

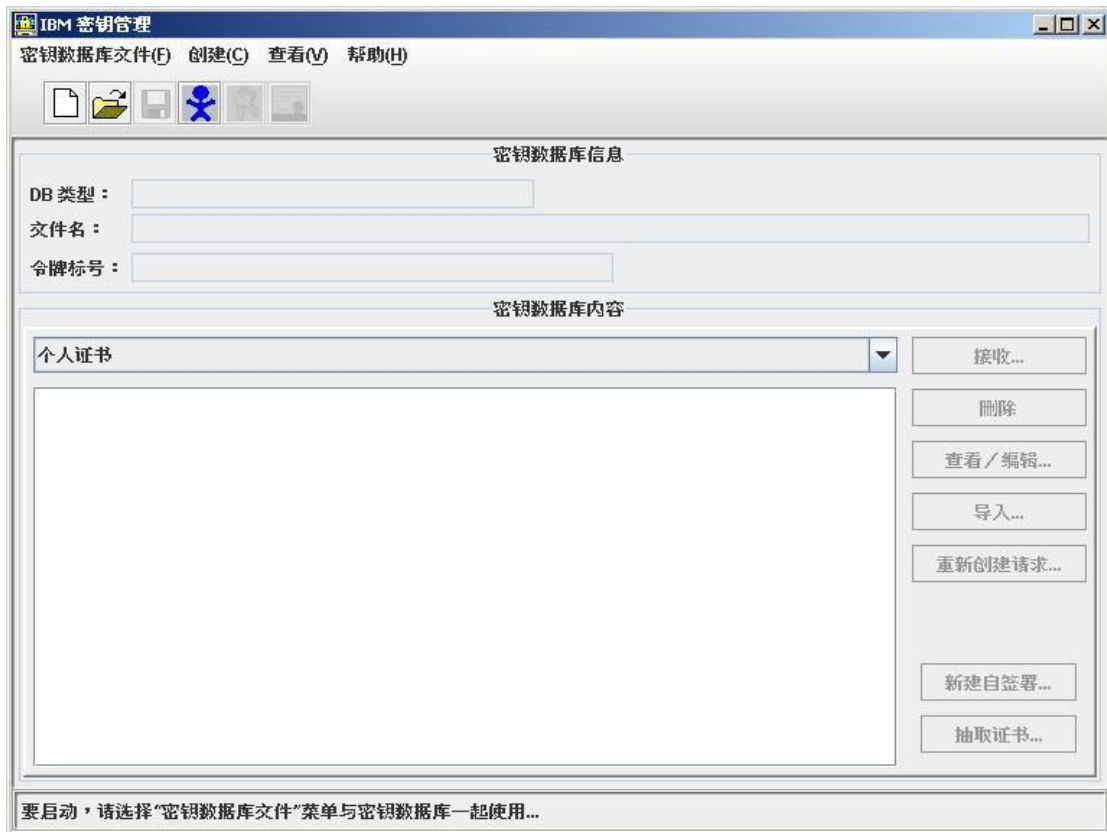
# **服务器 SSL 证书安装配置指南**

## **IBM HTTP SERVER 6.0**

更新日期：2016-11-7

## 第一步：生成证书签名请求文件(CSR)

运行 IKEYMAN（在 IBM HTTP Server 的 BIN 目录下）



创建 CMS 文件[kdb 文件]





点击创建，新建证书请求



填写正确的信息



**创建新密钥和证书请求**

请提供以下信息：

密钥标签(K)		cn.globalsign.com
密钥大小(E)		2048
签名算法(S)		SHA1WithRSA
共用名(M) (可选)		cn.globalsign.com
组织(G) (可选)		GlobalSign China Co.,Ltd.
组织单元(A) (可选)		Sales
市/县/区(L) (可选)		Shanghai
省/直辖市(T) (可选)		Shanghai
邮政编码(Z) (可选)		200060
国家或地区(U) (可选)		CN

