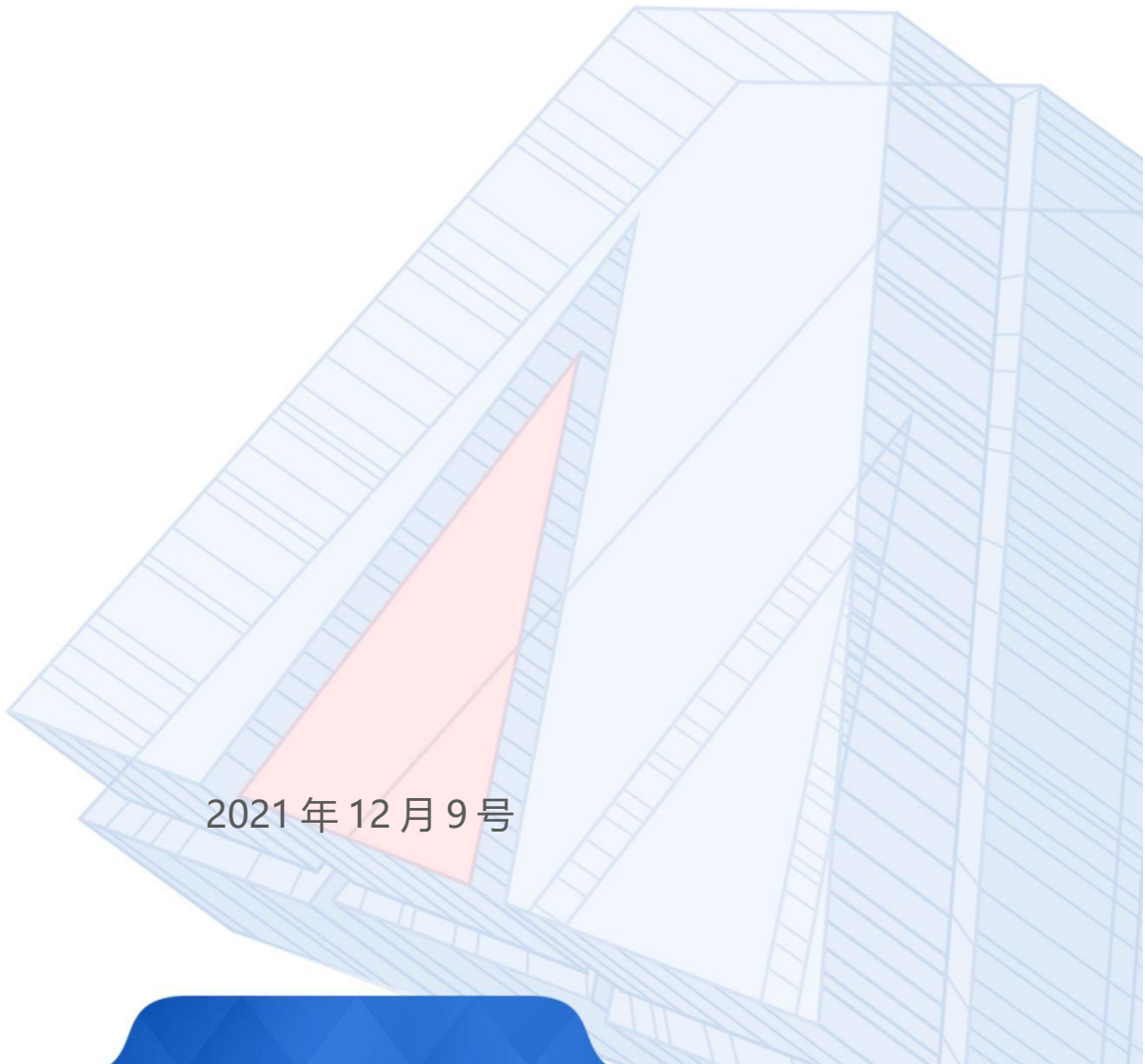
CFCA 中国金融认证中心
China Financial Certification Authority

国密服务器证书技术支持手册

CFCA SERVICE REPORT OF CHINA MINSHENG BANK

卓越创新科技 智享信息安全



2021年12月9号

文档修订记录

本文档会随时保持更新，请与中金金融认证中心有限公司索要最新版本

版本	内容	日期	编写	审核
1.0.0.0	编写文档	2021/12/9	陈超	施威
1.0.2.0	增加 nginx 部署内容	2022/6/14	李浩	陈超
1.0.2.1	增加 cfca nginx 部署内容 增加常见问题章节	2022/9/13	李浩	陈超
1.0.3.0	修改证书下载流程	2023/10/23	李浩	陈超

注：对该文件内容增加、删除或修改须填写此修订记录，详细记载变更信息，以保证其可追溯性。

目录

一、引言

为便于指导客户下载、部署国密服务器证书，加强客户服务沟通效率，特编写本手册用于说明国密通服务器证书的下载、部署流程。

二、国密服务器证书下载流程

特别说明：本文档是基于 SM2 算法、 密钥位数为 256 的服务器证书下载流程，

1、下载到硬件设备

国密服务器证书在下载前需要通过网关、硬件加密机等硬件设备上提前生成 p10 申请书，具体申请方法请与硬件厂商联系。

图 1 Web 服务器证书下载界面

2、软证书下载

（1）利用 CFCA SSL 证书管理系统 (需联系我司技术人员获取) 生成 CSR，密钥类型选择国密算法（SM2），生成 CSR 填写的信息一定要和申请证书时所填写的信息一致。

图 2 CSR 信息填写界面

（2）当用户输入的所有信息符合 DN 规则，然后点击“生成 CSR”按钮时，CFCA SSL 证书管理系统会弹出一个新的对话框，其中包含了 CSR（PKCS#10 证书）、签名私钥，用户可以选择复制或以文件形式保存到本地目录。

图 3 CSR 和密钥生成界面

（3）用户可使用 PKCS#10 证书并配合两码，从 CFCA 统一下载平台下载国密证书。

图 4Web 服务器证书下载界面

（4）依次保存签名证书、加密证书、加密私钥。加密私钥可以直接复制保存，可命名为未解密.key，稍后用于解密。注意：p7b 文件是证书链，不是加密私钥，可不下载，证书链可找我司技术单独提供。

