

playready 3.x 集成操作说明 v1.0

目录

playready 3.x 集成操作说明 v1.0.....	1
1 playready 版本信息	1
2 集成步骤如下: (以 playready3.2 高安为例,其他类似)	2
2.1 申请 playready 根证书	2
2.1.1 签署 SL3000 Amendment 协议	2
2.1.2 下载所需文档和工具	2
2.1.3 生成申请 playready 所需的 key.....	3
2.1.4 申请证书	3
2.1.5 下载证书	4
2.2 生成 playready 设备证书	4
2.3 下载 playready sdk 库文件	6
2.4 获取 tdk 代码	6
2.5 配置 playready 选项并编译	7
2.6 烧录 playready 设备证书	7
2.7 测试	8

1 playready 版本信息

目前 sdmc 各平台的 playready 版本信息如下:

平台	Playready 版本	tdk 版本
S905	Playready2.5	tdk-v1.2
S905X/S912	Playready3.x	tdk-v1.4

2 集成步骤如下: (以 playready3.2 高安为例,其他类似)

- (1) 申请 playready 根证书;
- (2) 生成 playready 设备证书 (keybox);
- (3) 下载 playready sdk 库文件;
- (4) 获取 tdk 代码 (即 secureOS);
- (5) 配置 playready 选项并编译;
- (6) 烧录 playready 设备证书 (keybox);
- (7) 测试 playready 功能;

下面分别介绍以上步骤.

2.1 申请 playready 根证书

要使用 playready 功能首先要申请 playready 根证书, 申请步骤如下:

2.1.1 签署 SL3000 Amendment 协议

(a) 邮件联系微软 WMLA 的工作人员, 向他们提出申请 playready3.x 证书的需求, 联系邮箱是: wmla@microsoft.com

(b) WMLA 收到申请需求后, 会回复一份 SL3000 Amendment 协议让我司确认协议内容并签字, 按要求签字并回复即可。

(c) 签字回复三个工作日左右, 微软 WMLA 方面会把需要电子签名的 SL3000 Amendment 协议链接发送到我司微软账号联系人, 点击链接进行电子签名即可。

到此完成 SL3000 Amendment 协议的签署。

2.1.2 下载所需文档和工具

到微软官网下载 PlayReady Documentation Package v.3.2.4242.exe 和 playready certificate generation request kit v3.0.2726.exe 这两个文件

其中 PlayReady Documentation Package v.3.2.4242.exe 是文档类的安装文件, 点击安装后生成 PlayReadyDocPack.msi 和另外两个文件, 再点击 PlayReadyDocPack.msi 进行安装得到 PlayReady.chm, 这是 playready 的参考文档。

playready certificate generation request kit v3.0.2726.exe 是工具类的安装文件, 点击安装后生成 PlayReadyCertRequestKit.msi 和另一个文件, 点击 PlayReadyCertRequestKit.msi 进行安装得到 generatecompanycertrequest.exe, generatemodelcert.exe, bcertdump.exe 和 generatekeypair.exe 这四个工具类文件, 这些工具在产生申请 playready 的公私密钥和设备证书的时候会用到。

2.1.3 生成申请 playready 所需的 key

在 dos 命令行下进入到上一步的工具类文件所在目录下，然后参考 PlayReady.chm 中产生公司级别 key，命令如下：

Generatecompanycertrequest.exe -r:sdmc_public.xml -p:sdmc_private.xml -m:sdmc

```
C:\playready3>
C:\playready3>generatecompanycertrequest.exe -r:sdmc_public.xml -p:sdmc_private.xml -m:sdmc
Microsoft (R) PlayReady, PlayReady Certificate Request Creation Tool
Copyright (c) Microsoft Corporation. All rights reserved.

Creating Request...
Creating DAC Request...
Creating Private key file...
Done.
Success!
C:\playready3>
```

其中 -m 选项参数是公司的名字，执行该命令会生产 -r 和 -p 两个选项参数所示的文件，其中 sdmc_public.xml 是用于申请 playready 根证书的公钥，sdmc_private.xml 是留给公司用的私钥，私钥必须保存好，不能外流，图示如下：

2.1.4 申请证书

(a) 登陆 <http://rrweb.smdisp.net/> (账号请联系项目经理)，进入 WMLA Licensing Portal 首页，选择 Deliverables，点击 Request Certificate 即可进入申请页面，选择需要申请的证书点击 Request New Cert，如下图所示：

Request Certificate

Your company is currently licensed to request certificates under the following license agreements.

By submitting a certificate request your company agrees that all use of the supplied certificate is subject to the terms and conditions of the license agreement between your company and Microsoft. In addition, please know that certificate requests are subject to the terms of the license agreement and may be delayed if your company has any outstanding invoices or royalty reports.

Begin the certificate request process by selecting the "Request New Cert" link next to the applicable certificate type.

If the certificate you require is not listed please review the FAQ and/or email <mailto:WMLA@microsoft.com> for assistance.

