YubiKey配置SSH证书认证

Published on Apr 25, 2021 UTC by Wang Ye <https://wangye.org>

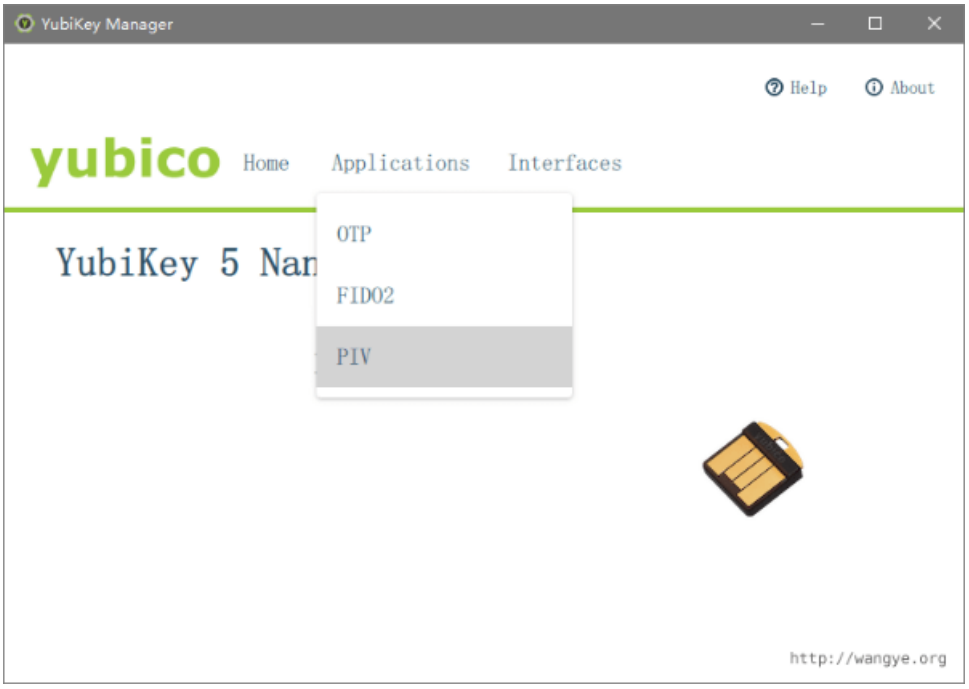
记得很久之前就尝试使用废弃的银行U盾存储加密用的数字证书，也考虑过购买空白USB Key或者智能卡，直到有一天看到了YubiKey这个小玩意儿，彻底被种了草，由于国内购买不便，淘宝上价格虚高也不放心，一直等到亚马逊支持了海外直邮，立马入手，如果说仅将YubiKey用来存储数字证书，那么没有完全发挥出其在个人信息安全保护上的威力。比如就现在的YubiKey而言，在我的个人信息安全保护体系中主要承担了重要信息资产两步认证、SSH证书登录、GnuPG签名与加密、常用密码数据库KeePass保护等等，预计今后将会通过YubiKey逐步替代掉所有不安全的认证方式。

今天主要介绍的是YubiKey配置SSH登录备忘，配置内容仅供参考，实际上SSH最早是在采用YubiKey 4的时候就已经配置了，当时仅有一把YubiKey，串在钥匙扣上，配置GnuPG的时候顺带支持了SSH登录，当然主要是依赖于GnuPG的实现，记不清在哪儿看过一篇报道，这种实现容易被在内存dump出私钥，实际上Windows系统自带有智能卡认证接口，相比较而言会更加安全，后期我也新购入几把YubiKey并重新配置了证书，为了利用Windows自带的认证接口，并且让XShell等客户端也能够支持SSH证书登录，这里使用了开源的WinCryptSSHAgent方案，需要下载最新版本备用。

