

How do I get my Symbian OS application signed?

A guide to Symbian Signed

INTRODUCTION	2
PRE-REQUISITES	2
PROCESS.....	3
STEP 1 - GETTING AN ACS PUBLISHER ID FROM VERISIGN	3
STEP 2 - SIGNING YOUR .SIS FILE WITH YOUR ACS PUBLISHER ID	6
<i>Use of ACS Export tool.....</i>	6
<i>ACS Publisher ID signing.....</i>	7
STEP 3 – SUBMIT YOUR APPLICATION FOR TESTING	8
<i>Registration</i>	8
<i>Submitting your application.....</i>	8
<i>What to submit in the .ZIP file</i>	8
<i>Important to check before submitting your application.....</i>	8
<i>Symbian Signed checklist.....</i>	9
STEP 4 – TEST HOUSE TESTING.....	9
WHEN THE APPLICATION HAS PASSED THE TESTS	10
APPLICATIONS CATALOG	10
WHERE TO GET HELP	10
APPENDIX.....	11
ACS PUBLISHER IDS AND CHINA	11

Introduction

This document provides a step by step guide on how to get your application Symbian Signed.

Pre-requisites

Symbian is available for native (C++) Symbian and AppForge MobileVB applications. At present, signing is offered for applications on a range of UIs.

If any of the following statements apply to you then you do not need to use Symbian Signed for your application:

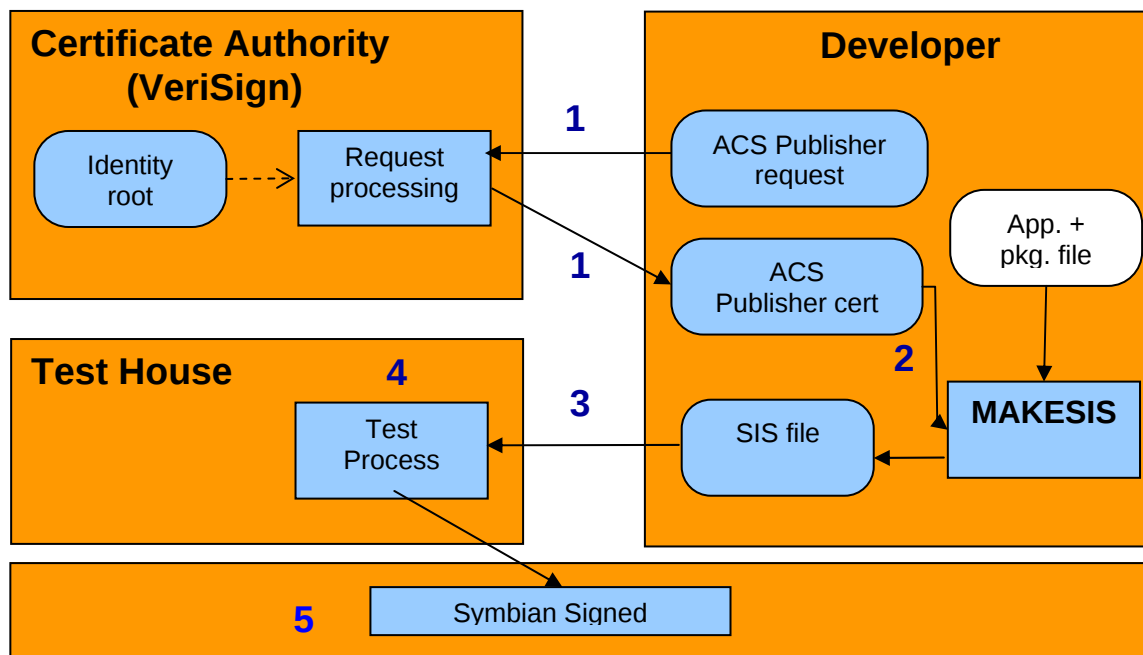
- Developers with applications for the Nokia 9200 Series Communicator should continue to work with Nokia.OK to test and sign their products.
- MIDP developers should use Sun's Java Verified Program – Symbian is working closely with this program to ensure Symbian OS phones are supported.
- Developers working with development languages other than C++ and AppForge MobileVB (e.g. OPL). We are examining how such development languages can be incorporated into the evolution of Symbian Signed.

