



## Contents

- [1 How to protect Flash Lite content with OMA DRM 1.0 Forward Lock when content is packaged into a Symbian installer .sis](#)
- [2 Packaging Flash Lite content into a SIS installer file](#)
- [3 Create a Protected Installation Package \(PIP\)](#)
- [4 Apply OMA DRM 1.0 Forward Lock to a PIP file](#)
- [5 Test OMA DRM 1.0 Forward Lock .pip protected content](#)

## How to protect Flash Lite content with OMA DRM 1.0 Forward Lock when content is packaged into a Symbian installer .sis

Following my previous article on [How to protect Flash Lite content with OMA DRM 1.0](#), I went a step forward and found the way to protect Flash Lite content when is packaged using the Symbian installer format: .sis.

### Packaging Flash Lite content into a SIS installer file

The first step is to create a .sis installer which allows packaging Flash Lite content into a single file ready for installation on a mobile phone.

### Create a Protected Installation Package (PIP)

To protect content packaged into a .sis installer there is an appropriate format called ?Protected Installation Package or PIP? which takes the extension .pip.

So let's say that you created your Flash Lite content (test.swf) and that you packaged it into a Symbian installer called **test.sis**. Here is an article on [How to make Flash launcher with Symbian C++](#)

Now you need to create a .pip file (**test.pip**) which is basically a zip file. (Create a zip file with the files listed below and rename the extension from .zip to .pip). It contains the following files:

**test.sis**

**datafiles.def**

**test.swf**

The **datafiles.def** will contain the following text:

**application**

**test.swf application/x-shockwave-flash c:\DATA\Others\test.swf**

It basically defines which file to protect, its MIME and the location where is stored on the mobile phone after installation.

The **test.swf** is your Flash Lite content which is contained also into the test.sis file. **Important Note:** to protect your Flash Lite content (.swf) you must know the location where the .swf is installed. The location (a directory) must be defined in the datafiles.def file as described above. For more information and details about .pip files format refer to the [S60 Platform: Implementing OTA Application Delivery and Protection](#) white paper on Forum Nokia. Remember that to apply OMA DRM 1.0 you need to use one of the delivery method explained by the OMA DRM specification. The simplest way is to create a mobile web page.

The following MIME types are defined for OMA DRM; you will need to configure them into your Web Server so that OMA DRM protected files will be recognized by the mobile phone upon downloads.

**application/vnd.oma.drm.rights+xml .dr**

**application/vnd.oma.drm.rights+wxml .drc**

**application/vnd.oma.drm.content .dcf**

**application/vnd.oma.drm.message .dm**

**application/vnd.oma.drm.dd+xml .dd**

Note: the **?application/vnd.oma.drm.message?** is the only one required for OMA DRM Forward Lock 1.0.

Also you will need to set the following MIME to support **.pip** and **.sis** file types:

**application/x-pip pip**

**x-epoc/x-sisx-app sis**

**x-epoc/x-sisx-app sisx**

## Apply OMA DRM 1.0 Forward Lock to a PIP file

I will use the NMIT 4.1 tool to apply OMA DRM Forward Lock 1.0 to a .pip file with a step by step process. I will not go into details for each option but you can refer to the NMIT 4.1 User Guide to learn more about all the capabilities and features of the tool.

**Step 1, see Figure 1:**

Start the [NMIT 4.1 tool](#). If you have the Nokia S60 SDK installed you will see the following screen.

