

使用说明

YQ 软件认证加密功能

版本号：V1.0 发布时间：2020.4.17

目 录

证书生成方法..... 3

1. 软件安装..... 3

2. 生成私钥: 3

3. 生成公钥和证书: 4

4. 导出公钥: 5

软件配置..... 6

1. 导入证书..... 7

2. 安装证书..... 8

Y 系列控制器（卡）支持认证加密功能，经过安装素材认证和通讯加密的证书，实现对素材和通讯的加密。下面将简单介绍一下 Y 系列控制器如何在 LedshowYQ 软件中实现素材认证和通讯加密的功能。

证书生成方法

1. 软件安装

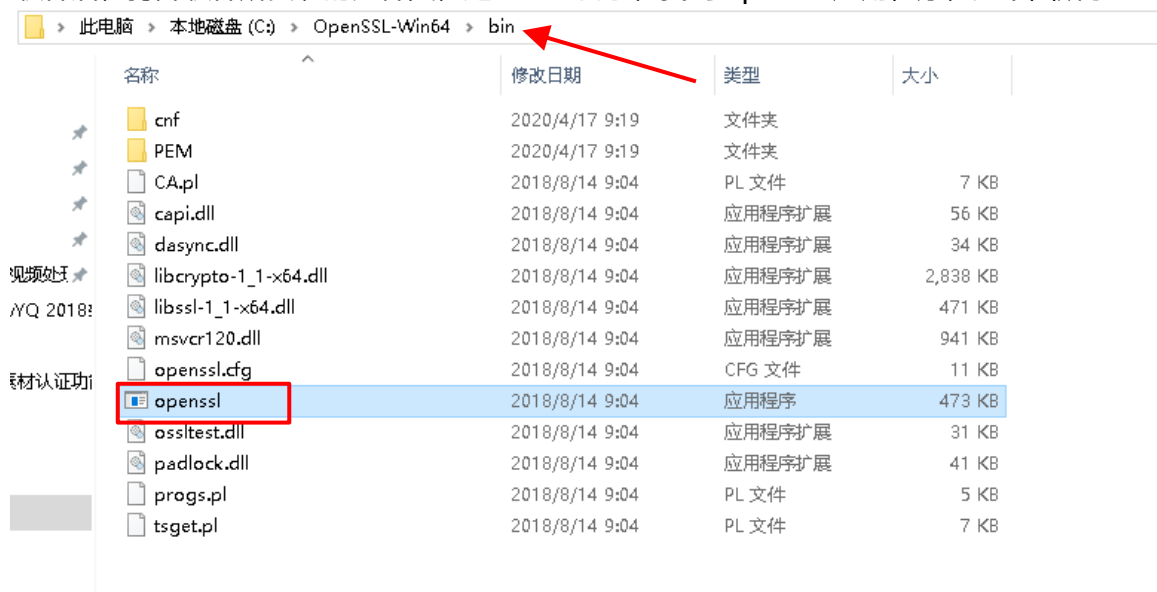
使用 OpenSSL 工具软件生成证书。

首先根据电脑的操作系统下载相关的 OpenSSL 证书生成工具，软件下载链接如下：

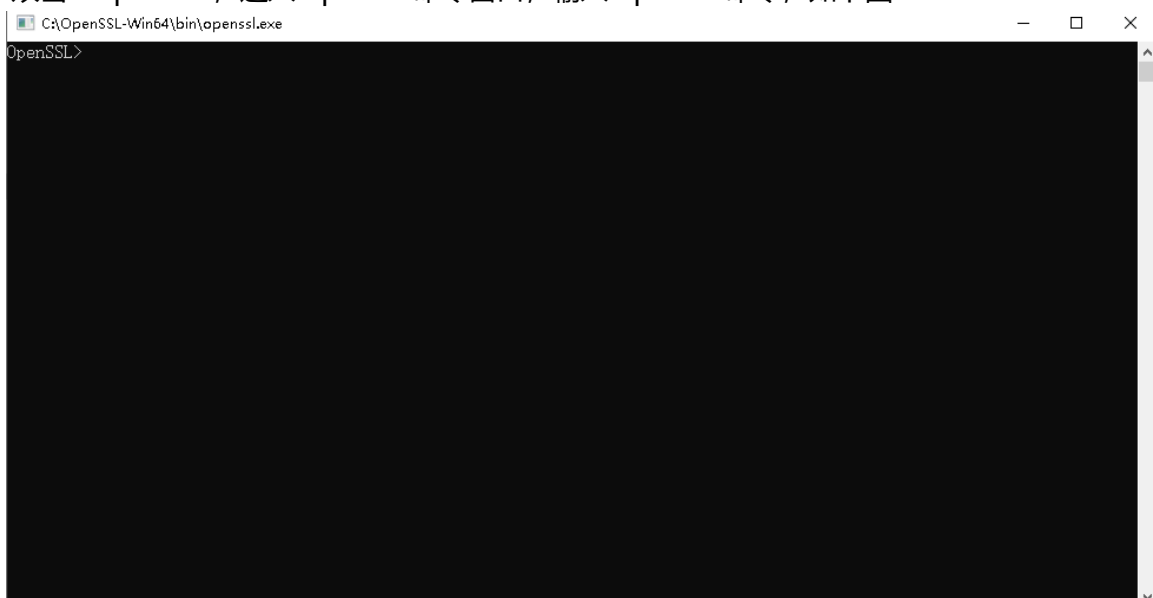
<https://oomake.com/download/openssl>

下面以 windows 64 位操作系统为例：（安装包为：Win64OpenSSL-1_0_2p）

安装软件后，打开软件所安装的文件夹，进入 bin 目录，找到 openssl 应用程序，如下图所示



双击“openssl”，进入 openssl 命令窗口，输入 openssl 命令，如下图：



2. 生成私钥：

```
genrsa -out rsa_private.pem 1024
```

```
Ca\OpenSSL-Win64\bin\openssl.exe
OpenSSL> genrsa -out rsa_private.pem 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
e is 65537 (0x10001)
OpenSSL>
```

3. 生成公钥和证书:

```
rsa -in rsa_private.pem -pubout -out rsa_public.pem
```

```
req -new -x509 -days 365 -out rsa_key.pem -keyout rsa_private.pem
```

输入命令后会需要输入密码，第一遍输入 6 位以上的数字密码后，按回车，第二步重复输入一遍密码后，再按回车即可。

```
Ca\OpenSSL-Win64\bin\openssl.exe