Important! It is recommended that you read the '[Frequently Asked Questions](#)'

Process

The diagram below outlines the process that needs to be followed to get an application signed.

1. Register for an ACS Publisher ID from VeriSign.
2. Sign your .SIS file with your ACS Publisher ID.
3. Submit your application for testing using www.symbiansigned.com.
4. Your application is tested by the TEST HOUSE against set test criteria.
5. If the application passes the tests your application will be able to download your Symbian Signed application.



Step 1 - Getting an ACS Publisher ID from VeriSign

To sign your application you will need an ACS Publisher ID (Authenticated Content Signing Publisher ID) from VeriSign. An ACS Publisher ID (also known as a developer identity certificate), uniquely identifies you, the software provider, and allows software passing through Symbian Signed to be traced to you, its source. If you already possess an ACS Publisher ID and your SIS file has already been signed with the ACS Publisher ID go to [Step 3 - Submit your application for testing](#).

Note: Make sure that you store the challenge response password as this will be required later.

You can obtain an ACS Publisher ID from VeriSign [here](#) and requires you to register with VeriSign. VeriSign will perform appropriate company background checks and when identity is verified, issue you with an ACS Publisher ID. There is a \$350 per annum charge for the ACS Publisher ID, however it is valid for one year and can be used to sign an unlimited number of applications through Symbian Signed. The ACS Publisher ID is also suitable for signing on other platforms and includes 10 free signing instances. To avoid any delay please ensure you provide all documentation required.¹

¹ If you are based in China then please refer to the Appendix for information on how to obtain your ACS Publisher ID.

When applying for the ACS Publisher ID you must provide a technical contact and the contact details of one other member of your organization. Both of your selected contacts will be contacted during the verifying process, and hence should be informed that they have been nominated.

You will be notified via email by VeriSign as soon as they have verified your details. Accessing the URL in the email, enter the PIN provided in the notification email (this is a 32 digit PIN) and the challenge phrase you used on registering.

Pick Up Certificate

When picking up your certificate, use the same machine and browser that you used during enrollment.

Copy and paste the certificate Personal Identification Number (PIN) to pick up your certificate. The PIN is found in the e-mail sent to the Technical Contact specified during enrollment.

Generating your certificate may take up to three minutes. Do not interrupt the browser until there is a response.

Enter PIN

Certificate Personal Identification Number (PIN):

Enter Challenge Phrase

Challenge Phrase:

If you do not remember the challenge phrase, please contact :
VeriSign Customer Support
Hours of Operation: 5AM-6PM Pacific Time, Monday-Friday
E-mail: support@verisign.com
Web: <http://www.verisign.com>
Phone: 1-877-GET-VRSN (1-877-438-8776) or 1-650-426-3400
Fax: 1-650-961-8870

Continue

After successful authentication, you will be prompted with the screen below. Do not change any of the default options. Ensure that the 'Check this box...' checkbox is not **ticked**. Protecting the private key will prevent the key being extracted from the certificate store, which will prevent you from signing your SIS file later. Select 'Continue' to progress.

Pick Up Certificate

When picking up your certificate, use the same machine and browser that you used during enrollment.

Copy and paste the certificate Personal Identification Number (PIN) to pick up your certificate. The PIN is found in the e-mail sent to the Technical Contact specified during enrollment.

Generating your certificate may take up to three minutes. Do not interrupt the browser until there is a response.

