

国密 SM2 证书 Nginx 安装指南



沃通电子认证服务有限公司

WoTrus CA Limited

目录

一、 申请证书.....	2
二、 环境准备.....	3
三、 安装证书.....	4
四、 检测 SSL 配置.....	6
五、 备份 SSL 证书.....	7

技术支持邮箱: support@wotrus.com

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

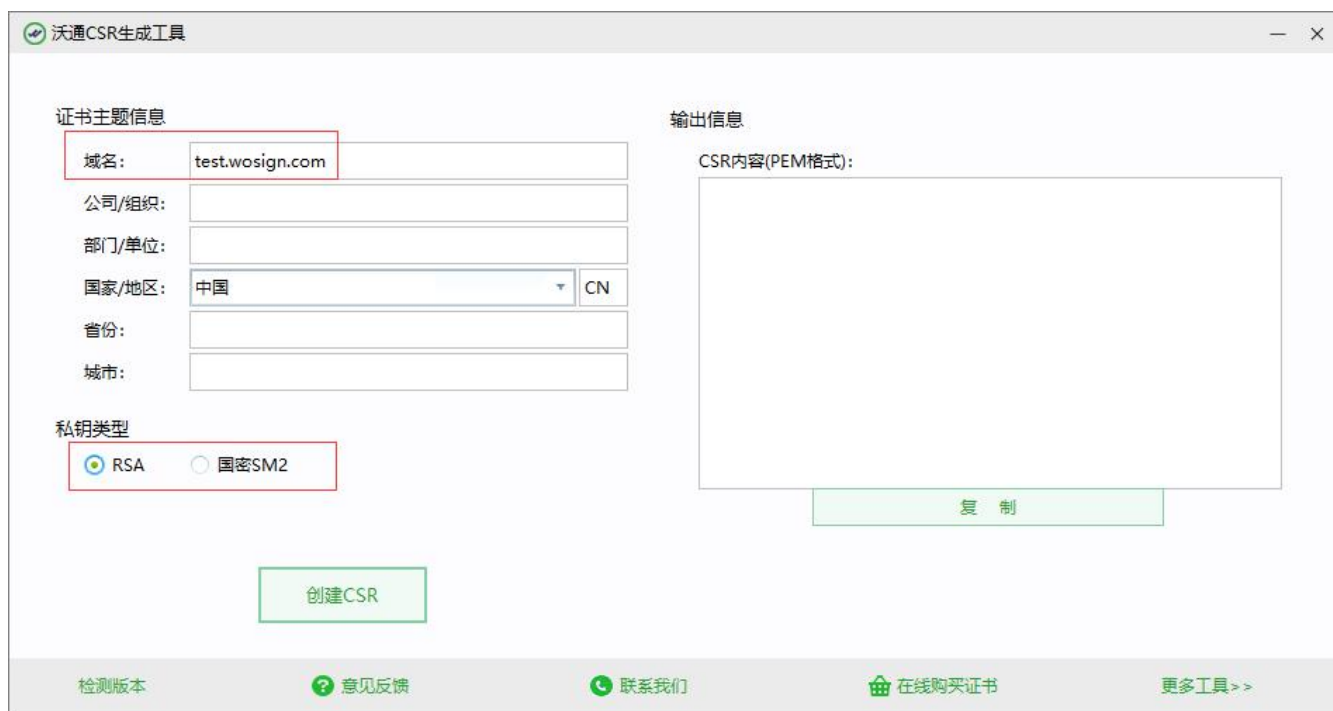
公司官网地址: <https://www.wotrus.com>

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

- 1、Linux 操作系统；
- 2、Nginx -1.14.2 及以上版本（推荐使用**最新稳定版**），附下载链接：<http://nginx.org/en/download.html>；
- 3、国密 SM2 模块，下载链接 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 Nginx**(文档以 **nginx-1.15.12** 为例，目录为 **/usr/local**，用户根据实际环境操作即可)；

在安装 nginx 前，需要确保系统安装了 gcc-c++、pcre-devel 和 zlib-devel 软件。

(1)、将上述步骤下载的 nginx 压缩包和 wotrus_ssl.tar.gz，上传至 linux 操作系统 **/usr/local/** 目录下，分别解压；