OpenSSL> genrsa -out rsa_private.pem 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
e is 65537 (0x10001)
OpenSSL> rsa -in rsa_private.pem -pubout -out rsa_public.pem
writing RSA key
OpenSSL> req -new -x509 -days 365 -out rsa_key.pem -keyout rsa_private.pem
Generating a 2048 bit RSA private key
.....+++++
writing new private key to 'rsa_private.pem'
Enter PEM pass phrase:
```

接着会要求输入一下国家名称（2 个字符）、省名、城市名称、单位名称、部门、姓名、电子邮箱，按照步骤输入即可。

```

C:\OpenSSL-Win64\bin\openssl.exe
OpenSSL> genrsa -out rsa_private.pem 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
OpenSSL> rsa -in rsa_private.pem -pubout -out rsa_public.pem
writing RSA key
OpenSSL> req -new -x509 -days 365 -out rsa_key.pem -keyout rsa_private.pem
Generating a 2048 bit RSA private key
.....+++++
...+++++
writing new private key to 'rsa_private.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ZG
State or Province Name (full name) [Some-State]:SH
Locality Name (eg, city) []:SH
Organization Name (eg, company) [Internet Widgits Pty Ltd]:onbon
Organizational Unit Name (eg, section) []:RD
Common Name (e.g. server FQDN or YOUR name) []:sandy
Email Address []:1635823@qq.com
OpenSSL>