Select your Cryptographic Service Provider

Select the cryptographic service provider (CSP) you will use with your certificate. If you use a specialized device (such as a smart card or hardware token) to manage your private key, select the appropriate provider from the list. If you are unsure which CSP to choose, select the default.

* Required Field

* Cryptographic Service Provider:

Check this Box to Protect Your Private Key ☐

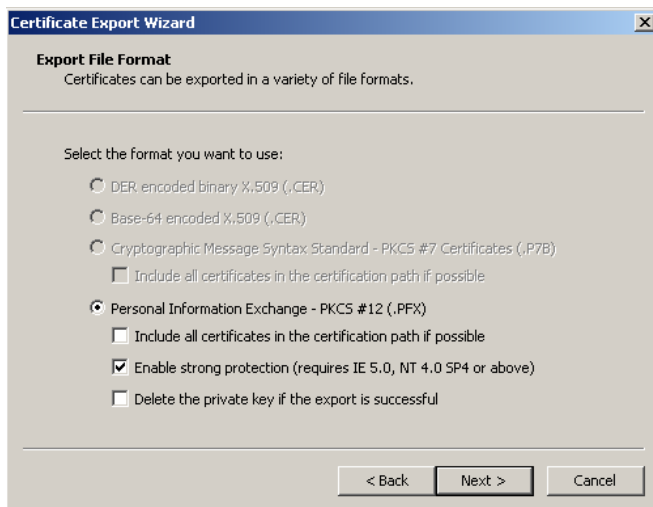
Continue

Once the install process is complete check the Certificate has been loaded to your browser correctly. Go into your Internet Explorer browser menu, select *Tools, Internet Options, Content* and click *Certificates*. You should see a certificate issued by VeriSign; this is your ACS Publisher ID.

Your ACS Publisher ID consists of a public and private key. The private key should be kept secret as it allows files to be signed with your identity. The public key allows third parties to verify that files have been signed with your valid private key.

Your public and private keys should be exported from your web browser into a .pfx file. To export your keys from Microsoft Internet Explorer 5 complete the following steps.

1. Select *Internet Options* from the Tools menu.
2. Click on the *Content* tab.
3. Click on the *Certificates* button.
4. Navigate to your ACS Publisher ID certificate using the tabs and scrollbar.
5. Select your ACS certificate, and click on the Export button.
6. Ensure the option to export private key is selected.
7. Select the PKCS#12 format (see below for details).



It is recommended you provide a password to protect your keys

8. Provide a file name (do not browse)
9. Export the file to a location to be used by the ACS Export tool.

Step 2 - Signing your .SIS file with your ACS Publisher ID

Before progressing further, download the **ACS Export tool** which can be found [here](#). This tool is required by the Symbian Signed process to convert your private key and public certificate into a format MakeSIS can use.

The signing process is divided into two stages.

- Export of Certificate (using the vs_pkcs tool that you have just downloaded from VeriSign).
- ACS Publisher ID signing your .SIS file.

Use of ACS Export tool

The ACS Export tool (vs_pkcs.exe) takes as input the .pfx file that you exported from your web browser, and produces a certificate file and private key file as output. The key and the certificate are output in a format that Makesis can use.

Note: that at this stage the private key file is unencrypted so keep it secure.

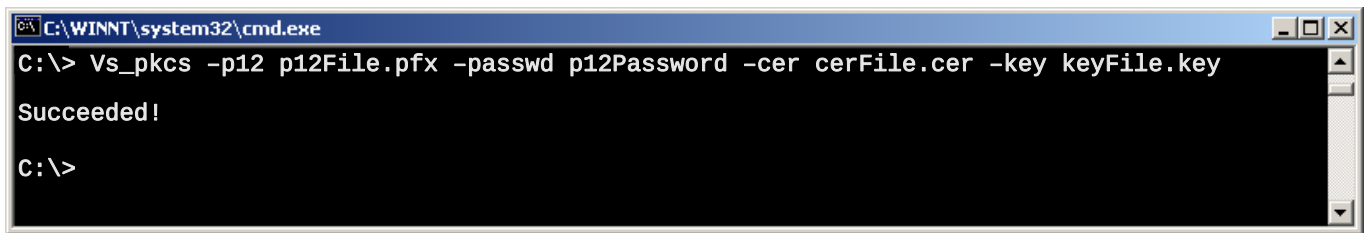
Installation

To install, copy the vs_pkcs executable file to the folder containing the .pfx file.

