微信小程序里使用免费的 https 证书

在小程序的文档里我们看到这么一个重要接口说明。

`wx.request` 发起的是 https 请求。**一个微信小程序，同时只能有 5 个网络请求连接。**

而小程序需要同服务器交互的时候，必定要用到这个接口。

https ?

对于大部分同学来说，了解 https 的详细过程似乎没太大必要，我们直接先说第一个结论。

> https 证书一般是需要购买的，而且价格不低。

自己签发的证书是不被公众认可的，所以就要找大机构拿证书。这时候就要交证书的费用。

比如下图：

最近的某 Sign 公司的证书又出了信任危机，有没有更有性价比的方案呢？有！！同城圈联盟现在就教你免费获得靠谱的 https 证书！

我们先教大家如何获取和配置证书！下面一段适合程序员来看。非程序员需要配置的，可以联系离你最近的程序员（比如页面底部那个）请教他。

前提：Linux 服务器，Python2.7

首先从著名同性交友社区下载需要的脚本和配置模板

wget https://raw.githubusercontent.com/xdtianyu/scripts/master/lets-encrypt/letsencrypt.conf
wget https://raw.githubusercontent.com/xdtianyu/scripts/master/lets-encrypt/letsencrypt.sh
chmod +x letsencrypt.sh

然后可以看到 letsencrypt.conf 的内容是这样的

```
# only modify the values, key files will be generated automaticly.
ACCOUNT_KEY="letsencrypt-account.key"
DOMAIN_KEY="example.com.key"
DOMAIN_DIR="/var/www/example.com"
DOMAINS="DNS:example.com,DNS:www.example.com"
#ECC=TRUE
#LIGHTTPD=TRUE
```

DOMAIN_KEY 是保存的文件名，比如我们设成 sub.mydomain.cn.key

DOMAIN_DIR 是 WEB 的根目录，也就是/index.html, /index.php … 所在的那个目录。

DOMAINS 是这个 WEB 目录上绑定的域名。常见的就是根域或是 www 域，或是你需要的子域名。

比如我修改成这个样子

?ACCOUNT_KEY="letsencrypt-account.key"

DOMAIN_KEY= “sub.mydomain.com.key"
DOMAIN_DIR= “/var/www/path/to/mydomain/"

DOMAINS= “DNS:sub.mydomain.com"?

然后确认 sub.mydomain.com 是可以正常访问的。因为生成证书的时候会对域名可访问性做验证。

然后执行

./letsencrypt.sh letsencrypt.conf

如果正常的话，这时候会在当前目录下生成一堆文件。

其中会有一个 sub.chained.crt 和 sub.mydomain.com.key 。这两个文件一会儿我们会用到。

现在去 nginx 下添加一个 443 端口的虚拟主机。

```
server
  {
    listen 443;
    ssl on;
    ssl_certificate /root/letsencrypt/sub.chained.crt;
    ssl_certificate_key /root/letsencrypt/sub.mydomain.com.key;
    server_name   sub.mydomain.com;
    index index.php;
    root  /var/www/path/to/mydomain/;
    if (-f $request_filename/index.php){
            rewrite (.*) $1/index.php;
       }
       if (!-e $request_filename){
```

```
            rewrite (.*) /index.php;
        }

    location ~ .*\.(php|php5)?$
    {
      fastcgi_pass   127.0.0.1:9001;
      fastcgi_index index.php;
      include fastcgi.conf;
    }
  }
```

红字部分需要重点看！（敲黑板）

重启 Nginx ，访问 https://sub.mydomain.com 就发现有绿色的证书标志啦！

对的，这个过程中我们没花一分钱。

One More Thing

证书都会过期的嘛，但这个证书是可以免费续期的！

先在 letsencrypt.sh 的最后加一行 service nginx reload

表示执行成功之后重启一下 Nginx。

然后在 crontab 里加一行，表示每个月 1 号 0 点自动续期，这样就可以保证这个证书状态一直是正常的了。记得改！路！径！

```
0 0 1 * * /etc/nginx/certs/letsencrypt.sh /etc/nginx/certs/letsencrypt.conf >> /var/log/lets-encrypt.log 2>&1
```

如果你用的是 Apache，那把 Nginx 配置 https 的方法换成 Apache 对应的就可以了，证书获取方法是不一样的。

Two More Thing

这个证书实际是从 letsencrypt.org 项目获得的。

Let’s Encrypt CA 项目由 Mozilla、思科、Akamai、IdenTrust 和 EFF 等组织发起，向网站自动签发和管理免费证书，加速将 Web 从 HTTP 过渡到 HTTPS。ISRG 则是开发 Let’s Encrypt CA 的非营利组织。而目前，Let's Encrypt 项目和互联网安全研究组（ISRG）都有 Linux 基金会托管。

所以证书的干爹还是靠谱的。

写这个教程的同学也是靠谱的。

Three More Thing

可能有的同学会找到官方的一个脚本来安装证书，为什么本文不推荐？因为那个脚本需要暂停 Web 服务！这篇文章的方法就不需要长时间暂停 Web 服务了。

现在你可以创建一个 https 站点，然后通过小程序调用这个接口了。有点爽么？