ssl - 如何使用 openssl 将自定义字段添加到证书

标签 ssl openssl x509

我正在尝试创建供内部使用的证书。我是 CA，我想在我的客户端证书中有一个附加字段，这样当我为客户端生成证书时，它将在该字段中保存一些特定数据。

我阅读了以下 article 和 another article 我知道我可以通过为每个字段生成一个 oid 来使用 x509 v3 格式来做到这一点，然后将它与 `-extfile` 一起使用创建公钥时的参数
所以我使用了默认的/etc/ssl/openssl.cnf 配置文件并取消注释提到的字段之一：

```
[ new_oids ]
testoid1 = 1.2.3.4
```

然后我通过以下方式生成所有证书：

```
openssl genrsa -aes256 -out ca-key.pem 4096
openssl req -new -x509 -days 365 -key ca-key.pem -sha256 -out ca.pem -config openssl.cnf
openssl genrsa -out key.pem 4096
openssl req -subj '/CN=client' -new -key key.pem -out client.csr
openssl x509 -req -days 365 -sha256 -in client.csr -CA ca.pem -CAkey ca-key.pem  -CAcreateserial -out cert.pem -extfile extfile.cnf
```

其中 extfile.cnf 内容是：

```
1.2.3.4 = Something
```

我得到：

```
Error Loading extension section default
140218200073872:error:22097082:X509 V3 routines:DO_EXT_NCONF:unknown extension name:v3_conf.c:125:
140218200073872:error:22098080:X509 V3 routines:X509V3_EXT_nconf:error in extension:v3_conf.c:95:name=1.2.3.4, value=Something
unable to write 'random state'
```

缺少本主题中的文档。有人可以引导我完成它并解释它是如何完成的吗？

最佳答案

为了添加自定义字段，首先创建一个配置文件：

```
[req]
req_extensions = v3_req

[v3_req]
1.2.3.4.5.6.7.8=ASN1:UTF8String:Something
```

然后，创建 CSR：

```
openssl req [params] -out mycsr.csr -config myconfig.cnf
```

然后，创建证书：

```
openssl x509 -req -sha256 -in mycsr.csr [params] -out mycert.pem -extfile myconfig.cnf -extensions v3_req
```

关于ssl - 如何使用 openssl 将自定义字段添加到证书，我们在Stack Overflow上找到一个类似的问题：
https://stackoverflow.com/questions/36007663/

上一篇：perl - OpenSSL DH key 太小错误
下一篇：macos - 在 Mac OS X 中将导入的证书设置为始终受信任

相关文章：

c# - 基于证书的文件共享身份验证
c - Windows 2008R2 CA & OpenSSL CSR : Error parsing CSR ASN1 bad value met
c - 使用 openssl 进行数据加密/解密
Ruby:用于 HTTPS 和 SSL 通信的 openssl 替代方案
javascript - 在 PHP openssl 中加密并在 javascript CryptoJS 中解密
Ruby 字符串拆分
java - Java:在Windows上进行测试的SSL证书？
ssl - 使用 SSL 的 CXF 客户端引发 SSLHandshakeException
laravel - SSL连接错误-对等体重置连接-在Homestead机器上
security - 如何使用 ssl/security 设置 Mercurial