目录

40-位 SSL 安全服务器证书 与 128-位 SSL 全球服务器证书有什么不同？

VTN40服务器证书与VTN128服务器证书主要差别在于各自所能激活的SSL的加密强度不同，即在每次进行加密过程中所产生的“会话密钥”长度不同。VTN128服务器证书可以实现高度安全的强制128位加密，而不管用户端的浏览器是40位的还是56位的。而VTN40证书，由于不支持SGC强制128位加密技术，因此根据浏览器支持的位数不同，建立40位到128位的加密强度。两者还有一个主要的差异点在于支持的服务器平台数目不同。

为什么申请DV证书失败了？

域名中含有以下字段时，无法申请Symantec品牌的DV证书：

live（不含 .live 顶级域名）、bank、banc、ban.c、alpha、test、example、credit、内/外网IP地址、主机名、pw（含.pw顶级域名）、apple、ebay、trust、root、amazon、android、visa、google、discover、financial、wordpress、discover、pal

DNS和文件验证有什么不同？

若用户选择DNS验证，系统会为用户生成一条CNAME记录，用户只需在自己的域名服务商处增加此条CNAME的解析记录，即可完成域名验证。

若用户选择文件验证，系统会为用户生成一个带有随机字符串的htm页面，用户需将此页面放在域名指向服务器中的指定位置，并确认可通过公网访问。

使用CDN会对DV证书的属主验证有影响吗？

如果有CDN，DV证书的属主验证可能受影响。 文件验证的方式，需要确保海外美国的CDN节点可用，Symantec的文件验证服务器在美国。 DNS验证的方式，使用CDN服务时，多数会将域名CNAME到CDN服务商，导致DNS验证方式的TXT记录与CANME记录冲突，DNS的TXT验证方式不可用。Symantec厂商正在对该问题进行策略优化。

如果改变了硬件、软件（web server）或者IP地址，证书需要重新申请吗？

服务器证书与硬件无关。系统和web server版本如果相同也不会有任何影响。如果改变了服务器软件，证书就要重新申请。服务器证书不可以更换平台使用。改变IP地址，对服务器证书也没有影响。

通过IP访问站点时，显示不是私密连接

用户请通过域名访问站点。通过IP的方式访问，与证书绑定的通过域名访问的方式不匹配。如果暂时还没做域名解析，用户可以先通过修改hosts文件，手动添加域名与IP的解析记录来测试本地域名访问。

通过Https访问站点时，显示证书已过期或未生效

出现该提示可能有三种情况：1、系统时间不对 2、站点的服务器证书过期 3、中间级证书过期。

首先检查客户端系统时间设置，确定客户端系统时间设置无误。

然后忽略站点证书错误提示信息，成功网文站点后查看站点服务器证书，确保网站服务器上查看到的证书有效期没有问题。

如果仍然提示证书过期，在服务器证书查看页面切换到“证书路径”选项卡，确认证书路径选项卡中的所有上级证书均未提示错误信息。

不安全方式使用ActiveX控件

"internet explorer 已经阻止此站点用不安全方式ActiveX控件.因此,此页可能显示不正确"，这主要是由于控件编程的问题，在activex控件中缺少实现ISafeobject接口。因为该ActiveX控件没有标记为脚本安全，在IE默认安全级别设置中对没有标记为安全的ActiveX控件进行初始化和脚本运行的选项为禁用，所以运行时报安全提示。如果要消除这个提示，必须在控件上加上一个脚本安全标志。

安装SSL证书后，解决混合内容造成页面错误提示的处理办法

出现“安全证书上的名称无效，或者与站点名称不匹配”的错误提示，是因为使用IP地址访问该站点。因为证书是与域名绑定的，在访问站点时，需要验证当前站点域名是否和证书上声明的域名一致。如要解决该问题，请使用域名访问该站点。

“本页不但包含安全的内容，也包含不安全的内容”该错误是由于网站页面出现混合内容引起的。要解决该问题，需要在网站页面上做一些调整。如站点上有 Flash 的资源，请将 Adobe Flashplyer 的控件安装包下载下来放到服务器上，并修改控件安装包的地址，指向服务器上的资源。网站页面尽量使用相对路径。使用相对路径的情况下，能够保证无论是使用http还是https都能够正常访问。如果需要使用绝对路径，并且该页面需要使用https来访问，请使用 https 的完整路径来指定资源的URL。

“本页不但包含安全的内容，也包含不安全的内容” 是因为网站页面包含 http 的资源引起的。

例如:

1.有外链资源的情况

在网站页面文件中，包含了其他网站非https的资源。如: http://***/img/baidu_logo.gif

2.无外链，但使用了完整路径

在网站页面文件中，使用了完整的 URL : http://***/image/image1024.gif

如果是第一种情况，请下载其他网站资源到服务器上，并修改资源路径，指向到服务器上。或者取得外部站点 https 的 URL : https://***/img/baidu_logo.gif