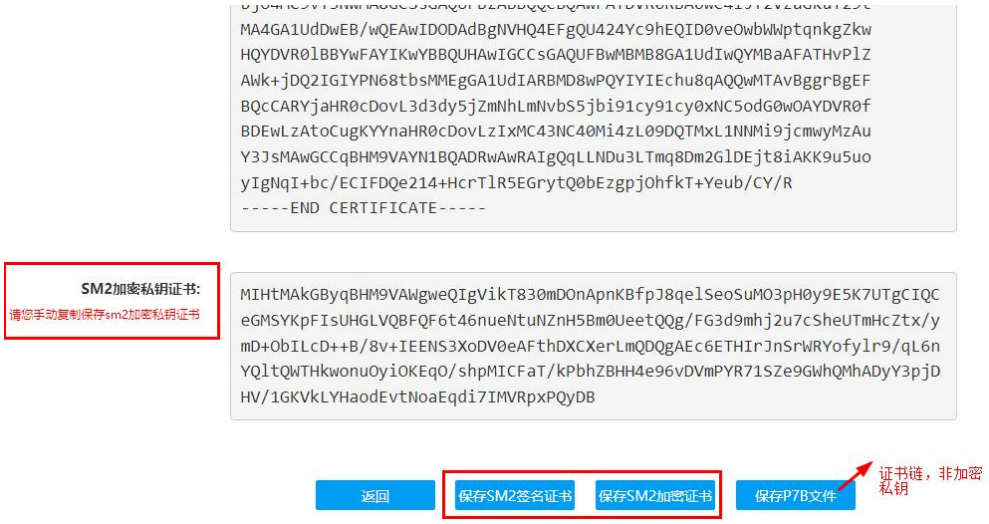


图 5 证书和私钥保存页面

（5）加密私钥是加密过的，不能直接应用，需要解密，在工具中上传页面保存的未解密的加密私钥文件、签名证书私钥文件，选择解密后加密私钥保存路径，点击解密，在对应目录下就可得到的解密后的加密私钥。

图 6 加密私钥密文解密

（6）到此，我们下载好了完整的国密软证书，包括签名证书、签名私钥、加密证书、解密后的加密私钥。

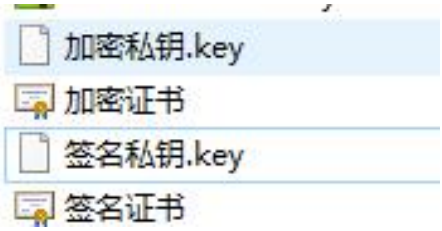


图 7 国密软证书合集

三、证书部署

硬件设备上的国密证书部署，请咨询对应的硬件设备厂商。国密证书部署到中间件上，需要先获取中间件支持国密的版本，目前主流的部分国密开源中间件有 gmssl 的国密 nginx、tomcat，江南天安的国密 nginx。这些版本有时效限制或需要收费，具体请自行联系相关厂商获取。

目前我司也有一款 nginx 国密中间件，但有时效限制，截止到 2024 年 1 月 1 日前可正常使用，到此日期后，停服或更改配置后均无法正常启动，届时如有需要，需联系我司技术获取新版本。

1、本次主要以 gmssl 的国密 tomcat 版本重点介绍。

（1）自行下载 8.5 以上 tomcat，登录 https://www.gmssl.cn/gmssl/index.jsp，下载 tomcat 国密编译包。

编号	描述	文件	长度	MD
1	openssl国密版	gmssl_openssl_1.1_b4.tar.gz	6,255,702	944eb3adb159fb75f
2	nginx国密版	gmssl_nginx_1.8.0_b10.tar.gz	5,417,131	e8ad8721470268666
3	Apache httpd国密版	gmssl_httpd_2.4.46_b8.tar.gz	17,247,573	bf9d759847e038e64
4	SM2可信证书链	demo1.sm2.trust.pem	1,410	0039c14a1076c41c1
5	SM2签名测试证书	demo1.sm2.sig.crt.pem	753	44cfd3a4d0abeaf5d
6	SM2签名测试私钥	demo1.sm2.sig.key.pem	205	5951c00986b0a7792
7	SM2加密测试证书	demo1.sm2.enc.crt.pem	753	643866f06be1dfaab
8	SM2加密测试私钥	demo1.sm2.enc.key.pem	205	14fc5ffff70217190
9	RSA可信证书链	demo1.rsa.trust.pem	2,474	4ba11046c6f0f1889
10	RSA测试证书	demo1.rsa.crt.pem	1,326	214c54d7712fcd8ef
11	RSA测试私钥	demo1.rsa.key.pem	1,679	e14fc6b7d2af2f11c
12	国密Java开发包	gmssl_provider.jar	3,565,886	9624bd00215bbcd77
13	Tomcat国密组件	gmssl4t.jar	9,326	fb10a0e33393ba0fa
14	SM2双证书/私钥	sm2.pfx	1,822	c0cee99ddf2107477
15	SM2双证书/密钥与RSA证书/私钥	sm2_rsa.pfx	4,235	b60b1925610dd43b7