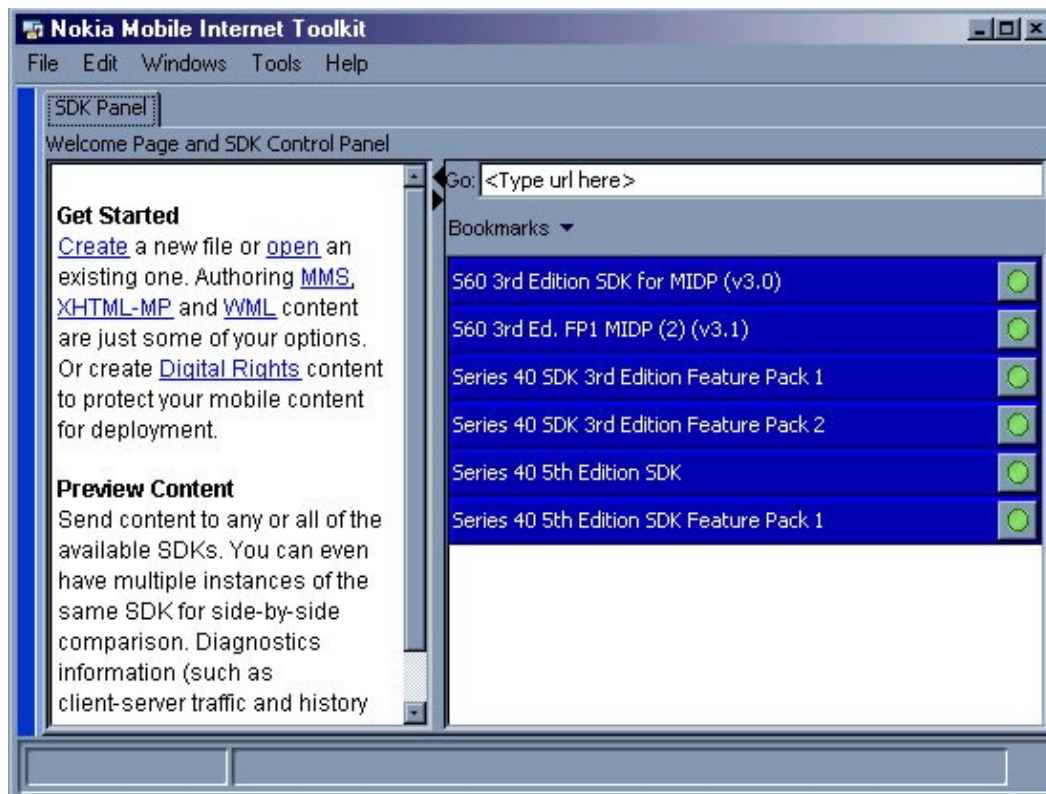


Figure 1, Nokia Multimedia Internet Toolkit 4.1 start-up screen

Step 2, see Figure 2:

1. Select File, New. The ?Available Content Types? screen will open
2. Select the Deployment tab
3. Select the DRM Message icon
4. Press OK

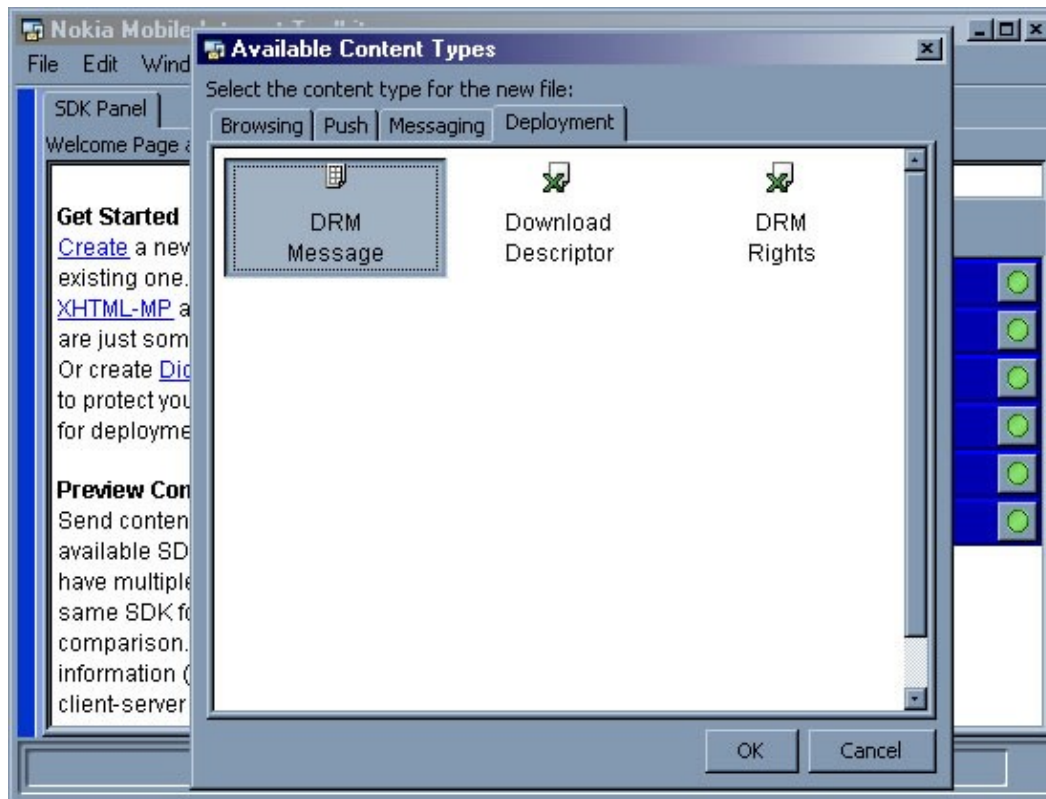


Figure 2, NMIT 4.1 ? Deployment screen

Step 3, see Figure 3.