如果是第二种情况，请使用相对路径如 < img src="image/image1024.gif"> 或者完整的 https 路径< img src=https://***/image/image1024.gif>

弹出这个提示是因为网站页面上包含混合内容导致的。

也就是说，网站页面上包含 http:// 的资源 也包含 https:// 的资源。

通常这种情况是需要在网站页面上做一些调整才能去除提示。以下是常用的解决方法:

网站页面上引用 图片，js 脚本等资源时，尽量使用相对路径（http://.../demo/image.jpg 为完整路径 demo/image.jpg 为相对路径）

网站页面引用 flash 资源时，需要将 adobe 的控件下载到服务器上，并修改控件路径。或直接删除控件安装的代码。

网站引用站点外部资源时，如果外网资源为 http 连接，请将外部资源下载到服务器上，修改资源路径，指向内部服务器。如果外网资源为 https 资源，引用时可以不受影响，直接引用。

chrome 53-54版本报错说明

近期有部分用户反馈，在使用chrome浏览器访问配置了Symantec及GeoTrust证书的网站时会弹出警告。

安卓手机APP使用Webview方式调用Chrome53、54版本内核也会出现证书问题。目前Symantec已经联系国内手机厂商并推动其将webview更新到不受影响的浏览器版本。

通过联系Symantec和Google工程师了解到,chrome 53/54版本存在BUG，未将所有Symantec在2016年6月1号以后签发的证书添加到证书透明度名单中，而其实这些证书是已经公开了证书透明度审核记录的。

下面是Symantec官方公告： https://www.symantec.com/connect/tr/blogs/chrome-53-bug-affecting-symantec-ssltls-certificates

https://knowledge.symantec.com/support/ssl-certificates-support/index?page=content&id=ALERT2160&actp=LIST&viewlocale=en_US

https://knowledge.symantec.com/support/ssl-certificates-support/index?page=content&id=ALERT2160

对于此问题，Google已经发布官方声明承认chrome存在的BUG，并在55/56版本彻底修复了此问题。Google已经发布后台修复补丁，帮助国外用户解决此问题。国内用户自带浏览器由于政策原因无法获取补丁修复，建议更换浏览器访问。

CSR文件生成方法

在申请证书前，用户需要提交CSR文件，以完成身份校验并生成证书公钥文件。**生成CSR文件时会同时生成私钥文件，请妥善保管和备份。**

OpenSSL生成CSR

1.输入指令 `openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout myprivate.key -out mydomain.csr`

```
[root@                    ]# openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout private.key -out domain.csr
Generating a 2048 bit RSA private key
..............+++
.....................................................................+++
writing new private key to 'private.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) [XX]:CN
State or Province Name (full name) []:北京
Locality Name (eg, city) [Default City]:北京
Organization Name (eg, company) [Default Company Ltd]:北京金山云网络技术有限公司
Organizational Unit Name (eg, section) []:产品部
Common Name (eg, your name or your server's hostname) []:www.ksyun.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@                    ]#
```

2.按提示输入以下信息，**注意：此处填写的信息要和补全证书信息时填写的内容一致**

字段	解释	示例	约束
Country Name	ISO国家代码	CN	英文大写，两位字符
State or Province Name	所在省份	北京	中英文均可
Locality Name	所在城市	北京	中英文均可
Organization Name	公司名称	北京金山云网络技术有限公司	中英文均可
Organizational Unit Name	部门名称	产品部	中英文均可
Common Name	申请证书的域名	www.ksyun.com	
Email Address	无需输入		
A challenge password	无需输入		
An optional company name	无需输入		

3.完成后，会在当前目录下生成 private.key（私钥文件）和 domain.csr（证书请求文件）。

keytool生成CSR

1.输入指令 keytool -genkey -alias cert -keyalg RSA -keysize 2048 -keystore ./domain.jks

```
[root@[redacted]]# keytool -genkey -alias cert -keyalg RSA -keysize 2048 -keystore ./domain.jks
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  www.ksyun.com
What is the name of your organizational unit?
  [Unknown]:  产品部
What is the name of your organization?
  [Unknown]:  北京金山云网络技术有限公司
What is the name of your City or Locality?
  [Unknown]:  北京
What is the name of your State or Province?
  [Unknown]:  北京
What is the two-letter country code for this unit?
  [Unknown]:  CN
Is CN=www.ksyun.com, OU=产品部, O=北京金山云网络技术有限公司, L=北京, ST=北京, C=CN correct?
  [no]:  Y

Enter key password for <cert>
        (RETURN if same as keystore password):
[root@[redacted]]#
```