Usage

Run the vs_pkcs.exe utility on the exported .pfx file from your web browser or command line. The usage is

```
Usage: vs_pkcs -p12 p12File [-passwd p12Password] [-key keyFile] [-cer certFile]
'p12File' is the PKCS#12 file that contains the private key and certificate
'p12Password' is the optional password for the PKCS#12 file
'keyFile' is the private key file, if no name is specified a file with '.key' extension is created
'certFile' is the certificate file, if no name is specified a file with '.cer' extension is created
```



```
C:\WINNT\system32\cmd.exe
C:\> Vs_pkcs -p12 p12File.pfx -passwd p12Password -cer cerFile.cer -key keyFile.key
Succeeded!
C:\>
```

You should now have both the private and public keys (for example) private.key and public.cer respectively.

ACS Publisher ID signing

Copy the private key (private.key) and public certificate (public.cer) files to the same directory as your .PKG file, then add the following line to the .PKG file on the code lines above specifying files to be copied onto the device:

```
"Private.key", "Public.cer", KEY="****"
```

where **** is the password for the private key. If the private key is not password protected you would add the line:

```
"Private.key", "Public.cer"
```

See below for a UIQ example .PKG file, where the appropriate code lines have been added:

```
;Languages
&EN, FR

;Header and app name, KExample UID - 0xdeadbeef
#{ "Example-EN", "Example-FR"}, (0xdeadbeef), 1, 2, 3, IU, SH

;Supported Platform Definitions
(0x101F617B), 2, 0, 0, { "UIQ20ProductID", "UIQ20ProductID" }

;Signing files (and password if applicable)
"Private.key", "Public.cer", KEY="****"

;And finally, the files to install
"\symbian\UIQ_70\epoc32\release\thumb\urel\tExample.exe" -"!:\System\tExample.exe"
"\symbian\UIQ_70\epoc32\release\thumb\urel\tExampleData.dat" -"!:\System\tExampleData.dat"
```

Execute MakeSIS as usual to create your .SIS file and you should now have a .SIS file that is signed and ready to be submitted for testing.

Note: For more information on MakeSIS and the package file syntax for signing consult the MakeSIS documentation with your current Symbian OS SDK.

Step 3 – Submit your application for testing

Registration

Before you submit an application, you must register with Symbian Signed. When you submit applications in future (or re-submit applications) simply log in with your existing details. To register for the first time see instructions below.

1. Visit the Symbian Signed website on www.symbiansigned.com.
2. Here you will find the extensive FAQ, test criteria and information on the available Test Houses (simply select the appropriate link on the left hand side).
3. To register, click the [‘Register’](#) link.
4. Follow the on-screen prompts and supply the requested information. (Note that the provided information will be used for the Symbian [Applications Catalog](#)).
5. When fully registered, you can proceed to submitting your ACS Publisher ID signed application.

Submitting your application

Following steps will take you through how to submit applications for testing.

1. Visit the Symbian Signed website at www.symbiansigned.com.
2. Log in using the username and password you created when registered.
3. Select ‘Submit New’ on the left hand side of the screen.
4. Select the Test House you require to test your application.
5. Once you have selected a Test House you will be shown your user information. You can add to/edit information for this specific submission if you wish.
6. You must now submit your application details including the application name, a description and which phone(s) it runs on. Note that some multiple phone choices are prevented (e.g. you cannot select the Sony Ericsson P800 and Nokia 6600 because they are based on different platforms and require different .SIS files)
7. Finally, you must submit the actual application itself and supporting materials. See ‘What to submit’ for more details.