1 YubiKey Manager配置证书

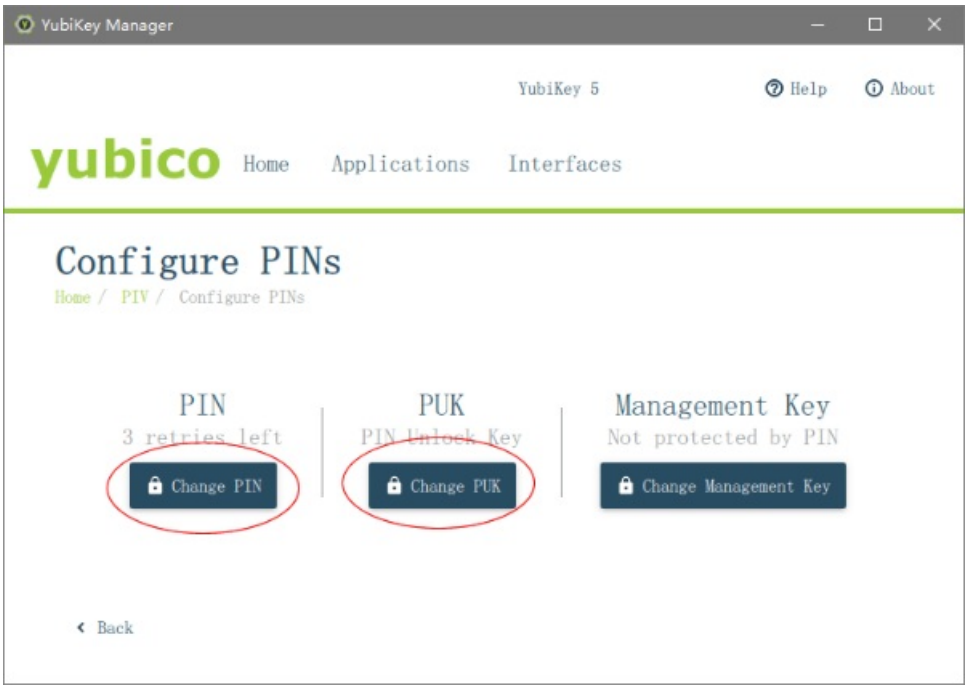
到Yubico官方网站上下载YubiKey Manager，这里强调一下涉及到信息安全的一定要在官方网站下载，下载完成后请验证数字签名，确保无误后安装。

插入你的YubiKey并运行YubiKey Manager，不出意外将会很快识别出YubiKey，需要注意的是这个软件一次性只能配置一个YubiKey，请确保计算机上有且只插入一个Key，依次点击Applications > PIV，如下图所示：



1.1 修改PIN和PUK

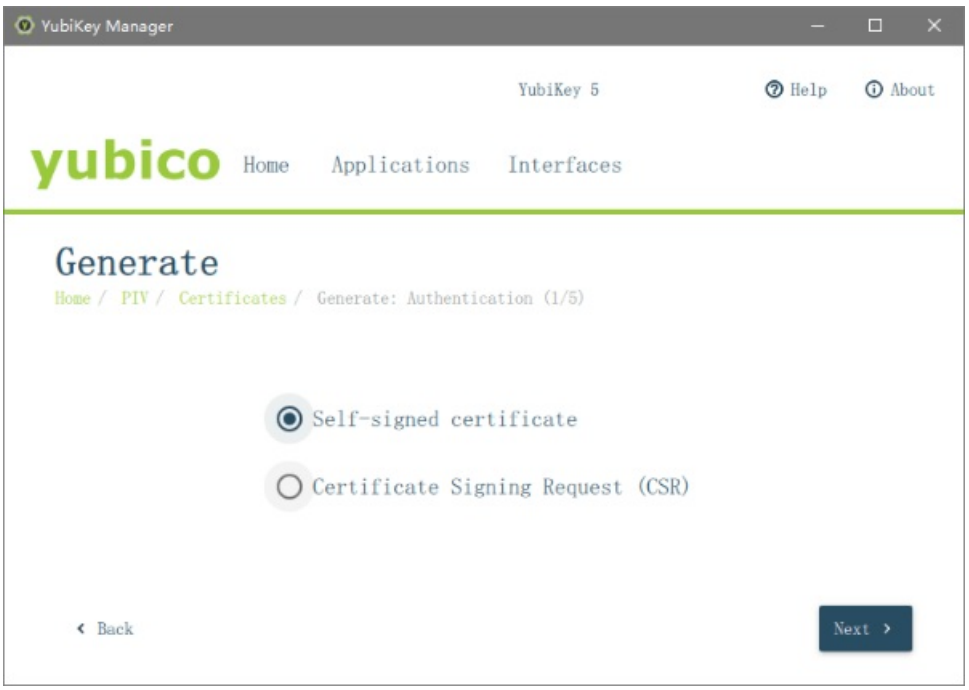
每个YubiKey出厂默认设置了PIN为123456，PUK为12345678，需要注意的是为了保障你的YubiKey不被未经授权的使用，建议修改，其中PUK是管理PIN，可以解锁被锁定的PIN码，请务必设置为和PIN码不一样并记录在安全位置，PIN码则是完成配置后每次登录SSH需要输入的认证码，一般设置为6位，这个PIN码仅允许尝试3次，3次失败后将会被锁定，需要PUK解锁。点击PIN Management下面的Configure PINs，分别点击Change PIN和Change PUK设置。



