

**Objective:** Provide a usable and secure system for implementing modular AIR applications.

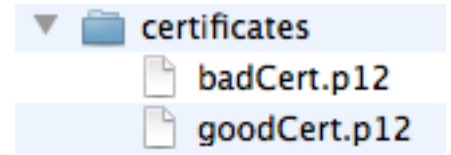
**Problem:** AIR offers two main loading methods. *Loader.load()* and *Loader.loadBytes()*. External swf content loaded using *load()* is heavily restricted by the non-application sandbox. External swf content loaded using *loadBytes()* is free to run riot on the user's system, and a potential source of malicious code.

**Solution:** A loading system which only allows swfs which have been signed using the same security certificate as the original AIR application to be loaded into the application sandbox.

### How do I create modules?

Signed modules should be created using Flash, published as .air packages and then renamed as .zip, or should be created using adt.

In this implementation the modules must also implement an interface: *ITestableModule*. If you want to load modules into this application you should sign them using the provided test certificates. The passwords are 'goodpw' and 'badpw'.



### How do I load modules?

In this implementation the user is invited to browse for an xml file containing the module specifications. A module spec consists of:

```
<moduleIdentifier_txt>GoodModuleA</moduleIdentifier_txt>
<moduleName_txt>Good Module A</moduleName_txt>
<moduleLocalPath_fp>GoodModuleA/GoodModuleA.swf</moduleLocalPath_fp>
<moduleResourcePath_fp><![CDATA[http://aaa.com/GoodModA.zip]]></moduleResourcePath_fp>
<isLoadToApplication_boo>1</isLoadToApplication_boo>
```

The application then attempts to install and load all the modules in the xml. So - just add your new modules to that file to see how they load.

### How do I remove modules?

The modules get installed in application-storage. On mac that's  
~user/Library/Preferences/ ... then the application id (com.newloop.air... etc).

### What can I use this code for?

Anything you like. It'll probably need a bit of tinkering with to meet your specific need, but if you have any questions contact me on the email above.

### What do you mean by 'secure'?

There's no such thing as perfect security. The objective here is to make this structure sufficiently resistant to man-in-the-middle attacks that it's not the route of choice for someone who wants to do something malicious to the user / company / network. If you find a big hole please let me know. If you can break it - let me know.

Overview of class responsibilities