```

4. 导出公钥:

pkcs12 -export -in rsa_key.pem -inkey rsa_private.pem -out rsa_key.pfx

在导出时需要输入证书的密码 (与第 2 步输入的密码相同), 输入正确后会要求输入导出的 pfx 证书的密码 (与第 2 步输入的密码相同)。

```

C:\OpenSSL-Win64\bin\openssl.exe
e is 65537 (0x10001)
OpenSSL> rsa -in rsa_private.pem -pubout -out rsa_public.pem
writing RSA key
OpenSSL> req -new -x509 -days 365 -out rsa_key.pem -keyout rsa_private.pem
Generating a 2048 bit RSA private key
.....+++++
...+++++
writing new private key to 'rsa_private.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ZG
State or Province Name (full name) [Some-State]:SH
Locality Name (eg, city) []:SH
Organization Name (eg, company) [Internet Widgits Pty Ltd]:onbon
Organizational Unit Name (eg, section) []:RD
Common Name (e.g. server FQDN or YOUR name) []:sandy
Email Address []:1635823@qq.com
OpenSSL> pkcs12 -export -in rsa_key.pem -inkey rsa_private.pem -out rsa_key.pfx
Enter pass phrase for rsa_private.pem:
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL>

```

生成后的证书如下图所示:

地址 > 本地磁盘 (C:) > OpenSSL-Win64 > bin

名称	修改日期	类型	大小
rsa_key	2020/4/17 15:11	Personal Inform...	3 KB
rsa_key.pem	2020/4/17 15:08	PEM 文件	2 KB
rsa_private.pem	2020/4/17 15:08	PEM 文件	2 KB
.rnd	2020/4/17 15:06	RND 文件	1 KB
rsa_public.pem	2020/4/17 15:05	PEM 文件	1 KB
openssl	2018/8/14 8:42	应用程序	491 KB
bad_dtls_test	2018/8/14 8:42	应用程序	17 KB
clienthllotest	2018/8/14 8:42	应用程序	9 KB