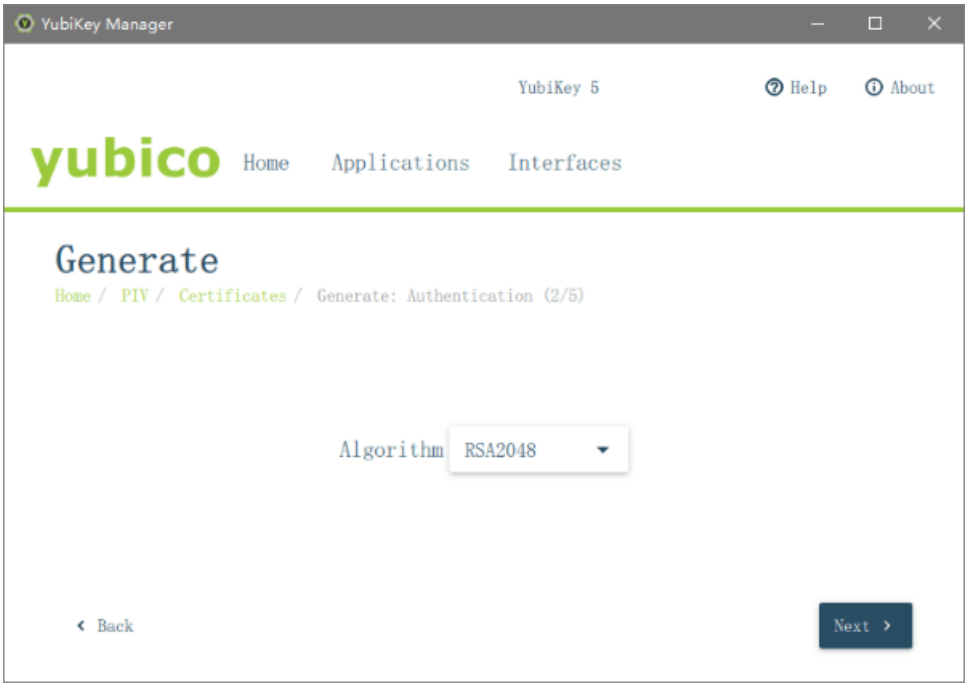
1.2 生成认证证书

完成第1.1步后，让我们返回，点击Certificates栏目下的Configure Certificates按钮，可以看见Certificates页面下有Authentication、Digital Signature、Key Management和Card Authentication几项证书功能，这里我们用到的是第一个Authentication，点击Generate，如下图所示：