图 8 tomcat 国密编译包下载

（2）安装 jdk8，需安装 1.8.0_151 及以上的 jdk，并对 jdk 进行国密编译和加密模式解锁。

国密 Java 包 gmssl_provider.jar 放到 JRE 的 lib/ext/目录下

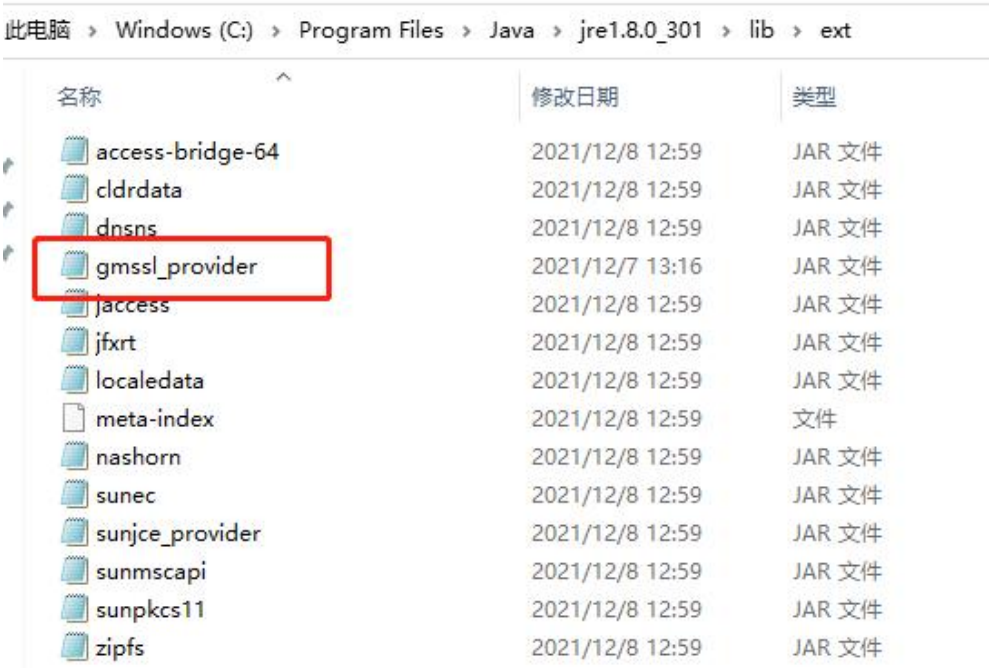


图 9 对 JDK 国密编译

打开 JRE 的\lib\security 目录下的 java.security 文件，找到 crypto.policy=unlimited，去掉#注释。

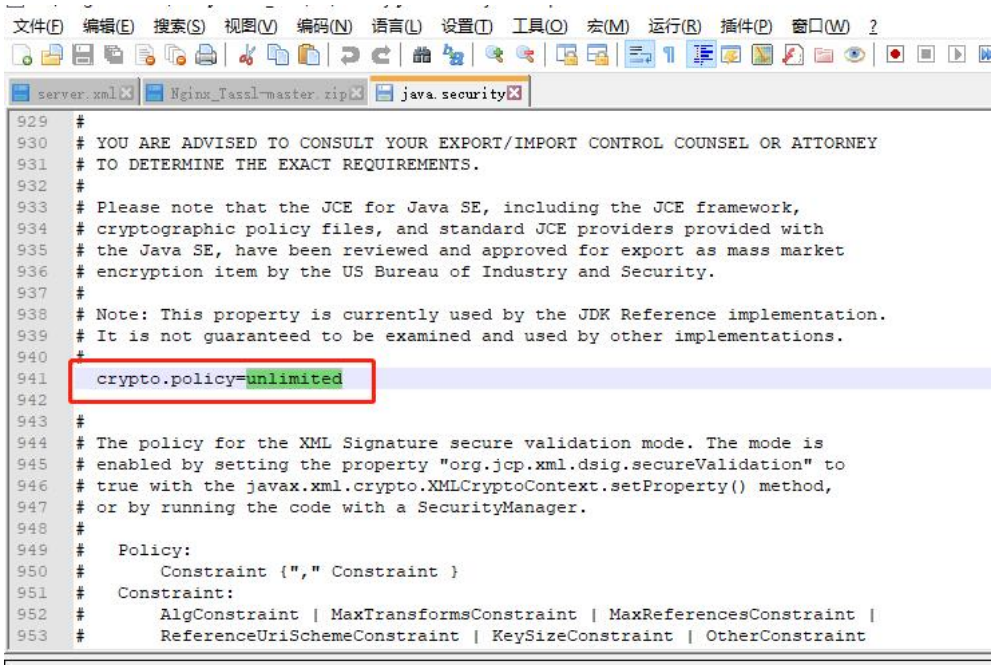


图 10 JDK 加密模式解锁

(3)Tomcat 国密组件 gmssl4t.jar 放到 tomcat 的 lib 目录下,到此 tomcat 国密环境已编译完成。

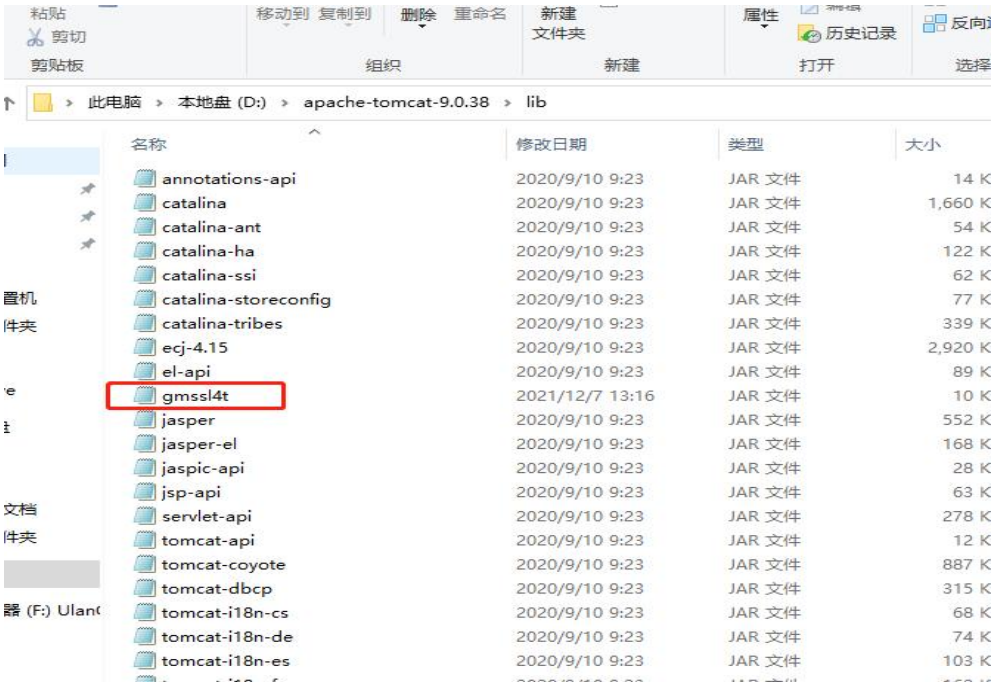


图 11 tomcat 国密编译

(4) 制作国密 tomcat 所需的证书，证书格式为 pfx。打开 CFCA SSL 证书管理系统，分别上传前面制作完成的签名证书、签名私钥、加密证书、解密后的加密私钥，选择要保存的 PFX 文件路径，设置 PFX 文件的密码。点格式转