The following screen is where I will define the type of DRM to apply to the .pip file. There are four sections on this screen.

?The first section, ?1. Select Message Type? allows you to select which type of OMA DRM 1.0 to apply to the content. I will use Forward Lock so no changes are needed since this is the default.

?The second section, ?2. Load Media Content?, allow you load to load the file that you want to protect. In my case it will be a PIP file (.pip). Also leave the ?Content-Transfer-Encoding? to binary.

?The third section, ?3. Edit Header?, allow you to define the headers. I will enter the application/x-pip information into the Content-Type line.

?The fourth section, ?4. Specify Rights? is not used for Forward Lock DRM. In case you use another DRM protection method you will have several options available. Refer to the manual for more information.

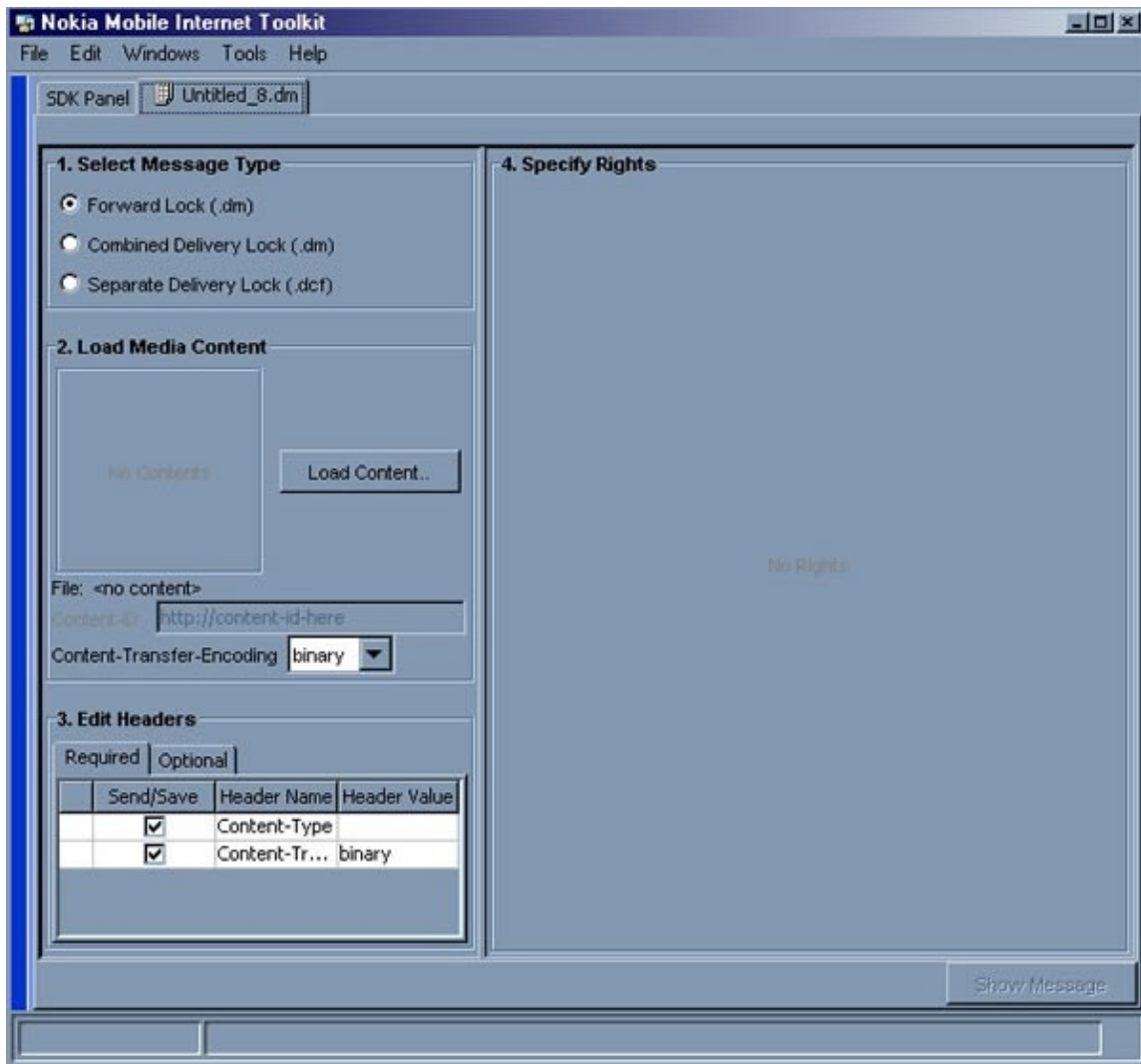


Figure 3, DRM definition window

Step 4, see Figure 4:

1. Load your .pip file using 'Load Content' button from the section '2. Load Media Content'. I loaded the **test.pip**.

2. Add the **application/x-pip** information into the Content-Type line in the '3. Edit Headers' section. This step is necessary since the tool does not recognize the Flash file format.