Shenzhen SDMC Technology Co., Ltd

License No.: 5175420025

License Agreement: PlayReady Device Final Product Distribution License

<input checked="" type="checkbox"/>	PlayReady Device PK 2.5/2.11 Certificate	Request New Cert
<input checked="" type="checkbox"/>	PlayReady Device 3.x Certificate SL3000	Request New Cert
	PlayReady Device 3.x Certificate SL2000	Request New Cert
	PlayReady Device PK 2.0 Certificate	Request New Cert
	PlayReady Client SDK for iOS 2.4.1 SL2000 Library	Request New Cert

(b) 填写相关申请信息，如下图所示

Request Certificate

SL3000 PlayReady Device 3.x Company Certificates can only be used in PlayReady Final Products that meet the Requirements for PlayReady Trusted Execution Environments (as defined in the PlayReady Compliance and Robustness Rules). PlayReady Device 3.x Certificates should only be used with the generatemodelcert.exe version 3 tool to create device model certificates in order to support PlayReady 3.x features such as A/V Separation and Secure Stop. !! IMPORTANT !! Company may request a SL3000 Certificate if and when they have signed an additional Amendment to the PlayReady Final Product License. Please contact wmla@microsoft.com with questions.

Existing Cert Info:

Requested Date	9/21/2016 6:41:41 PM
Requested By	Ryan Yan (ryan_yan@sdmctech.com)
Delivered To	Ryan Yan (ryan_yan@sdmctech.com)

New Cert Request:

Ship to contact	ryan_yan@sdmctech.com
PlayReady Public Key	
Company Name	
Generatecompanyrequest.exe Version	

其中三个红框的信息如下：

Playready public key: 这里要填的是 2.1.3 步中所产生的公钥 sdmc_public.xml 文件中的 key 信息，如下图所示：

```
<OEMPrivateKeys>
  <PlayReady>
    <PRIVKEY> jXA+DTklwoSg2EQKGiKQgGzH6YD+w3XiYD0aGPgn7vM=</PRIVKEY>
  </PlayReady>
  <ManufacturerName>SDMC</ManufacturerName>
</OEMPrivateKeys>
```

Company Name: Shenzhen SDMC Technology Co.,LTD

Generatecompanyrequest.exe Version: playready certificate generation request kit v3.0.2726（根据实际情况填写）

填写完成后提交申请。

2.1.5 下载证书

完成 2.1.4 步的申请后，邮件通知 WMLA，顺利的话一般三个工作日左右微软会把证书以链接的形式发过来，打开链接下载即可得到回复的根证书文件，此次的 playready3.2 的证书文件是 Shenzhen_SDMC_Technology_Co._Ltd_Device3.xCompanyCert_5175420025_6125_SL3000.exe，点击安装后即可得到 PRDACResponse.dat，PRDACRequest.xml 和 GeneratePRDevice3000.cmd 三个文件，其中 PRDACResponse.dat 和 PRDACRequest.xml 就是申请的 playready 根证书。

2.2 生成 playready 设备证书

生成 playready 设备证书的工具是 2.1.2 步中的 generatemodelcert.exe，参

考 PlayReady.chm 中 generatemodelcert.exe 的使用, 生成证书的命令如下:

```
generatemodelcert.exe -z:PR -u:unsignedtemplate3000.dat -b:PRDACResponse.dat -f:sdmc_private.xml -g:bgroupcert.dat -h:zgpriv.dat
```

```
C:\playready3>
C:\playready3>generatemodelcert.exe -z:PR -u:unsignedtemplate3000.dat -b:PRDACRe
sponse.dat -f:sdmc_private.xml -g:bgroupcert.dat -h:zgpriv.dat
Microsoft (R) PlayReady Model Certificate Creation Tool
Copyright (c) Microsoft Corporation. All rights reserved.

Reading OEM private keys...
Reading unsigned template...
Reading binary company certificate...
Parsing OEM keys file to obtain necessary private keys...
Generating binary certificate...
Success!
C:\playready3>
```

其中 -z, -u, -b, -f 四个选项为输入参数, -g 和 -h 选项参数为输出结果。

各输入参数说明如下:

-z 参数: 指示证书类型;

-b 参数: 公司所申请到的根证书, 也即 2.1.5 步中微软回复的根证书文件 PRDACResponse.dat;

-f 参数: 公司的私钥, 也即 2.1.3 步中产生的私钥文件 sdmc_private.xml;

-u 参数: 设备证书的模板, 可参考 PlayReady.chm 中相关的章节进行创建或修改, 但最好跟 amlogic 原厂的 RD 拿一份现成的过来用, 该文件中的 NAME 域是设备的名称, 可根据公司的情况修改; SECURITYLEVEL 对于 playready3.x 来说是 3000; CLOCK 域填的是 1, 具体可参考下图:

```
1 <UNSIGNEDTEMPLATE>
2 <NAME>ContosoCoolNewDevice</NAME>
3 <MODEL>XR-700</MODEL>
4 <SECURITYLEVEL>3000</SECURITYLEVEL>
5 <FEATURES>
6 <CLOCK>1</CLOCK> <!-- 1 for anti rollback clock or 2 for secure clock -->
7 <SUPPORT_REVOCATION>1</SUPPORT_REVOCATION>
8 <PLAYREADY3FEATURES>1</PLAYREADY3FEATURES>
9 <!--<TRANSMITTER>1</TRANSMITTER>-->
10 <!--<RECEIVER>1</RECEIVER>-->
11 </FEATURES>
12 <keyusages>
13 <Sign>1</Sign>
14 <IssuerDevice>1</IssuerDevice>
15 <!--<IssuerLink>1</IssuerLink>-->
16 </keyusages>
17 </UNSIGNEDTEMPLATE>
```