换按钮，即会在对应目录产生对应的 PFX 文件。

在上传证书文件时，可以按 CTRL 键选择两个证书文件，实现上传两个证书文件，上传私钥文件同理。

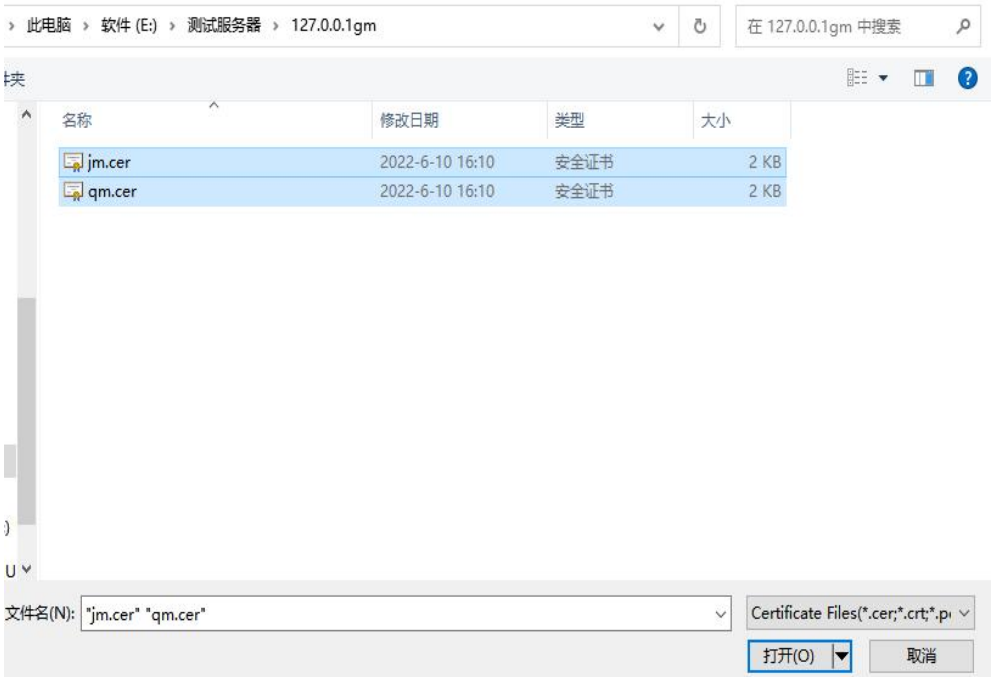


图 12 选择证书文件

图 13 证书格式转换界面

（5）配置 tomcat 下 conf 下的 server.xml 文件进行国密证书部署。

单向配置示例：

```
<Connector port="443"
protocol="HTTP/1.1"
SSLEnabled="true"
sslImplementationName="cn.gmssl.tomcat.GMSSLImplementation"
sslProtocol="GMSSLv1.1"
keystoreFile="/root/sm2.pfx"
keystoreType="PKCS12"
keystorePass="12345678">
</Connector>
```

双向配置示例：

```
<Connector port="443"
protocol="HTTP/1.1"
SSLEnabled="true"
clientAuth="true"
sslImplementationName="cn.gmssl.tomcat.GMSSLImplementation"
sslProtocol="GMSSLv1.1"
keystoreFile="/root/sm2.pfx"
keystoreType="PKCS12"
keystorePass="12345678">
</Connector>
```

实际配置案例：

```
    -->
    <Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
    <!-- A "Connector" using the shared thread pool-->
    <!--
    <Connector executor="tomcatThreadPool"
               port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
    -->
    <Connector port="443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
SSLEnabled="true"
maxThreads="150"  clientAuth="false"
sslImplementationName="cn.gmssl.tomcat.GMSSLImplementation"
sslProtocol="GMSSLv1.1"
keystoreFile="E:\sm3.pfx"
 keystoreType="PKCS12"
 keystorePass="123456"
 ciphers=
```

图 14 tomcat 配置案例

（6）配置后启动 tomcat，并查看验证配置后的效果。

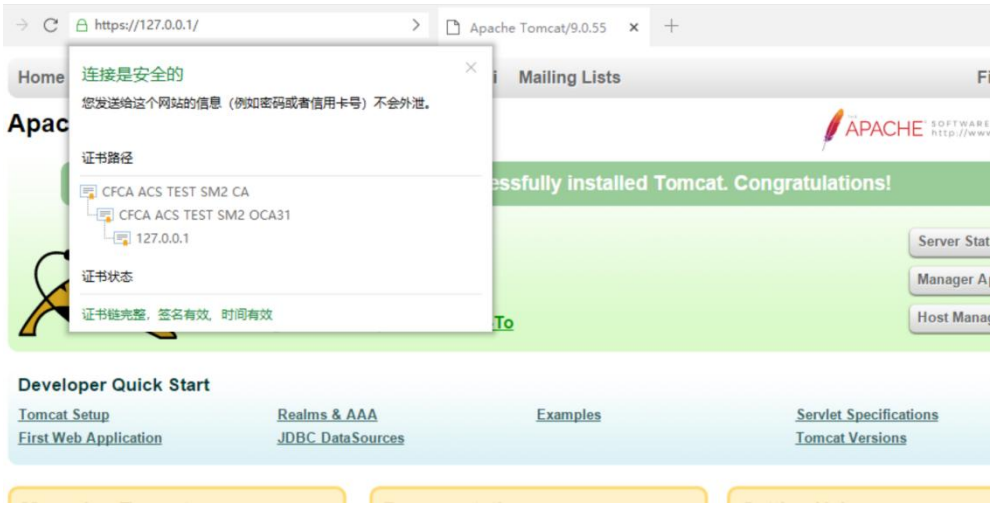


图 15 网页访问验证

2、国密版 nginx 服务器部署

若需使用国密版 nginx 部署国密服务器证书，请自行购买对应国密 nginx 版本。本次以 gmssl 的国密 nginx 中间件和 cfca 的国密 nginx 中间件为例，进行部署流程说明。