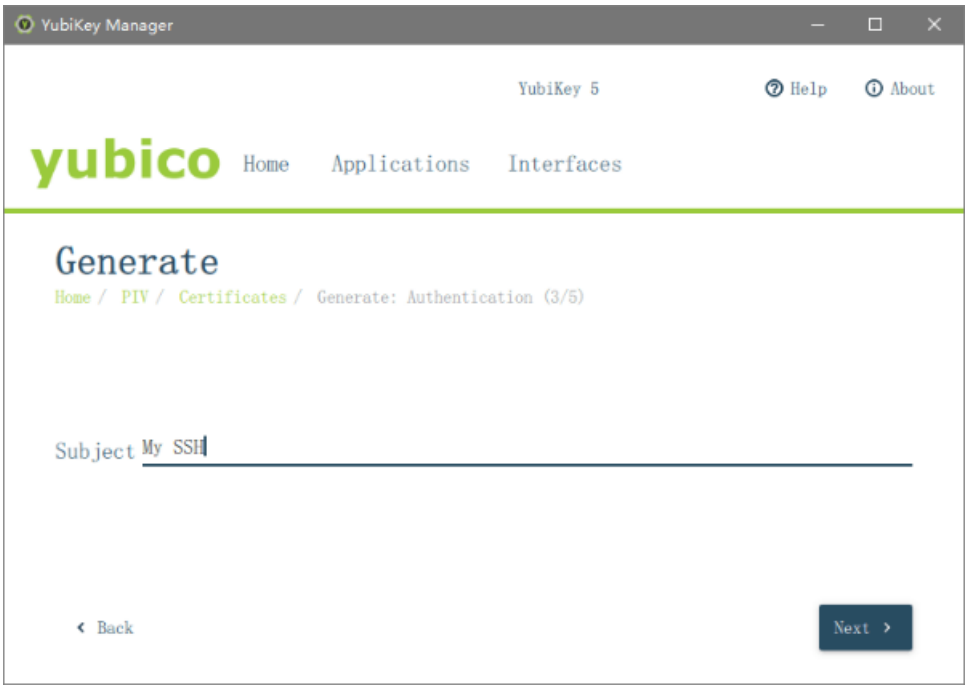
选择Self-signed certificate，点击Next。



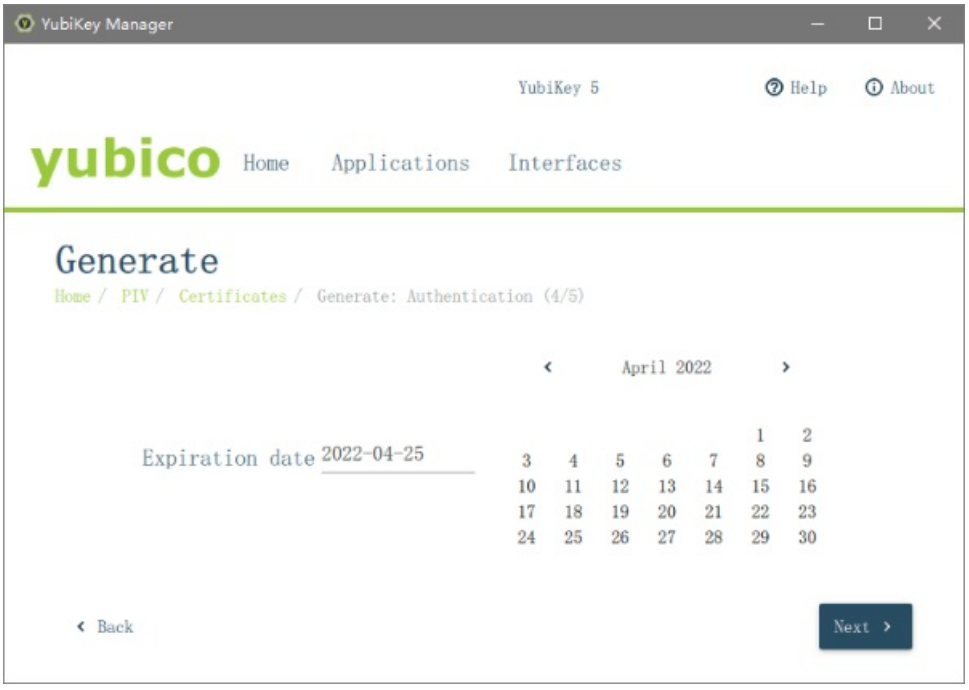
Algorithm选择RSA2048，兼容性较好，安全系数也较高，点击Next。



