电子认证服务有限公司

WoTrus CA Limited

目录

技术支持邮箱：support@wotrus.com

技术支持热线电话：0755-26027828 / 0755-26027859 / 0755-26027827

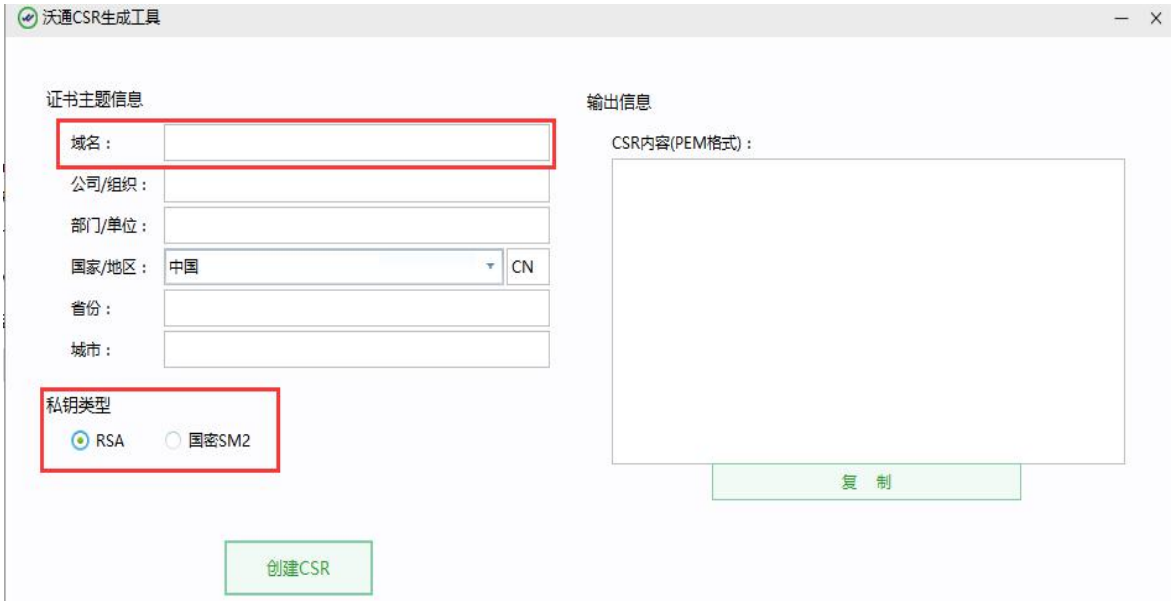
公司官网地址：https://www.wotrus.com

一、申请证书

1、下单：访问 https://buy.wotrus.com/，点击右上角“登录/注册”，登录后，选择需要申请的 SM2 SSL 证书类型，点击“立即购买”，填写相关信息，证书安装模式选择“**手动模式**”；

2、下载 CSR 生成工具：点击提交 CSR 上的 CSR 生成工具或者通过 https://download.wotrus.com/wotrus/WoTrusCSRTool.exe 下载生成 CSR 工具；

3、创建 CSR：运行 WoTrusCSRTool.exe，输入申请证书的域名(多域名证书任意输入其中一个域名即可)，点击创建 CSR，然后将 CSR 和私钥.key 保存下来(默认命名即可)，私钥类型选择 RSA 和国密 SM2 分别进行一次创建 CSR 的操作！



4、提交 CSR，完成订单提交！

二、环境准备

目前仅支持 Linux 环境下 Apache；

1、Linux 操作系统；

2、Apache 下载链接:http://httpd.apache.org/download.cgi；

3、国密 SM2 模块(根据系统版本，提供 V1 和 V2 两种版本国密模块，以 Centos 为例)

Centos 6 及以下版本: https://www.wotrus.com/download/wotrus_ssl_v1.tar.gz;

Centos 7 及以上版本: https://www.wotrus.com/download/wotrus_ssl.tar.gz;

4、沃通国密 SM2 SSL 证书;

三、安装证书

1、**安装 Apache**(文档以 apache-2.4.46 为例，目录为/usr/local，用户根据实际环境操作即可);

安装 apache 之前，先安装相关的依赖库，如果系统是全新的，请先安装 gcc/gcc-c++：yum install -y gcc　yum install -y gcc-c++;

(1) 、安装 apr：http://mirror.bit.edu.cn/apache//apr/apr-1.7.0.tar.gz，下载并上传 apr-1.7.0.tar.gz 至/usr/local 目录下：

解压：tar -zvxf apr-1.7.0.tar.gz

检测：cd apr-1.7.0

./configure --prefix=/usr/local/apr

编译：make && make install

(2) 、安装 apr-util：http://archive.apache.org/dist/apr/apr-util-1.5.4.tar.gz，下载并上传至/usr/local 目录下：(推荐使用 apr-util-1.5 的版本，1.6 的兼容性有问题)