2.1、gmssl 国密 nginx 部署

gmssl 网站上的国密中间件，主要是用国密版 openssl 工具对标准 nginx

进行编译后，获得国密版 nginx，相关工具见 gmssl 网站，具体部署流程如下：

（1）本次运行环境 Centos7 x86_64，请确保相关依赖库都已安装，如 pcre-devel。

（2）准备 gmssl_openssl：登录 https://gmssl.cn/gmssl/index.jsp 下载国密 openssl 工具包。

编号	描述	文件	长度	MD5
1	openss1国密版	gmssl_openssl_1.1_b6.tar.gz	6,298,627	2db6f20bcde89819a7d955efa9e8
2	SM2可信证书链	demo1.sm2.trust.pem	1,410	0039c14a1076c41c1d1d2e04a465
3	SM2签名测试证书	demo1.sm2.sig.crt.pem	753	44cfd3a4d0abeaf5d8cfb170e3a5
4	SM2签名测试私钥	demo1.sm2.sig.key.pem	205	5951c00986b0a7792db129cc5920
5	SM2加密测试证书	demo1.sm2.enc.crt.pem	753	643866f06be1dfaab670a1a7e4eb
6	SM2加密测试私钥	demo1.sm2.enc.key.pem	205	14fc5ffff70217190de34f939a52
7	RSA可信证书链	demo1.rsa.trust.pem	2,474	4ba11046c6f0f188945759db1b98
8	RSA测试证书	demo1.rsa.crt.pem	1,326	214c54d7712fcd8eff0534af5faa
9	RSA测试私钥	demo1.rsa.key.pem	1,679	e14fc6b7d2af2f11cf376b956a5e
10	国密Java开发包	gmssl_provider.jar	3,559,368	99ed2373bd6ad7eebc06b0dbde97
11	Tomcat国密组件	gmssl4t.jar	9,326	b781b3b4b561f56cf1f016e885a3
12	SM2双证书/私钥	sm2.pfx	1,822	c0cee99ddf21074774f7b3332d68
13	SM2双证书/密钥与RSA证书/私钥	sm2_rsa.pfx	4,235	b60b1925610dd43b7d15cebb54df

图 16 openssl 工具包下载

拷贝 gmssl_openssl_1.1_b6.tar.gz 到/root/目录。

解压 gmssl_openssl 到指定目录。

tar xzfm gmssl_openssl_1.1_bxx.tar.gz -C /usr/local。

/usr/local/gmssl 为国密版 openssl 目录。

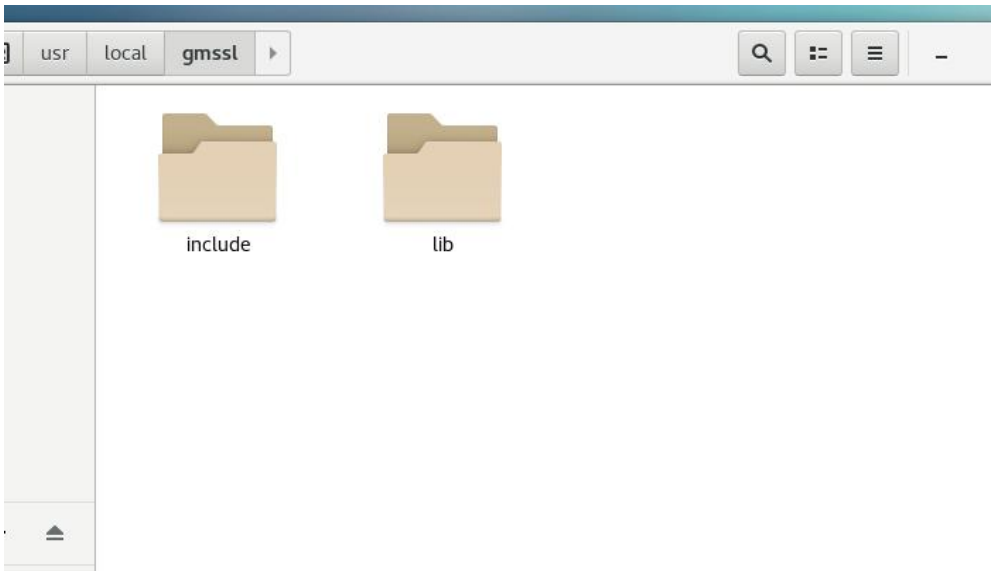


图 17 openssl 目录

（3）准备 nginx：gmssl 支持 nginx1.6 以上，自行下载 nginx 标准版，下载页面 http://nginx.org/download/。

将下载的 nginx 拷贝到/root/目录下。

解压 tar xzfm nginx-1.18.0.tar.gz。/root/nginx-1.18.0 为 nginx 目录。

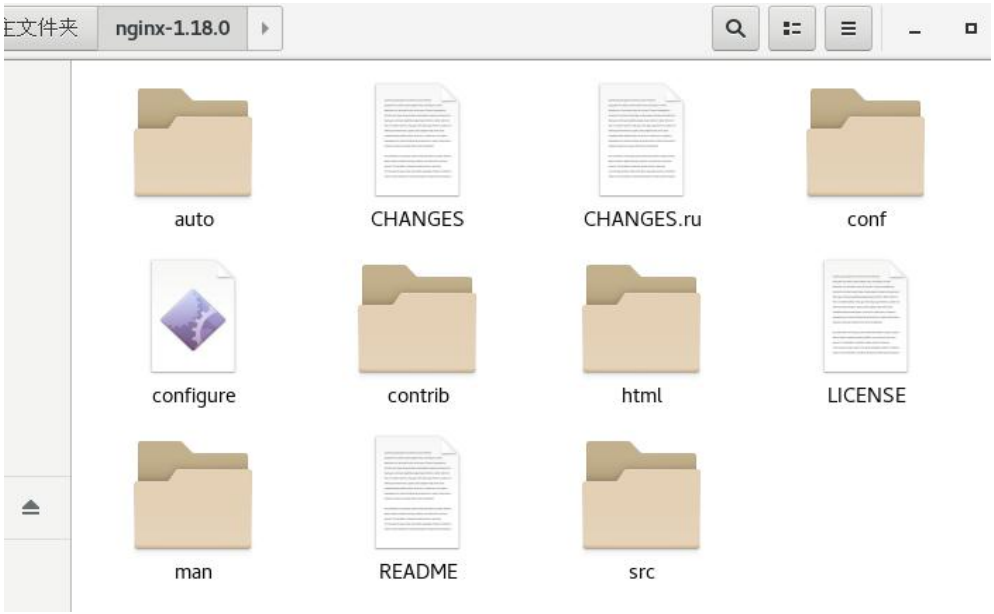


图 18 nginx 目录结构

进入 nginx 目录 cd /root/nginx-1.18.0

编辑 auto/lib/openssl 目录下的 conf 文件，将全部$OPENSSL/.openssl/修改为$OPENSSL/并保存，至此 nginx 方面准备工作已做好。

