AFNetworking对HTTPS的支持说明

2015年9月19日 星期六 23:33

使用AFNetworking来支持HTTPS(也可以验证自建证书还是不是)

AFNetworking是iOS/OSX开发最流行的第三方开源库之一，其作者是非常著名的iOS/O
其博客NSHipster也是iOS/OSX开发者学习和开阔技术视野的好地方。AFNetworking已经
好，甚至更完善，在AFSecurityPolicy文件中，有兴趣可以阅读这个模块的代码；

AFNetworking上配置对HTTPS的支持非常简单：

```
//-------------------------

NSURL * url = [NSURL URLWithString:@"https://www.google.com"];
AFHTTPRequestOperationManager * requestOperationManager = [[AFHTTPRequestOpera
seURL:url];
dispatch_queue_t requestQueue = dispatch_create_serial_queue_for_name("kRequestCo
requestOperationManager.completionQueue = requestQueue;
AFSecurityPolicy * securityPolicy = [AFSecurityPolicy policyWithPinningMode:AFSSLPinning

//allowInvalidCertificates 是否允许无效证书（也就是自建的证书），默认为NO
//如果是需要验证自建证书，需要设置为YES
securityPolicy.allowInvalidCertificates = YES;

//validatesDomainName 是否需要验证域名，默认为YES；
//假如证书的域名与你请求的域名不一致，需把该项设置为NO
//主要用于这种情况：客户端请求的是子域名，而证书上的是另外一个域名。因为SS
假如证书上注册的域名是www.google.com，那么mail.google.com是无法验证通过的；
的域名*.google.com，但这个还是比较贵的。
securityPolicy.validatesDomainName = NO;

//validatesCertificateChain 是否验证整个证书链，默认为YES
//设置为YES，会将服务器返回的Trust Object上的证书链与本地导入的证书进行对比，
书链是这样的：
//GeoTrust Global CA
//    Google Internet Authority G2
```

SX开发者Mattt Thompson，
经将上面的逻辑代码封装

tionManager alloc] initWithBa

mpletionQueue");

gModeCertificate];

L证书上的域名是独立的，
当然，有钱可以注册通配符

这就意味着，假如你的证

```
//      *.google.com
//那么，除了导入*.google.com之外，还需要导入证书链上所有的CA证书
（GeoTrust Global CA, Google Internet Authority G2）；
//如是自建证书的时候，可以设置为YES，增强安全性；假如是信任的CA所签发的证书
securityPolicy.validatesCertificateChain = NO;
requestOperationManager.securityPolicy = securityPolicy;

//-------------------------
```

这就是AFNetworking的支持HTTPS的主要配置说明，AFHTTPSessionManager与之基本一

书，则建议关闭该验证；

一致，就不重复了。