(2)、cd 进入 nginx 的解压目录 **/usr/local/nginx-1.15.12**，执行 **./configure --prefix=/usr/local/nginx --with-http_stub_status_module --with-stream --with-http_ssl_module --with-stream_ssl_module --with-openssl=/usr/local/wotrus_ssl**(这里只指定了几个需要的模块，其他模块用户可自行增加)；

(3)、上述步骤执行完成后，再输入 **make && make install**，编译 nginx。执行该步骤后，若无报错，则表示编译成功，可以开始配置证书；如果执行过程中出现

```
make[1]: *** [/usr/local/wotrus_ssl//.openssl/include/openssl/ssl.h] 错误 127  
make: *** [build] Error 2
```

如上图显示的错误，则需要进入 **nginx-1.15.12/auto/lib/openssl** 目录，

vi/vim 编辑 conf 文件(可先备份)，找到下面所示的四行代码：

```
CORE_INCS="$CORE_INCS $OPENSSL/.openssl/include"  
CORE_DEPS="$CORE_DEPS $OPENSSL/.openssl/include/openssl/ssl.h"  
CORE_LIBS="$CORE_LIBS $OPENSSL/.openssl/lib/libssl.a"  
CORE_LIBS="$CORE_LIBS $OPENSSL/.openssl/lib/libcrypto.a"
```

改为：

```
CORE_INCS="$CORE_INCS $OPENSSL/include"  
CORE_DEPS="$CORE_DEPS $OPENSSL/include/openssl/ssl.h"  
CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libssl.a"  
CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libcrypto.a"
```

保存后，先执行 make clean,再重新执行(2)步骤的./configure 和(3)步骤的 make && make install;

(4)、编译完成后，cd 进入/usr/local/nginx 目录，用

/usr/local/nginx/sbin/nginx -t 检测是否正常，正常则输入 usr/local/nginx/sbin/nginx 启动 nginx;

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，将下载得到两个.zip 的压缩包，分别是 SM2 签名证书和加密证书，分别解压得到 for nginx.zip 里面的 crt 文件；

(2)、上传 SSL 证书，cd 进入/usr/local/nginx/conf，新建 sm2 目录，将上面解压的两个 crt 文件以及创建 CSR 时生成的两个.key 文件(签名证书对应 domain.com_sign.key, 加密证书对应 domain.key_en.key)上传至该目录；

(3)、配置 SSL 证书，进入/usr/local/nginx/conf，vi/vim 编辑 nginx.conf 文件，增加如下配置，然后保存：

```
server {
```

```
listen          443 ssl;

server_name    domain.com;

ssl_certificate /usr/local/nginx/conf/sm2/domain.com_rsa.crt;
ssl_certificate_key /usr/local/nginx/conf/sm2/domain.com_rsa.key;

ssl_certificate /usr/local/nginx/conf/sm2/domain.com_sign.crt;
ssl_certificate_key /usr/local/nginx/conf/sm2/domain.com_sm2.key;

ssl_certificate /usr/local/nginx/conf/sm2/domain.com_en.crt;
ssl_certificate_key /usr/local/nginx/conf/sm2/domain.com_sm2.key;
#先配置签名证书，再配置加密证书，签名加密证书私钥 key 为同一个！

ssl_session_timeout 5m;

ssl_protocols    TLSv1 TLSv1.1 TLSv1.2;

ssl_ciphers

SM2-WITH-SMS4-
SM3:ECDH:AESGCM:HIGH:MEDIUM:!RC4:!DH:!MD5:!aNULL:!eNULL;

ssl_prefer_server_ciphers    on;

location / {
    root    html;
    index  index.html index.htm;
}
}
```

以上仅为参考，具体的 `server_name`，证书名称，证书存放目录，`location` 等配置请根据实际环境配置！

(4)、检测，执行 `/usr/local/nginx/sbin/nginx -t`，看配置是否正常，正常显示如下图：

```
[root@localhost nginx-1.15.12]# /usr/local/nginx/sbin/nginx -t
Use GM signing certificate.
Use GM signing private key.
Use GM encryption certificate.
Use GM decryption private key.
nginx: the configuration file /usr/local/nginx/conf/nginx.conf syntax is ok
nginx: configuration file /usr/local/nginx/conf/nginx.conf test is successful
```

如果有提示错误，请根据提示排查错误，直到显示正常！

(5)、重启 nginx：执行/usr/local/nginx/sbin/nginx -s reload，重启 nginx！

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！