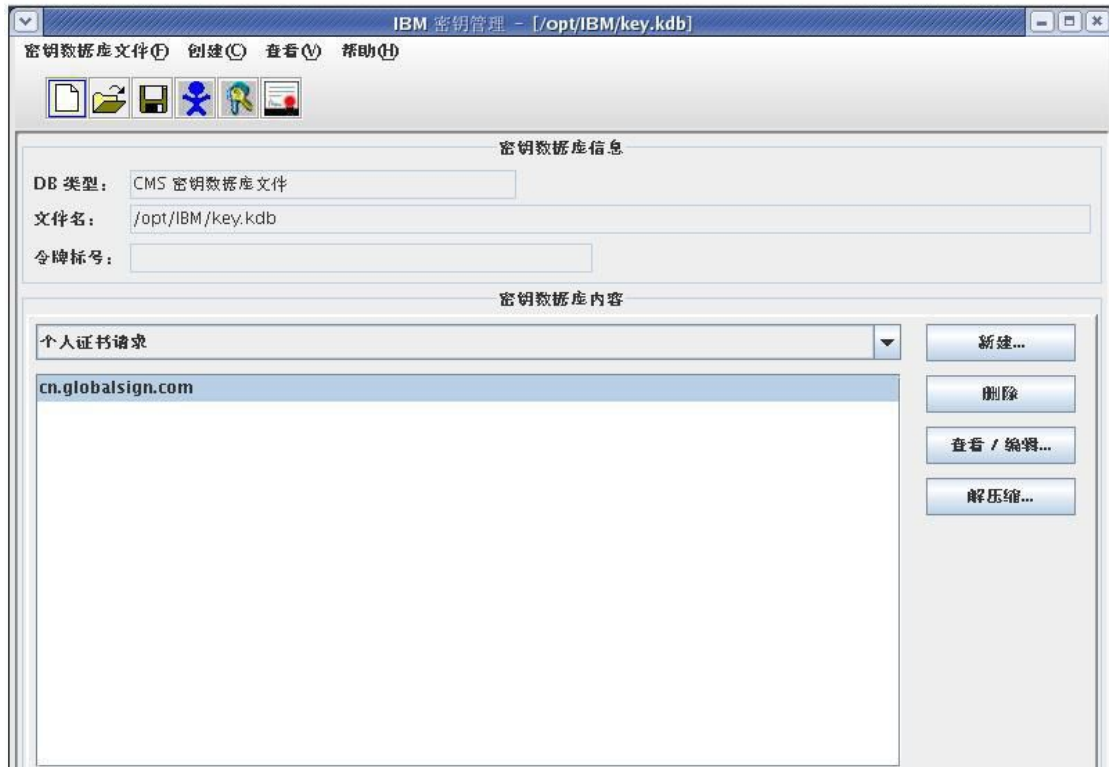
输入存储证书请求的文件的名称(H)：

/opt/IBM/certreq.arm 浏览(B)...

确定(O) 重新设置(R) 取消(C)



点击确定



以上的步骤完成后，CSR 文件就已经被生成了。

## 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。CSR 位于 /opt/IBM/certreq.arm，请将此文件发送给我们。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

获取服务器证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户），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）。并获取 GlobalSign 根证书和对应的中级证书

