服务器 SSL 证书安装配置指南

Apache 2.x

更新日期：2015-11-2

GlobalSign China Co., Ltd.

第一步：生成证书请求文件(CSR)

进入 OpenSSL 安装的目录，运行如下命令生成私钥：

```
openssl genrsa -des3 -out server.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase:
Verifying - Enter pass phrase:
```

如果使用-des3 参数，将会需要输入一个密码对私钥进行加密，如不需要对私钥加密请不要使用-des3 选项。

输入两次密码后，将会生成 server.key 私钥文件

运行如下命令生成证书请求文件（CSR）

```
openssl req -new -key server.key –out server.csr
```

如是 Windows 系统，请使用下面命令生成证书请求文件（CSR）

```
set OPENSSL_CONF=openssl.cnf
openssl req -new -key server.key -out server.csr
```

接下来提提示输入私钥密码和申请证书的详细信息

```
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:CN
State or Province Name (full name) []:Shanghai
Locality Name (eg, city) []:Shanghai
Organization Name (eg, company) []:GlobalSign China Co., Ltd.

Organizational Unit Name (eg, section) []:IT Dept.
Common Name (eg, your websites domain name) []:cn.globalsign.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

从 Email 地址开始，下面的信息都不需要，请保留为空，直接回车即可。

需要输入的信息说明请见下表：

字段	说明	示例
Country Name	ISO 国家代码（两位字符）	CN
State or Province Name	所在省份	Shanghai
Locality Name	所在城市	Shanghai
Organization Name	公司名称	GlobalSign China Co., Ltd.
Organizational Unit Name	部门名称	IT Dept.
Common Name	申请证书的域名	Cn.globalsign.com
Email Address	不需要输入	
A challenge password	不需要输入	

完成以上的操作后会在对应的目录下生成 server.key 和 server.csr，请妥善保存这两个文件。

第二步：提交 CSR，申请证书

递交证书申请表及相关资料，并把证书请求文件（CSR）提交给我们。
我们确认资料齐全后，三个工作日内完成证书颁发。

第三步：获取服务器证书

1. 获取 SSL 证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第一段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为 server.cer（文本格式）。

2. 获取中级证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第二段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为 intermediate.cer（文本格式）。

请把 intermediate.cer、server.cer 和 server.key 这三个文件保存到同一个目录下，例如放到 /etc/ssl/crt/目录下。

第四步：更新 httpd.conf 配置文件

用文本编辑器打开 httpd.conf 并更新以下内容

```
<VirtualHost xxx.xxx.xxx.xxx:443>
DocumentRoot "/var/www/html"
ServerName cn.globalsign.com

SSLEngine on
SSLCertificateFile /etc/ssl/crt/server.cer              //公钥文件（GlobalSign颁发）
SSLCertificateKeyFile /etc/ssl/crt/server.key       //私钥文件
SSLCertificateChainFile /etc/ssl/crt/intermediate.cer     //中级证书
</VirtualHost>
```

按照以上的步骤配置完成后，重新启动 Apache（如果有设置 server.key 私钥密码，这时会提示输入） 后就可以使用 https://www.domain.com 来访问了。

如有任何问题或疑问请直接与我们联系，谢谢！