解压：tar -zvxf apr-util-1.5.4.tar.gz

检测：cd apr-util-1.5.4

./configure　--prefix=/usr/local/apr-util --with-apr=/usr/local/apr

编译：make && make install

Ps:make 时如果出现`#include <expat.h> ^ compilation terminated.`的报错，请`yum install -y expat-devel`安装依赖库。

(3) 、安装 pcre：连网状态下，可执行命令 yum install -y pcre-devel 或者通过

https://ftp.pcre.org/pub/pcre/pcre-8.43.tar.gz 下载并上传至/usr/local 目录下：

解压：tar -zvxf pcre-8.43.tar.gz

检测：cd pcre-8.43

./configure --prefix=/usr/local/pcre

编译：make && make install

(4) 、上述三个文件编译安装完成后，将下载的 apache 国密版和国密模块也上传至/usr/local 目录下：

解压：tar -zvxf wotrus_ssl.tar.gz

tar -zvxf apache-2.4.46.tar.gz

检测：cd apache-2.4.46

./configure --prefix=/usr/local/httpd --enable-so --enable-ssl --enable-cgi --enable-rewrite --enable-modules=most --enable-mpms-shared=all --with-mpm=prefork --with-zlib --with-apr=/usr/local/apr --with-apr-util=/usr/local/apr-util --with-ssl=/usr/local/wotrus_ssl (v1 版本为 wotrus_ssl，v2 版本为 wotrus_ssl2)

Ps:以上只编译了部分模块，如有需求，请用户自行添加需要的模块

编译：make

make install

Ps:上述步骤中的目录皆是测试环境的目录，具体路径，请根据实际用户环境！

2、配置 SSL

(1)、下载 SSL 证书，申请证书后，将下载得到三个.zip 的压缩包，分别是 RSA 证书，SM2 签名证书和加密证书，分别解压得到 for apache.zip/ApacheServer 里面的 crt 文件；

(2)、上传 SSL 证书，cd 进入/usr/local/httpd/conf，新建 cert 目录，将上面解压的 crt 文件以及创建 CSR 时生成的两个.key 文件(分别是 rsa 和 sm2 命名的 key 文件)上传至

该目录；

(3)、 配置 SSL 证书，进入/usr/local/httpd/conf，vi/vim 编辑 httpd.conf 文件，找到 #LoadModule ssl_module modules/mod_ssl.so，去掉前面的注释符#，增加 Include conf/ssl.conf，保存退出后在/usr/local/httpd/conf，vi/vim 新建一个 ssl.conf 文件，增加如下配置:

Listen 443

<VirtualHost *:443>

ServerName domain.com

DocumentRoot website 根目录

SSLEngine on

#RSA config

SSLCertificateFile /usr/local/httpd/conf/domain.com.crt

SSLCertificateKeyFile /usr/local/httpd/conf/domain.com_rsa.key

SSLCertificateChainFile /usr/local/httpd/conf/root_bundle.crt

#SM2 sign config

SSLCertificateFile /usr/local/httpd/conf/domain.com_sign.crt

SSLCertificateKeyFile /usr/local/httpd/conf/domain.com_sm2.key

SSLCertificateChainFile /usr/local/httpd/conf/bundle.crt

#SM2 encrypt config

SSLCertificateFile /usr/local/httpd/conf/domain.com_en.crt

SSLCertificateKeyFile /usr/local/httpd/conf/domain.com_sm2.key

SSLCertificateChainFile /usr/local/httpd/conf/bundle.crt

#sign 和 encrypt 配置中的.key 和 bundle.crt 为同一个

SSLProtocol all -SSLv2 -SSLv3

SSLCipherSuite

ECC-SM4-SM3:ECDH:AESGCM:HIGH:MEDIUM:!RC4:!DH:!MD5:!aNULL:!eNULL

```
SSLHonorCipherOrder on
  <Directory "website 根目录">
     Options -Indexes -FollowSymLinks +ExecCGI
     AllowOverride None
     Order allow,deny
     Allow from all
     Require all granted
  </Directory>
</VirtualHost>
```

以上仅为参考(http 的配置请自行处理)，具体的 ServerName，证书名称，证书目录，Directory 等配置请根据实际环境配置！

(4)、检测：/usr/local/httpd/bin/httpd -t,若提示 Syntax OK，则表示配置正常，可以启动 apache。

如果有提示错误，请根据提示排查错误，直到显示正常！

(5)、启动：执行/usr/local/httpd/bin/httpd -k start，启动 apache！

四、检测 SSL 配置

下载沃通密信浏览器测试 https 访问，下载地址:https://www.mesince.com/zh-cn/browser 下载安装后，打开浏览器，在地址栏输入 https://domain.com(证书实际绑定域名)测试是否能正常访问以及显示小绿锁，如无法正常访问，请确保防火墙或安全组等策略有放行 443 端口（SSL 配置端口）。

五、备份 SSL 证书

请将下载的.zip 压缩包和自主生成的私钥.key 文件备份，以防丢失，影响后续使用！