输出结果为:

-g 参数: 生成的设备证书 bgroupcert.dat

-h 参数： 生成的设备证书所对应的私钥 zgpriv.dat

playready3.x 需要用 KeyWrapTool.exe 工具对上面产生的私钥 zgpriv.dat 进行封装，以更好地保护私钥，命令如下：

KeyWrapTool.exe -k:zgpriv.dat -w:SampleKeyWrapContext.xml -o:zgpriv_protected.dat

```
C:\playready3>KeyWrapTool.exe -k:zgpriv.dat -w:SampleKeyWrapContext.xml -o:zgpriv_protected.dat
Microsoft (R) Key Wrapping Tool
Copyright (c) Microsoft Corporation. All rights reserved.

Success!!
C:\playready3>
```

各命令参数解析如下：

-k 参数： 为上一步用 generatemodelcert.exe 所产生的私钥 zgpriv.dat

-w 参数： 封装所用到的密钥模板，可参考 PlayReady.chm 中 KeyWrapTool.exe 的使用来进行创建或修改，也可以跟原厂要一份现成的来用，其内容如下：

The XML format is as follows:

```
<root>
  <KeyWrapContext>
    <RootAesKey>iyIv/R52GVZ2zycDiYxCfw==</RootAesKey>
    <Label>nOk0MsfXQBa6aEdj+AHhNg==</Label>
    <Context>AAAAAAAAAAAAAAAAAAAAAA==</Context>
  </KeyWrapContext>
</root>
```

-o 参数： 最终所用的私钥 zgpriv_protected.dat

2.3 下载 playready sdk 库文件

从 git 独立仓库中下载 playready sdk 3.x 的库文件到 vendor 目录下，命令如下：

```
cd vendor
git clone ssh://git@openlinux.amlogic.com/vendor/playready -b m-amlogic-3.x
```

2.4 获取 tdk 代码

高安需要运行于 secure OS 上，因此要下载 tdk 代码，下载到的路径为 vendor/amlogic，命令如下：

```
cd vendor/amlogic/
git clone username@10.10.121.100:/home/svn/amlogic\_kk\_git\_mirror/kitkat/tdk -b tdk-v1.4
```

其中 username 为你个人的账号

2.5 配置 playready 选项并编译

高安需要用特定的 uboot 来使能 secure OS，此处是把 2.4 步中下载的 tdk 代码中的 bl32.img 文件拷到 uboot 下对应的目录，如下所示：

```
cp vendor/amlogic/tdk/secureos/gx/bl32.img uboot/fip/gxl/bl32.img
```

再编译 uboot 并把所需的编译结果文件拷到 device 目录下即可，以 q201 为例，操作如下：

```
cd uboot
./mk gxm_q201_v1
cd ..
cp uboot/fip/gxl/u-boot.bin device/amlogic/q201/
cp uboot/fip/gxl/u-boot.bin.usb.bl2 device/amlogic/q201/upgrade/
cp uboot/fip/gxl/u-boot.bin.usb.tpl device/amlogic/q201/upgrade/
cp uboot/fip/gxl/u-boot.bin.sd.bin device/amlogic/q01/upgrade/
```

android 6.0 的代码中不需要手动去配置其他的选项，只需要在编译 android 源码的时候 export BOARD_PLAYREADY_LEVEL=1 即可打开所有需要的开关，编译出高安的升级包，（android 源码根目录下）操作如下：

```
export BOARD_PLAYREADY_LEVEL=1
source ./build/envsetup.sh
lunch q201-user-32
make otapackage -j8
```

2.6 烧录 playready 设备证书

把上面生成的 key 文件 bgroupcert.dat 和 zgpriv_protected.dat 拷到 tf 卡根目录下，进入 uboot，手工烧录 playready keybox 的命令如下：

```
keyunify init 0
mmcinfo
fatload mmc 0 12000000 bgroupcert.dat
keyunify write prpubkeybox 0x12000000 1344
fatload mmc 0 12000000 zgpriv_protected.dat
keyunify write prprivkeybox 0x12000000 48
```

注意：上面第四条命令的最后一个参数 1344 是 bgroupcert.dat 文件的长度，是第三条命令中读取文件所得的长度，每个不同的 bgroupcert.dat 长度是不一样的，请根据读取到的文件长度进行相应的修改。

2.7 测试

安装 PlayReady.apk，并播放第一个视频链接，可以播放则 playready3.x 高安版本集成成功。