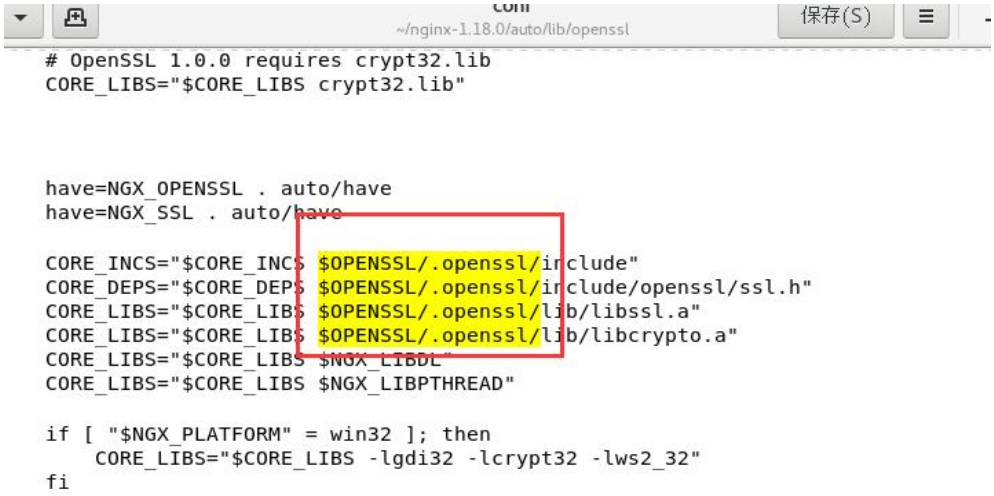


图 19 nginx 配置文件修改

（4）编译配置，获取 nginx 国密版。

进入 nginx 目录 cd /root/nginx-1.18.0，输入以下信息进行编译配置，其中涉及到的路径为 gmssl_openssl 解压后的路径。

```
./configure \
--without-http_gzip_module \
--with-http_ssl_module \
--with-http_stub_status_module \
--with-http_v2_module \
--with-file-aio \
--with-openssl="/usr/local/gmssl" \
--with-cc-opt="-I/usr/local/gmssl/include" \
--with-ld-opt="-lm"
```

执行编译安装命令 make install，然后/usr/local/nginx 目录下会生成国密版的 nginx。

（5）国密证书部署，nginx 可使用 key+crt 格式的证书，可用上述第 2.2 软证书下载章节中最终获取的签名证书、签名私钥、加密证书、解密后的加密私钥，其中 cer 文件可直接改后缀为 crt 文件。

对于证书链的添加，一般只用国密签名证书里面添加证书链就行，可用记事本打开签名证书 crt 文件和中级证书、根证书文件。将中级证书和根证书编码按下图顺序复制进签名 crt 文件后保存（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）。相关证书链文件可自行登录 cfca 官网下载专区中下载，http://www.cfca.com.cn/zhengshuzizhu/，或找我司技术单独提供。

图 20 证书链结构示例

注意如需用 360 国密浏览器访问，则签名、加密公钥中都需要加入证书链。

进入到国密 nginx 目录，/usr/local/nginx/conf，编辑目录下的 nginx.conf 文件，配置国密 ssl。

配置示例(国密单向)：

```
server
{
  listen 0.0.0.0:443 ssl;
  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
  ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA:DES-CBC3-SHA:ECC-SM4-CBC-SM3:ECC-SM4-GCM-SM3;
  ssl_verify_client off;

  ssl_certificate /usr/local/nginx/conf/demo1.sm2.sig.crt.pem;
  ssl_certificate_key /usr/local/nginx/conf/demo1.sm2.sig.key.pem;

  ssl_certificate_key /usr/local/nginx/conf/demo1.sm2.enc.key.pem;
  ssl_certificate /usr/local/nginx/conf/demo1.sm2.enc.crt.pem;

  location /
```

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

配置示例(国密双向):

```
server
{
  listen 0.0.0.0:443 ssl;
  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
  ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA:DES-CBC3-SHA:ECC-SM4-CBC-SM3:ECC-SM4-GCM-SM3;
  ssl_client_certificate /usr/local/nginx/conf/demo1.sm2.trust;
  ssl_verify_client on;

  ssl_certificate /usr/local/nginx/conf/demo1.sm2.sig.crt.pem;
  ssl_certificate_key /usr/local/nginx/conf/demo1.sm2.sig.key.pem;

  ssl_certificate /usr/local/nginx/conf/demo1.sm2.enc.crt.pem;
  ssl_certificate_key /usr/local/nginx/conf/demo1.sm2.enc.key.pem;

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

实际配置案例:

```
    # HTTPS server
    #
server
{
  listen 0.0.0.0:443 ssl;
  server_name  192.168.126.128;
  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
  ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA:DES-CBC3-SHA:ECC-SM4-CBC-SM3:ECC-SM4-GCM-SM3;
  ssl_verify_client off;

  ssl_certificate /usr/local/nginx/conf/qm.crt;
  ssl_certificate_key /usr/local/nginx/conf/qm.key;

  ssl_certificate_key /usr/local/nginx/conf/jm.key;
  ssl_certificate /usr/local/nginx/conf/jm.crt;

