链滴

openssl 生成 https 证书

作者：snake
原文链接：https://ld246.com/article/1679045037020
来源网站：链滴

PEM 证书是一种常见的数字证书格式，常用于 Web 服务器和其他网络应用程序中。它是基于 Base64 编码的 ASCII 文本格式，包含公钥、私钥、证书链等信息，并通常以 .pem 扩展名保存。

要在 Ubuntu 上创建 PEM 证书，您可以使用 OpenSSL 工具。以下是创建 PEM 证书的步骤：

1. 创建私钥

在终端中执行以下命令，以创建一个新的私钥文件：

```
sudo openssl genrsa -out mykey.pem 2048
```

上述命令将创建一个名为 mykey.pem 的私钥文件，并使用 2048 位密钥长度。

2. 生成证书请求

在终端中执行以下命令，以生成一个新的证书请求：

```
sudo openssl req -new -key mykey.pem -out myreq.pem
```

执行上述命令时，您将被要求提供一些证书请求的相关信息，例如组织名称、国家代码、城市名称等。

3. 签发证书

在您获得证书之前，您需要将证书请求发送给证书颁发机构（CA），以获取由 CA 签发的数字证书。果您只是需要使用自签名证书，则可以执行以下命令：

```
sudo openssl x509 -req -in myreq.pem -signkey mykey.pem -out mycert.pem
```

上述命令将使用您之前创建的私钥和证书请求生成一个新的自签名证书文件 mycert.pem。

4. 将证书与私钥合并

将证书和私钥合并到单个 PEM 文件中，以便将其用于 Web 服务器或其他应用程序。在终端中执行下命令：

```
sudo cat mycert.pem mykey.pem > mypem.pem
```

上述命令将证书文件 mycert.pem 和私钥文件 mykey.pem 合并到一个名为 mypem.pem 的 PEM 件中。

现在您已经成功创建了 PEM 格式的数字证书，并将其保存在名为 mypem.pem 的文件中，可以将其于您的 Web 服务器或其他应用程序中。请注意，自签名证书可能无法提供与受信任的证书相同的保水平，因此在某些情况下可能需要受信任的证书。