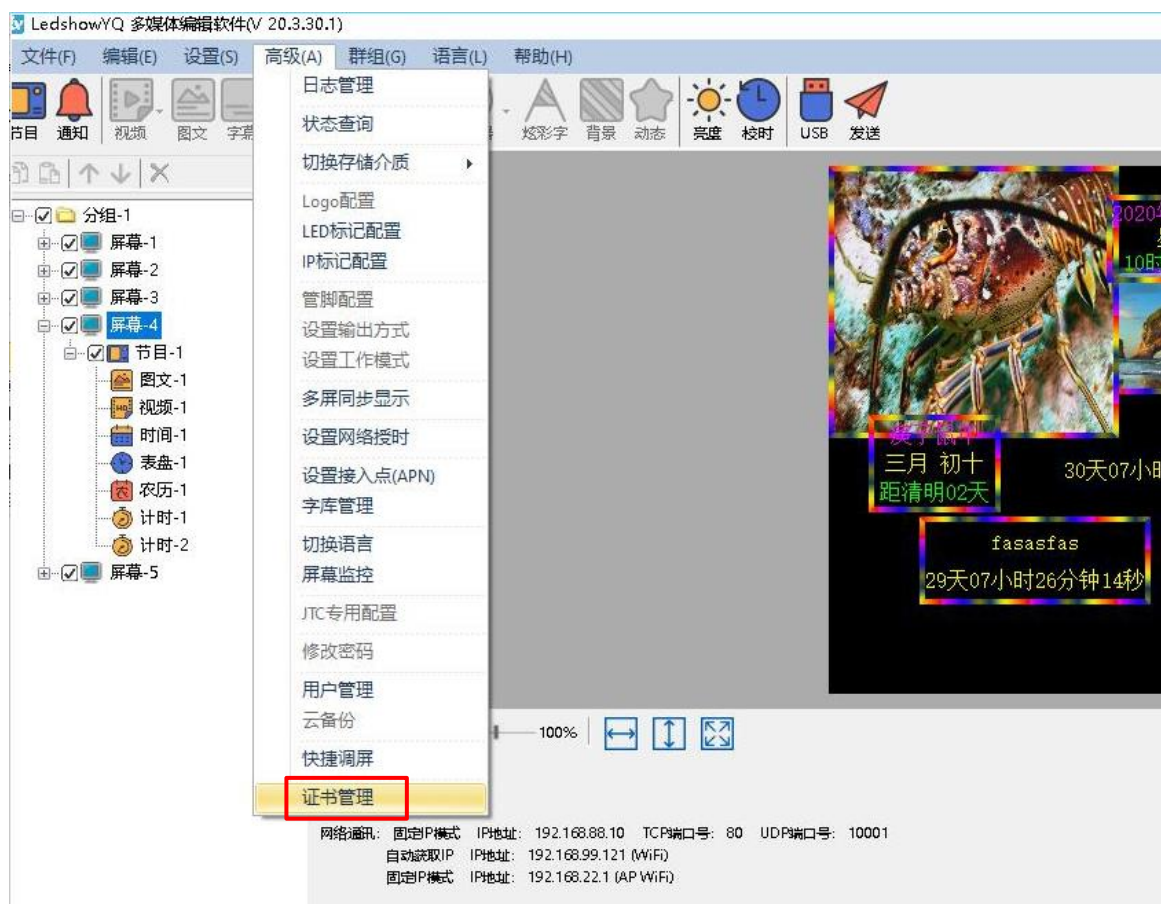
注意：假如客户执行“3.生成公钥和证书”这条命令，出现以下提示：

“ [Unable to load config info from /usr/local/ssl/openssl.cnf] ”

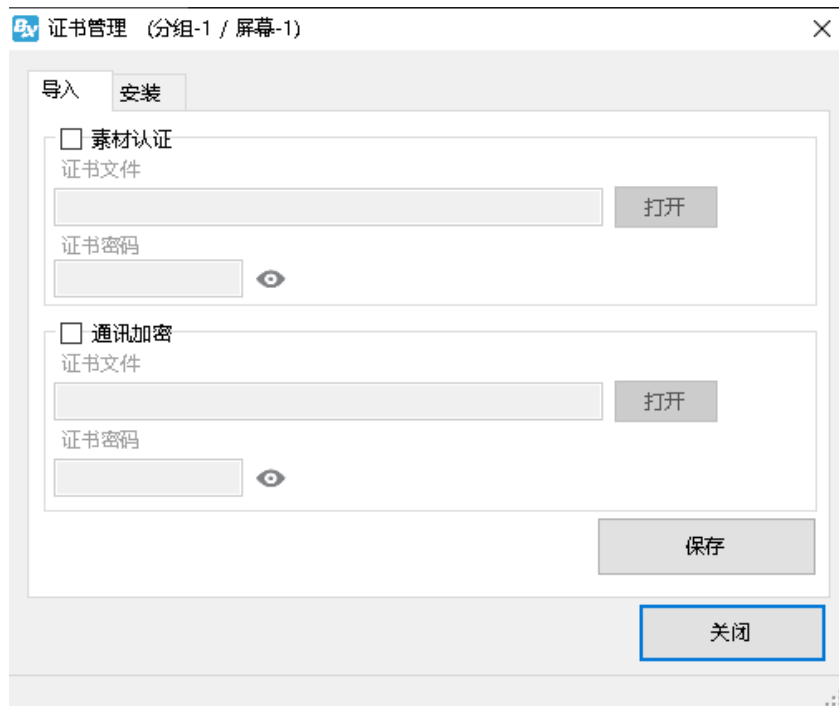
请自行百度搜索“openssl.cnf”，在本地电脑中新建文件夹 c:/usr/local/ssl，把 openssl.cnf 文件放入 ssl 文件夹下就可以解决了。

