Software Development Kit

Apple Data Security Services

Installation and Usage Notes

Version 1.0b
August 4, 1999

Apple Data Security SDK overview

This SDK includes all of the components needed by developers to digitally sign Macintosh files and use the new application program interfaces provided as part of the Apple Data Security architecture.

Installation

Apple Data Security components are installed as part of the basic Mac OS 9 installation. If you need to reinstall these components, they are provided in the folder labeled "to System Folder". Select all of the files in this file, drag them on top of a closed System Folder, and restart.

Creating a keychain

The certificates used for signing and verifying files are stored in a keychain file. To create a new keychain, select "Keychain Access" from the Apple menu. The resulting keychain file will be stored in a folder called "Keychains" inside the Preferences folder in the System Folder.

Using the Apple Debug Root certificate

When signing files that will be shipped to your customers, you will need to use a level 2 signing certificate from Verisign or Thawte. Since this certificate must remain secure, it should not be used for testing purposes. To test signed files with your application, you can use a special root certificate provided with this SDK. This certificate is provided in its own keychain file. The file, "AppleDebugRoot" is contained in the "Utilities" folder of the SDK. To use this file, copy it to the "Keychains" inside the Preferences folder in the System Folder.

The CreateCertChain application will search this special keychain when it is looking for valid signing root certificates. When the signing application asks you to unlock the AppleDebugRoot keychain, enter a blank password.

Note that files signed with testing certificates signed by the Apple Debug Root certificate will show a special dialog to the user when the file is verified indicating that the signature is for testing purposes only. In addition, calls to the verify API functions will return a special error (if no other errors are detected first).

Using the CreateCertChain application

This tool is provided to create certificate chains that can be used for testing purposes. The AppleDebugRoot certificate cannot be used for signing, since the private key is not available. Use this tool to create a certificate chain with a new signing certificate. When the application asks "`Choose a signing root:`", you should always choose `"[1] APPLE ROOT FOR DEBUGGING PURPOSES ONLY".` The other option will also create a certificate chain, but the files signed with those certificates do not meet the requirements for the Macintosh File Signing trust policy, and so verification will fail.

A sample run of the CreateCertChain application is shown below.

Sample Run of the CreateCertChain application

```
Beginning

Choose a key algorithm:
  [1] RSA
  [2] DSA
-> 1
With that algorithm, the key size (in bits) should be
Any size (suggested 512, 768, 1024)
Enter the key size (in bits):  1024
Allowed signing algorithms:
  [1] MD2WithRSA
  [2] MD5WithRSA
  [3] SHA1WithRSA
Choose a signing algorithm:
3
Choose a signing root:
  [1] APPLE ROOT FOR DEBUGGING PURPOSES ONLY
  [2] Newly generated root
-> 1
Enter number of certs to create (1 - 8): 3
Cert chain verifies OK
```

Using the FileSignerTool MPW Tool

Copy this MPW tool from the Utilites folder of the SDK to the "Tools" folder inside your MPW folder. You should have already run the CreateCertChain tool to create a signing certificate. Open Keychain Access and find the certificate labelled "Personal Certificate". Double click on this, or select it and click on "Get Info". The name of the certificate in the information dialog can be copied and used for the "-c" parameter of the tool. Here is a sample run of the tool:

```
FileSignerTool -f 'Hard Disk:Test Files:test7' -c
"William Debug Shakespeare cert"
...Removing old signature
...File "test7" signed successfully
```

The -c parameter is the name of the signing certificate as it appears in the keychain.