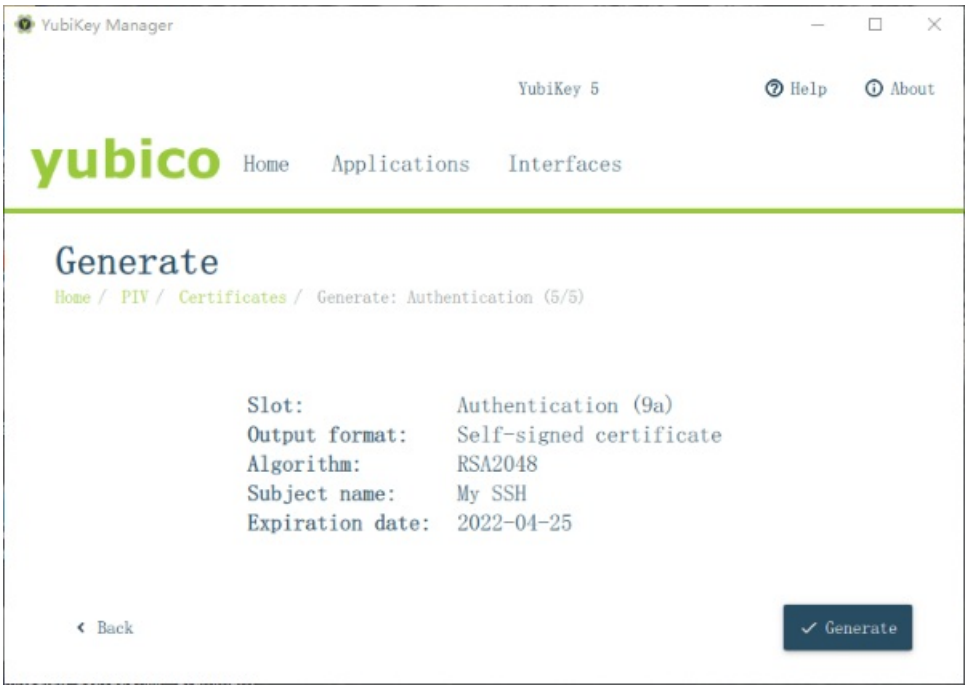
Subject选择一个名称，可以是证书用途描述等，点击Next。



Expiration date可以选择一个较长期限，当然比较好的做法是选择1年后过期，并且在过期前记得更换证书（重新生成），点击Next。



确认无误后就可以点击最后一步Generate生成，这里会要你输入PIN码，请输入刚才配置的PIN码即可，对于Management Key可以勾选Default。



完成生成后就可以在Authentication下看到证书，点击Export将导出证书，点击Delete将删除证书，我发现这里Export实际上导出的是公钥，私钥是无法导出的。 运行WinCryptSSHAgent后在计算机右下角找到那个小锁图标，右击菜单点击`Show Public Keys`就会出现刚才生成证书的SSH登录公钥，点击OK就复制到剪切板中了，这里如果显示No Keys，请重新拔插YubiKey或重启计算机，将登录公钥复制到主机`~/.ssh/authorized_keys`中即可。

2 导入配置好的SSH证书对（私钥+公钥）

如何实现一个证书复制到多个YubiKey呢？刚才我们知道通过YubiKey Manager生成的证书私钥是无法导出的，也就是说其他YubiKey虽然可以导入证书，但无法导入私钥，那么也就无法实现认证，一开始我也为此困惑过，后来豁然开朗——按照安全规范理应多个YubiKey分别生成证书，分别用Subject区分，`authorized_keys`分别存放公钥证书，这样只要其中一个YubiKey丢失或者被窃，只需要注销这个Key的公钥即可消除安全隐患，并且也避免影响其他Key的正常使用，所以我们不需要将所有的Key设置为一个证书对。

当然文章这里我还是简单介绍一下如何实现，以便于有特殊需求的读者参考，以

下操作参考文章Export existing private ssh key to OpenPGP card or YubiKey，因为涉及到私钥，请确保操作的计算机安全。

2.1 将已有的私钥由RFC4716格式转换为PEM格式

使用ssh-keygen命令，注意这个命令只有安装OpenSSH套件才有，操作之前请先备份私钥到安全位置：

```
ssh-keygen -p -f id_rsa -m pem
```

下面的命令用来检查转换是否成功：

```
openssl rsa -in id_rsa -text
```

其中publicExponent的值应该是65537。

2.2 使用转换的私钥创建X.509证书

```
openssl req -new -key id_rsa -out myid.csr
```

完成签名：

```
openssl x509 -req -days 24854 -in myid.csr -signkey id_rsa -out
myid.crt
```

2.3 将私钥和公钥导入YubiKey证书槽9a

参考Yubico官方文档，命令如下：

```
ykman piv import-certificate 9a myid.crt
ykman piv import-key 9a id_rsa
```

当然也可以再次运行YubiKey Manager，依次点击Applications > PIV，Certificates栏目下点击Configure Certificates，点击Generate旁边的Import按钮，导入myid.crt和id_rsa，这里可能看不到id_rsa，将id_rsa改为id_rsa.pem即可。

External References (Links)

WinCryptSSHAgent
https://github.com/buptczq/WinCryptSSHAgent
下载YubiKey Manager
https://www.yubico.com/support/download/yubikey-manager/
Export existing private ssh key to OpenPGP card or YubiKey
https://gist.github.com/artizirk/47dc7104c18c9b02153242476d0a30f0
Yubico官方文档
https://developers.yubico.com/PIV/Introduction/Certificate_slots.html