### 第四步：安装服务器证书

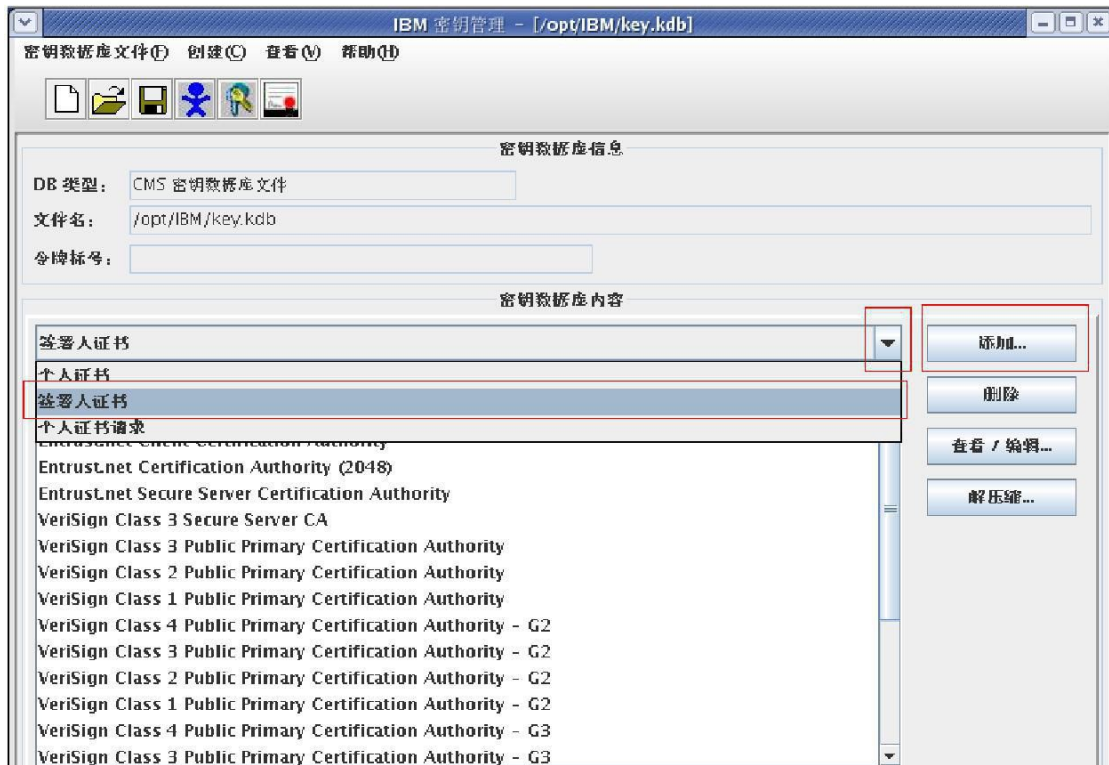
点击签署人证书，添加根证书及中级证书

获取 GlobalSign 根证书，将此段代码保存成 GlobalSign Root CA.cer:

```
-----BEGIN CERTIFICATE-----
```

```
MIIDdTCCAI2gAwIBAgILBAAAAAABFUtaW5QwDQYJKoZIhvcNAQEFBQAwwVzELMAkG
A1UEBhMCQkUxGTAxBGNVBAoTEEdsb2JhbFNpZ224gbnYtc2ExEDAQBgNVBAwTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ224gUm9vdCBDQTAeFw05ODA5MDEwMjAw
MDBaFw0yODAwMjAwMjAwMDBaMFcxZzAJBgNVBAYTAKJFMRkwFwYDVoQKExBHbG9i
YXxTaWduIG52LXNhMRAwDgYDVoQKLEwdSb290IENBMRSwGQYDVQQDExJHbG9iYWxT
aWduIFJvb3QgQ0EwggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ
jc6j40+Kfvvxi4Mla+piH/EqsLmVEQS98GPR4mdmzxzdxtIK+6NiY6arymAZavp
xy0Sy6scTHAHOt0KMM0VjU/43dSMUBUc71DuxC73/OIS8pF94G3VNTCOXkNz8kHp
1Wrjsok6Vjk4bwY8iGlbKk3Fp1S4blnMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJ
U26Qzns3dLlwR5EiUWMWWea6xrEmCMgZK9FGqkjWZCrXgzT/LCrBbBIDSgeF59N8
9iFo7+ryUp9/k5DPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SszANBgkqhkiG9w0B
AQUFAAOCAQEA1nPnfE920I2/7LqivjTFKDK1fPxsncwrVqmeU79rXqoRSLbICKOz
yj1hTdNGCbM+w6DjY1Ub8rrvrTnhQ7k4o+YviiY776BQVvnGCv04zcQLcFGUI5gE
38NfINUVyRRBnMRddWQVdf9VMOyGj/8N7yy5Y0b2qvzfvGn9LhJIZJrgIfcm7ymp
AbEVtQwdpf5pLGkkeB6zpxxxYu7KyJesF12KwvHhHm4qxFYldBniYUr+WymXUad
DKqC5JIR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/QR6cf9tveCX4XSQRjbgbME
HMUfpIbvFSDJ3gyICh3WZIXi/EjKSZp4A==
```

```
-----END CERTIFICATE-----
```