3. Save the file. I saved as test.dm.

At this point I have a so called DRM message file ready for deployment. I will need to upload it to my web server for download and installation.

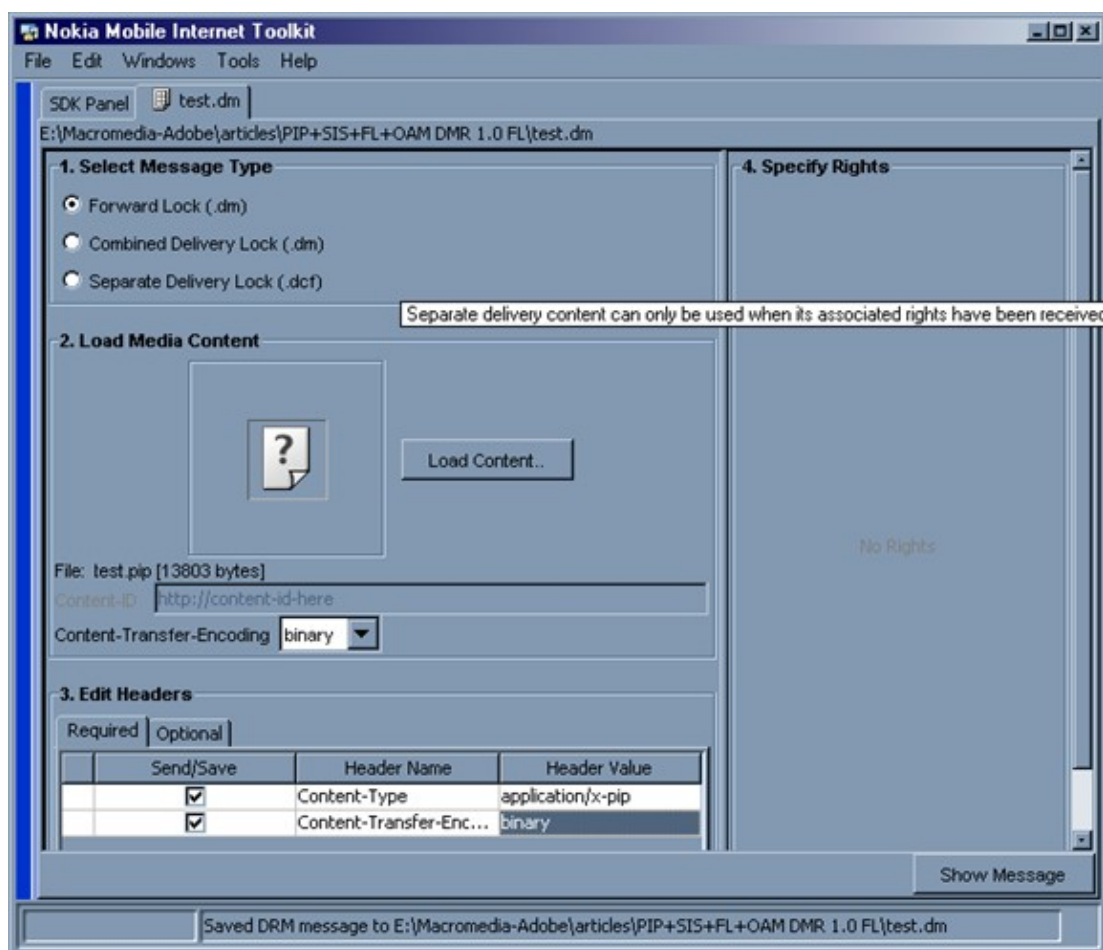


Figure 4, apply OMA DRM 1.0 Forward Lock to the test.pip

**Important Note:** the protection will only be applied once a user downloads the test.dm file from the mobile site to the phone.

## Test OMA DRM 1.0 Forward Lock .pip protected content

To test the protected .pip content you can follow the step by step instruction from my previous article on [How to protect Flash Lite content with OMA DRM 1.0](#) and adapt them to your content. You just need to upload your test.pip file.

Alessandro