软件配置

在正确连接 Y 系列控制器后，打开 LedshowYQ 软件。选择“高级”菜单→“证书管理”。



输入密码“888”，进入“证书管理”的界面，如下图所示：



1. 导入证书

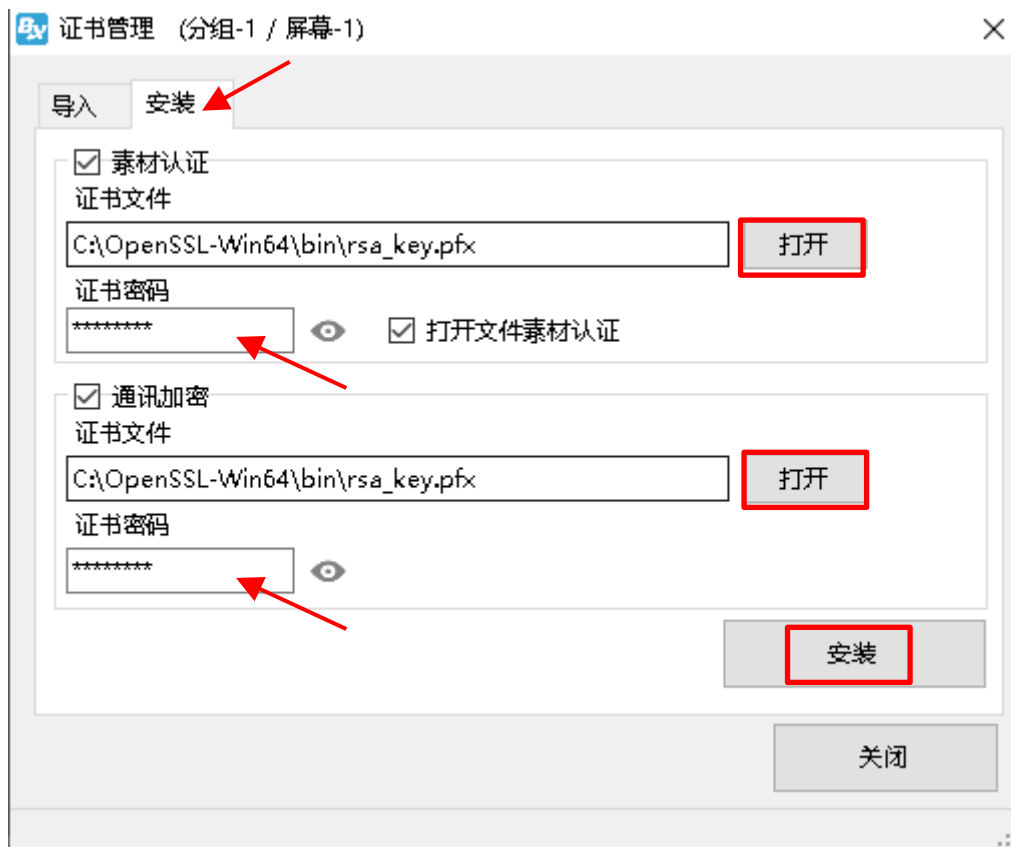
在“证书管理”界面选择“导入”选项，勾选“素材认证”和“通讯加密”，在“素材认证”和“通讯加密”下分别点击“打开”选择对应的证书文件，并且输入证书密码。设置完成后，先点击“保存”，最后点击“关闭”，如下图所示：



证书文件导入完成后，则表示 LedshowYQ 软件中已经导入了对应的证书文件了。

2. 安装证书

在“证书管理”界面选择“安装”选项，勾选“素材认证”和“通讯加密”，在“素材认证”和“通讯加密”下分别点击“打开”选择对应的证书文件，并且输入证书密码，勾选“打开文件素材认证”。设置完成后，先点击“安装”，最后点击“关闭”，如下图所示：



证书文件安装完成后，则表示已经将认证文件安装到了所连接的控制器（卡）中，用户所使用的 LedshowYQ 软件和控制器（卡）已经得到认证加密保护，在使用 LedshowYQ 软件和控制器（卡）的过程中需要通过证书验证后，才能进行通信和节目发送。

上海仰邦科技股份有限公司

地址：上海市徐汇区钦州北路 1199 号 88 幢 7 楼

网址：www.onbonbx.com

昆山光电产业基地

地址：江苏省昆山市开发区富春江路 1299 号



仰邦微信公众号