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

图 21 nginx 配置示例

配置说明

a. 需要先配置国密签名证书/私钥，再配置国密加密证书/私钥

b. 证书及其私钥需要连续配置

c. 国密算法支持 ECC-SM4-CBC-SM3 、 ECDHE-SM4-CBC-SM3 、ECC-SM4-GCM-SM3、ECDHE-SM4-GCM-SM3

d. 国密协议内置，无需配置

e. 纯国密也需配置上标准算法（兼容性原因）

f. 国密证书链配置到国密签名证书里面

（6）配置后，启动 nginx，浏览器中访问查验效果。

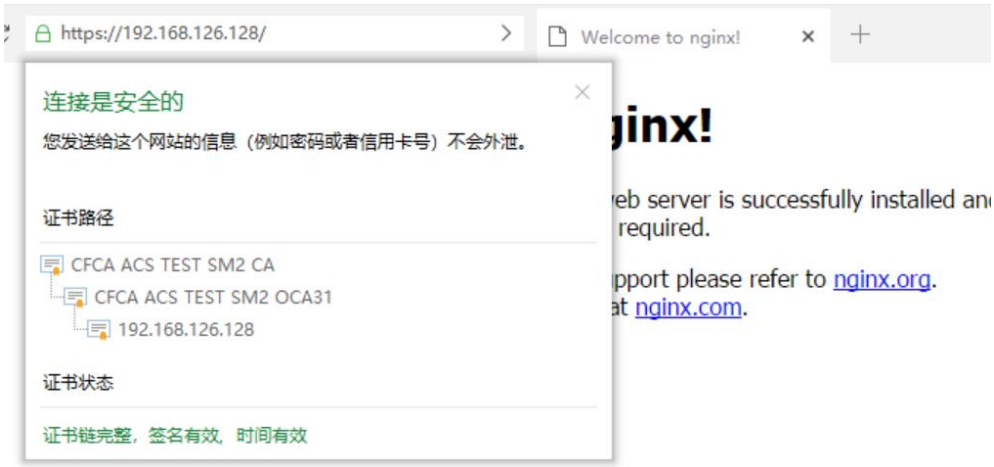


图 22 浏览器访问验证

2.2、cfca 国密 nginx 部署

目前我司也有一款 nginx 国密中间件，但有时效限制，截止到 2024 年 1 月 1 日前可正常使用，到此日期后，停服或更改配置后均无法正常启动，届时如有需要，需联系我司技术获取新版本。以下为使用此版本在 Linux 下部署使用的大致流程。

（1）本次运行系统环境

操作系统 CentOS7 x64（7.0-7.9），只支持 64 位，系统内核 kernel-3.10.0，相关依赖 gcc4.8.2-4.8.5、glibc2.17。

安装前请务必注意系统环境。非以上环境即便能安装也不能保证稳定使用。

（2）安装 nginx

将 ngx-sm-x.x.x-x.x86_64.rpm 上传到目标服务器（x.x.x-x 为对应软件版本）

rootrpm -ivh ngx-sm-x.x.x-x.x86_64.rpm；观察安装过程中是否有报错，

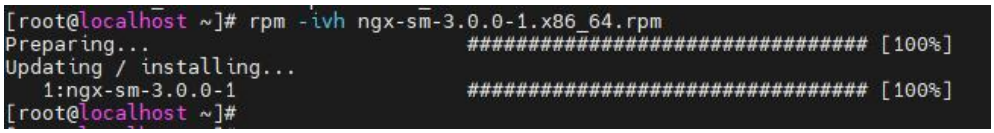


图 23 nginx 安装

（3）安装目录

软件安装目录为/usr/local/nginx/

其中 sbin 为可执行程序目录，conf 为配置文件目录，html 为静态页面目录，log 为日志目录，其它为临时目录。

```
[root@localhost nginx]# ll
total 0
drwx------. 2 root root   6 Jan 18 03:48 client_body_temp
drwxr-xr-x. 2 root root 112 Jan 18 04:51 conf
drwx------. 2 root root   6 Jan 18 03:48 fastcgi_temp
drwxr-xr-x. 2 root root  24 Jan 18 03:48 html
drwxr-xr-x. 2 root root  58 Jan 18 03:48 logs
drwx------. 2 root root   6 Jan 18 03:48 proxy_temp
drwxr-xr-x. 2 root root  19 Jan 18 03:48 sbin
drwx------. 2 root root   6 Jan 18 03:48 scgi_temp
drwx------. 2 root root   6 Jan 18 03:48 uwsgi_temp
[root@localhost nginx]#
```

图 24 nginx 目录结构

注意，如果目标机器已经安装官方 nginx 软件，安装前需注意目录是否冲突，防止文件被覆盖。

（4）证书部署

可直接用 key+cer 文件部署，可用上述第 2.2 软证书下载章节中最终获取的签名证书、签名私钥、加密证书、解密后的加密私钥。

对于证书链的添加，一般只用国密签名证书里面添加证书链就行，可用记事本打开签名证书 cer 文件和中级证书、根证书文件。将中级证书和根证书编码按下图顺序复制进签名 crt 文件后保存（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）。相关证书链文件可自行登录 cfca 官网下载专区中下载，http://www.cfca.com.cn/zhengshuzizhu/，或找我司技术单独提供。

```
-----BEGIN CERTIFICATE-----
服务器证书编码
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
中级证书编码
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
根证书编码
-----END CERTIFICATE-----
```

图 25 证书链结构示例

注意如需用 360 国密浏览器访问，则签名、加密公钥中都需要加入证书链。

进入到国密 nginx 目录，/usr/local/nginx/conf/nginx.conf，打开 nginx.Conf 文件，配置国密 ssl。

配置示例：

```
#https server
user root;
error_log logs/error.log info;
events {
worker_connections 1024;
}
http {
upstream app_server {
server 127.0.0.1:80; 应用服务器地址和端口
}
server {
listen 443 ssl;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2 GMVPNv1.1; 协议版本
ssl_session_cache  shared:SSL:1m;
ssl_certificate sign.crt;签名证书，PEM X509 格式
ssl_certificate_key sign.key;签名私钥，PEM P1 格式
ssl_enc_certificate enc.crt;加密证书，PEM X509 格式
ssl_enc_certificate_key enc.key;加密私钥，PEM P1 格式
ssl_verify_client on; 双向认证
ssl_verify_depth  10;验证深度，需比设置的信任证书链个数多
ssl_client_certificate client_chain.cer; 设置的证书信任链，PEM X509 格式，多个需拼接在一个文件中
location / {
root html;
index index.html index.htm;
```

```
proxy_pass http://app_server;
    }
  }
}
```

实际配置案例：

```
#https server

user  root;
error_log  logs/error.log  info;

events {
    worker_connections  1024;
}

http {

    server {
        listen  443 ssl;

        ssl_protocols            TLSv1 TLSv1.1 TLSv1.2 GMVPNv1.1;
        ssl_session_cache        shared:SSL:1m;

        ssl_certificate          /usr/local/nginx/conf/qm.cer;
        ssl_certificate_key      /usr/local/nginx/conf/qm.key;
        ssl_enc_certificate      /usr/local/nginx/conf/jm.cer;
        ssl_enc_certificate_key  /usr/local/nginx/conf/jm.key;

        #ssl_verify_client        on;
        #ssl_verify_depth         10;
        #ssl_client_certificate   client_chain.cer;

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

            proxy_pass http://127.0.0.1:80;
        }
    }
```