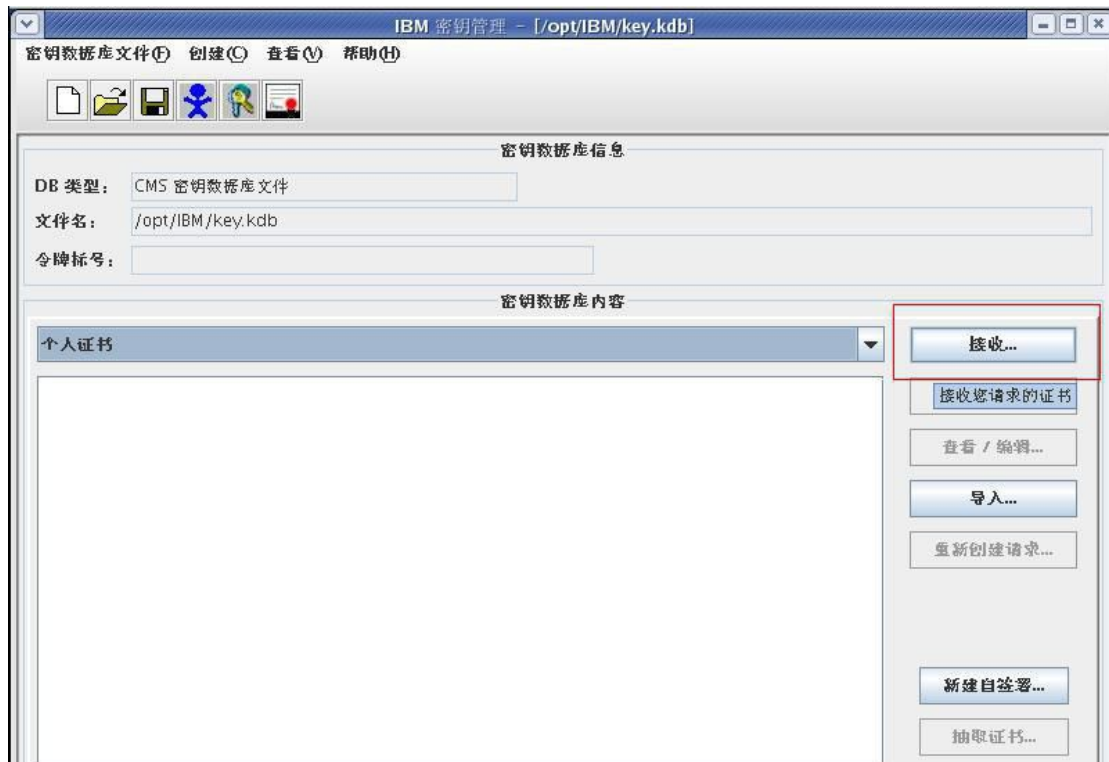
### 添加中级证书

获取中级证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把这内容保存为 intermediate.cer（文本格式）



### 最后点击个人证书接收添加颁发的服务器证书

获取服务器证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户），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）







### 第五步：配置 SSL 到 conf 文件

1、将扩展名为 kdb, rdb, sth 的 key 文件复制到 conf 目录, 编辑 httpd.conf 文件在 IBM HTTP Server httpd.conf 配置文件中启用 SSL 伪指令。

a. 取消注释 `LoadModule ibm_ssl_module modules/mod_ibm_ssl.so` 配置伪指令。

b. 使用以下示例和伪指令在 httpd.conf 文件中创建一个 SSL 虚拟主机节。

c. `LoadModule ibm_ssl_module modules/mod_ibm_ssl.so`

d. `<IfModule mod_ibm_ssl.c>`

e. `Listen 443`

f. `<VirtualHost *:443>`

g. `SSLEnable`

h. `</VirtualHost> </IfModule>SSLDisable`  
`KeyFile "/opt/IBM/key.kdb"`

启动 IHS

按照以上的步骤配置完成后就可以使用 `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！

