国密 SM2 证书 Nginx 安装指南-Windows 版

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

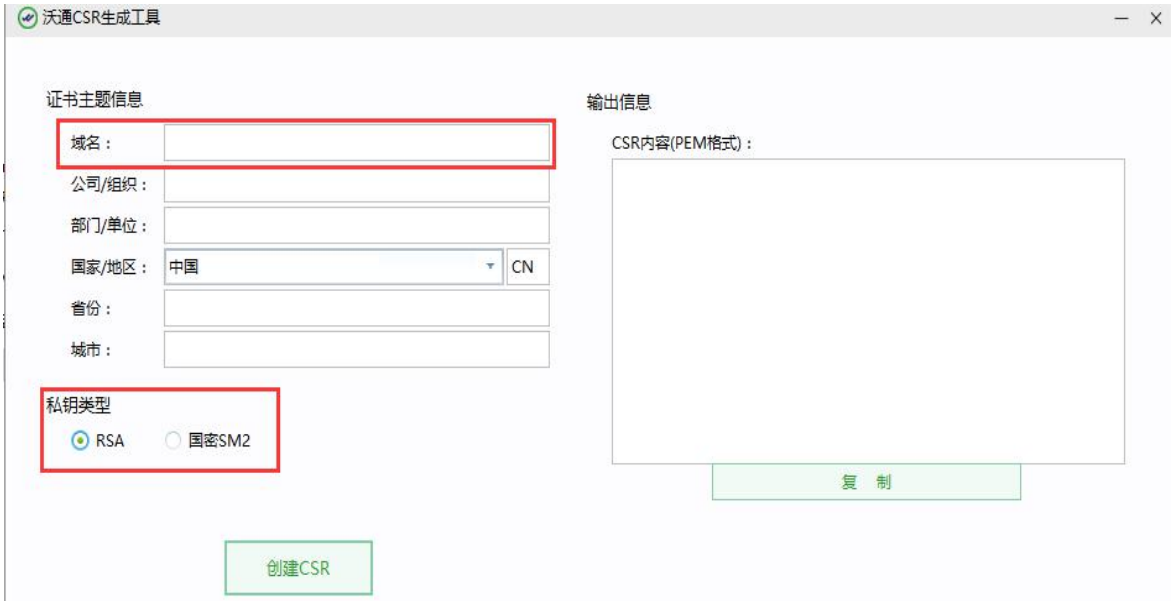
公司官网地址：https://www.wotrus.com

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

1、Windows 操作系统；

2、Nginx 国密版，附下载链接：

64 位操作系统：https://www.wotrus.com/download/gm_nginx-1.16.1.zip

32 位操作系统：https://www.wotrus.com/download/gm_nginx-1.18.0.zip

3、沃通国密 SM2 SSL 证书；

三、安装证书

安装和配置 Nginx(文档以 nginx-1.16.0(x64)/nginx-1.17.0(x86)为例，目录为 D:\gmssl，用户根据实际环境操作即可)；

(1) 、根据操作系统版本(32/64 位)，选择对应的 nginx 压缩包，复制到服务器上，并解压到相应的目录，如 d:\gmssl;

(2) 、在 nginx 的目录下(如 conf)创建存放证书的文件夹，如 ssl；

(3) 、解压从沃通下载的证书压缩包，将每个压缩包 for nginx 中的 crt 文件和创建 CSR 时保存的.key 文件放到第(2)步创建的文件夹下(共三个.crt,两个.key)；

(4) 、编辑 nginx/conf 目录下 nginx.conf 文件，在 http{}中，添加 include ssl.conf;

(5) 、在 nginx/conf 目录下，新建 ssl.conf 文件；

(6) 、编辑新建的 ssl.conf 文件，添加证书配置，如下所示:

```
server {
        listen          443 ssl;
        server_name     domain.com;
        ssl_certificate         d:/gmssl/nginx-1.16.0/conf/ssl/domain.com_rsa.crt;
        ssl_certificate_key     d:/gmssl/nginx-1.16.0/conf/ssl/domain.com_rsa.key;

        ssl_certificate         d:/gmssl/nginx-1.16.0/conf/ssl/domain.com_sign.crt;
        ssl_certificate_key     d:/gmssl/nginx-1.16.0/conf/ssl/domain.com_sm2.key;

        ssl_certificate         d:/gmssl/nginx-1.16.0/conf/ssl/domain.com_en.crt;
        ssl_certificate_key     d:/gmssl/nginx-1.16.0/conf/ssl/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;
            }
    }
```

PS:建议用 Administrator 账户配置证书，若用非管理员权限账户配置，可能出现找不到证书的错误！

以上配置仅为参考，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！

(7)、检测，在服务器 dos 命令下，cd 进入 nginx 目录，如 cd d:\gmssl\nginx-1.16.0，输入 nginx -t，检测 nginx 配置是否正常，正常显示如下图:

```
D:\gmssl\nginx-1.16.0>nginx -t
Use GM signing certificate.
Use GM signing private key.
Use GM encryption certificate.
Use GM decryption private key.
nginx: the configuration file D:\gmssl\nginx-1.16.0/conf/nginx.conf syntax is ok
nginx: configuration file D:\gmssl\nginx-1.16.0/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)、启动 nginx：进入 nginx 目录，双击运行 nginx.exe！

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！