图 26 nginx 配置示例

（5）启动服务

执行/usr/local/nginx/sbin/nginx -c /usr/local/nginx/conf/nginx.conf

观察是否成功，可以使用 ps -ef | grep nginx ； 命令查看进程状态

```
[root@localhost ~]# ps -ef | grep nginx:
root       1371      1  0 03:48 ?        00:00:00 nginx: master process /usr/local/nginx/sbin/nginx -c /usr/local/nginx/conf/nginx.conf
root       1372   1371  0 03:48 ?        00:00:00 nginx: worker process
root       1385   1339  0 03:49 pts/0    00:00:00 grep --color=auto nginx:
[root@localhost ~]#
```

图 27 启动 nginx 服务

（6）浏览器中访问，查验效果。

图 28 网页访问验证

注意：配置国密服务器证书的 网站需使用支持国密的浏览器打开，使用普通浏览器或者支持国密的浏览器没有开通支持国密的服务是无法正常访问网站的。

四：常见问题

1、国密 ssl 证书是否支持申请多域名、单域名、通配符证书

国密 ssl 证书（无 ev/ov 叫法，与 ev/ov 为两套系统），但可以发放多域名、单域名、通配符类型证书、支持公网/内网 IP 发放。

2、开源中间件支持情况

国密 ssl 证书一般用于国产硬件设备，如 cfca 网关、信安世纪、深信服等厂商网络产品，开源中间件需要经过国密编译后才能使用，目前主流的部分国密开源中间件有 gmssl 的国密 nginx、tomcat，江南天安的国密 nginx。这些版本有些需要收费，具体请自行联系相关厂商获取。目前我司也有国密 nginx 中间件，有需要也可以使用。

3、国密 SSL 证书支持操作系统及浏览器版本

目前与操作系统厂商--麒麟软件、统信软件；

浏览器厂商--360 浏览器、奇安信浏览器、赢达信浏览器的互认互信。

证书类型	单域名	多域名	通配符
应用环境	Windows XP SP3及以上版本，需要支持国产密码算法的浏览器		
Mac OS	×		
Android	√（国密SADK）		
IOS	√（国密SADK）		
JDK	×		
算法	SM2		
公钥长度	256		
支持SAN（UC）	×	√	√
国际化域名	√		
发证速度	1-3个工作日		
有效期内免费证书重发/换发	√		

图 29 国密 ssl 证书支持情况

4、正常配置后，其他浏览器打开没问题，360 国密浏览器提示不受信任问题

用 360 国密浏览器访问，需部署过程中，签名、加密公钥中都加入证书链。

5、客户配置或导入证书的时候提示 key 与公钥文件不匹配。

可通过 CFCA SLL 证书管理系统去做国密证书公私钥匹配，或者去 myssl 网站（https://myssl.com/match_key.html）上去做国密证书公私钥是匹配问题。如不匹配可能是客户多次产生过 p10，保存错 key 文件了，如找不到对应 key 文件，可重新补发证书重新下载。

6、客户通过 myssl 网站产生国密双证 p10，最终使用证书时提示加密 key

私钥与加密公钥不匹配

目前通过 myssl 网站(https://myssl.com/csr_create.html)上点国密 cfca 会生成两个 key 文件，签名 key 和加密 key，正常加密 key 文件需要使用 cfca 官网上下载证书时返回的，客户用 myssl 网站上生成的加密 key 与 cfca 官网上下载的加密公钥文件去使用就会提示不匹配。所以客户如果需要中间件部署，建议用我们提过的工具去下载证书，参考 2.2 软证书下载章节。

7、用户中间件如 tomcat 部署好后访问，网站提示此网站无法提供安全连接，发送的响应无效。

此种情况大多是客户本地网络跳转、域名解析问题，常见于服务器证书部署好后，通过域名去访问网站报错，此种情况可让客户先检查中间件是否正常启动，如正常启动可让客户把网址中的域名换成用证书部署所在的业务服务器的 IP，可内网 IP 本地访问，如能正常访问，网站上能正常查看到证书，则在证书部署这块没有问题，建议客户排查本地网络策略。

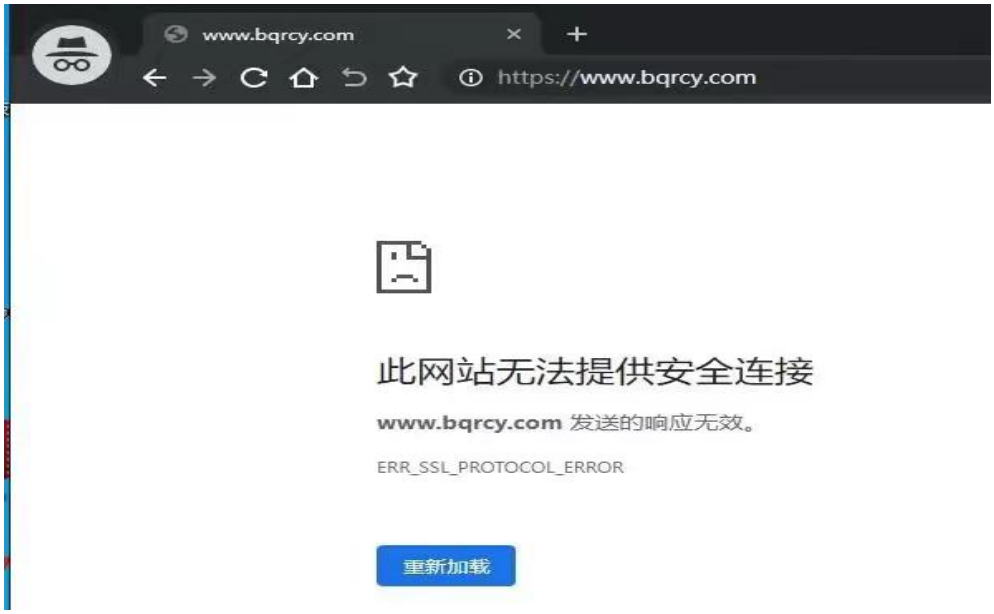


图 30 报错示例

7x24 客服热线

400-880-9888

CFCA 官方微信

地址：北京市西城区菜市口南大街平原里 20-3

前台电话：83526655　投诉电话：80864105

公司官网：http://www.cfca.com.cn　中国电子银行网：http://www.cebnet.com.cn