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

©2004-2024 沃通电子认证服务有限公司 WoTrus CA Limited All Rights Reserved

目录

一、 环境准备 2
二、 安装证书 3
三、 检测 SSL 配置 5
四、 备份 SSL 证书 5

技术支持邮箱：supp3@wotrus.com

技术支持热线电话：18822828659 / 0755-26027827

公司官网地址：https://www.wotrus.com

一、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/nginx-1.16.1.zip

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

3、沃通国密 SM2 、RSA SSL 证书；

二、安装证书

安装和配置 Nginx(文档以 nginx-1.16.0 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，将得到三个文件夹，将每个文件夹下 NginxServer 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)；

名称	修改日期	类型
test.wosign.com_rsa	2024/2/26 14:04	文件夹
test.wosign.com_sm2_encrypt	2024/2/26 14:04	文件夹
test.wosign.com_sm2_sign	2024/2/26 14:04	文件夹

(4) 、编辑 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:w

```
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      TlSv1.1 TLSv1.2 TLSv1.3;
ssl_ciphers
ECC-SM4-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！

三、检测 SSL 配置

下载沃通密信浏览器测试 https 访问，下载地址:

https://download.wosign.com/wosign/MeSignBrowser_setup.exe

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国密字样，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）。

四、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！