2.输入证书保护密码，并按提示输入以下信息，**注意：此处填写的信息要和补全证书信息时填写的内容一致**

问题	解释	示例	约束
What is your first and last name?	申请证书的域名	www.ksyun.com	
What is the name of your organizational unit?	部门名称	产品部	中英文均可
What is the name of your organization?	公司名称	北京金山云网络技术有限公司	中英文均可
What is the name of your City or Locality?	所在城市	北京	中英文均可
What is the name of your State or Province?	所在省份	北京	中英文均可
What is the two-letter country code for this unit?	ISO国家代码	CN	英文大写，两位字符

4.完成后确认信息无误，[no]:Y 输入

5.输入密钥密码

6.通过证书文件生成证书请求

keytool -certreq -sigalg SHA256withRSA -alias mycert -keystore ./mydomain.jks -file ./mydomain.csr

```
[root@[redacted]]# keytool -certreq -sigalg SHA256withRSA -alias cert -keystore ./domain.jks -file ./domain.csr
Enter keystore password:
[root@[redacted]]#
```

完成

SSL中常见密钥格式与证书格式

密钥库文件格式（Keystore）

格式：JKS 拓展名：.jks/.ks

JKS (Java KeyStore): 密钥库的Java实现版本，provider为SUN，java的密钥存储文件,二进制格式,是一种 Java 特定的密钥文件格式， JKS的密钥库和私钥用不同的密码进行保护。

格式：JCEKS 拓展名：.jce

JCEKS （JCE Keystore）：密钥库的JCE实现版本，provider为SUN JCE，java的密钥存储文件，在JCEKS中存储和装载不同条目的过程类似于JKS，相对于JKS安全级别更高，JDK1.4版本后可直接使用，保护Keystore私钥时采用TripleDES。

格式：PKCS12 拓展名：.p12/.pfx

PKCS12：是公钥加密标准，它规定了可包含所有私钥、公钥和证书。其以二进制格式存储，也称为 PFX 文件，在windows中可以直接导入到密钥区，密钥库和私钥用相同密码进行保护

格式：BKS 拓展名：.bks

BKS（Bouncycastle Keystore）：密钥库的BC实现版本，provider为BC，保护Keystore私钥时采用TripleDES，它能够防止证书库被不小心修改（Keystore的keyentry改掉1个bit都会产生错误），BKS能够跟JKS互操作。

格式：BUER 拓展名：.ubr

BUDER（Bouncycastle UBER Keystore）：密钥库的BC更安全实现版本，provider为BC，当密码是通过命令行提供的时候，它只能跟keytool交互。整个keystore是通过PBE/SHA1/Twofish加密，因此 keystore能够防止被误改、察看以及校验。SunJDK允许你在不提供密码的情况下直接加载一个Keystore，类似cacerts，UBER不 允许这种情况。

证书文件格式（Certificate）

格式：DER 拓展名：.cer/.crt/.rsa

DER（ASN .1 DER）：用于存放证书，不含私钥，为二进制。

.DER =扩展名.DER用于二进制DER编码的证书。这些证书也可以用CER或者CRT作为扩展名。

.CRT = 扩展名CRT用于证书。证书可以是DER编码，也可以是PEM编码。扩展名CER和CRT几乎是同义词。这种情况在各种unix/linux系统中很常见。

.CER = CRT证书的微软型式。可以用微软的工具把CRT文件转换为CER文件（CRT和CER必须是相同编码的，DER或者PEM）。扩展名为CER的文件可以被IE识别并作为命令调用微软的cryptoAPI（具体点就是rudll32.exe cryptext.dll, CyrptExtOpenCER），进而弹出一个对话框来导入并/或查看证书内容。

格式：PKCS7 拓展名：.p7b/.p7r

PKCS#7,也叫做加密消息的语法标准，由RSA安全体系在公钥加密系统中交换数字证书产生的一种加密标准。 其中p7b以树状展示证书链，不含私钥；p7r为CA对证书请求签名的回复，只能用于导入

格式：CMS 拓展名：.p7c/.p7m/,p7s

CMS(Cryptographic Message Syntax):

p7c：只保存证书；

p7m：signature with enveloped data；

p7s：时间戳签名文件

格式：PEM 拓展名：.pem

PEM（Privacy nhanced Mail）：该编码格式在RFC1421中定义，但他也同样广泛运用于密钥管理，实质上是 Base64 编码的二进制内容。

格式：PKCS10 拓展名：.p10/.csr

CSR：证书签发请求(Certificate Signing Request)，或者叫做认证申请，是一个发送到CA的请求认证信息。有两种格式，应用最广泛的是由PKCS#10定义的，另一个用的少的是由SPKAC定义的，主要应用于网景浏览器。 P10：证书请求文件，类似于CSR文件。

格式:SPC 拓展名：.pvk/.spc

SPC(Software Publishing Certificate)：微软公司特有的双证书文件格式，经常用于代码签名，其中.pvk用于保存私钥、.spc用于保存公钥。