What to submit in the .ZIP file

The following files/documents are required to be in the .ZIP file you submit.

- **Your .SIS file (signed with your ACS Publisher ID).** This will be installed, the application inside tested and, if successful, the .SIS file will be re-signed with a unique application certificate and returned to you for distribution
- **The .PKG file used to create that .SIS file.** This will be cross-referenced by the Test House to ensure correct target platform and specification.
- **A completed Readme.txt or a user guide in PDF format.** This should include any release notes and quick advice on how to use the application (OR a separate user guide should be included within the .ZIP file in its own right).

Note: If in any doubt compare the .ZIP you are about to submit with the **Sample.zip** file available on the Pre-Test tools section of the website.

Important to check before submitting your application

It is in your interests to ensure everything you submit is likely to pass the testing process. The aim of this process is to minimize the back-and-forth discussions between developer and Test House. Not only will this speed up your time-to-market with a correctly signed .SIS file, but it will also help keep your costs to a minimum. Therefore be sure that you have completed the following steps.

and the testing process will be repeated. Pricing information for re-tests is available under the Test House information section. This cycle will be re-iterated until your application passes all tests.

When the application has passed the tests

Once your application has successfully passed all of the tests conducted by the Test House, the Test House will upload your application to VeriSign, the Certificate Authority. VeriSign will remove the ACS Publisher ID, store details of the application in a revocation database², resign the application against the Symbian root certificate, and send the signed application back to the Test House. The Test House will inform you that you are able to download your Symbian Signed application from the site.

Applications catalog

The applications catalog offers a powerful mechanism for getting your application seen by distributors and network operators. The test criteria used for Symbian Signed have been defined by the industry, so distributors can be confident that Symbian Signed applications are ready for distribution. We therefore expect that Symbian Signed applications will receive preferential treatment compared to unsigned applications.

The catalog itself provides a convenient information repository for Signed applications, raising the profile of those that have successfully passed the testing. The catalog is only accessible to distributors of 3rd party applications and hides any application files. Those that use the catalog must first sign an agreement with Symbian, ensuring that your data will not be misused. Presented with correct and descriptive information about your applications, Catalog users are more likely to contact you. This can in turn lead to a larger addressable market and ultimately increased revenue.

Note: *that the catalog includes your contact details and details about your application but does not include the application itself.*

Once your application has been Symbian Signed, if you indicated that you wanted your application details included in the applications catalog (by using the default “ticked” in the application submission form), it will now appear in the catalog. You can opt in or out of the catalog at any time, though we recommend that most ISVs include their applications.

Note: *Only fully signed applications will be displayed in the catalog.*

Where to get help

If you have any questions about the Symbian Signed, the process involved or what is required of you in order to receive a properly signed application, contact symbiansigned@symbian.com

Disclaimer

The information contained in this document is for general information purposes only and should not be used or relied on for any other purpose whatsoever. While Symbian has taken great care in the preparation of this document, Symbian makes no warranty or guarantee about the suitability or accuracy of the information contained in this document.

² By storing the application details in a revocation database, if the application is malicious it is possible to use VeriSign’s infrastructure to revoke the application from the phones on which it is installed. Revocation is considered a last resort. There would be extensive discussion with the ISV before this drastic measure would be taken.

Appendix

ACS Publisher IDs and China

You may find the following information useful if you are based in China and need an ACS Publisher ID.

1. Go to www.verisign.com to register.
2. Note down the order number and common name as you will need this later.
3. Go to VeriSign's online status page at <http://www.verisign.com/status/> to check the status of your order.
4. Enter the order number and select to pay by wire transfer. Note the information below for your transfer.
 - Beneficiary Customer: VeriSign, Inc.
 - Beneficiary Bank: Northern Trust
 - Bank Address: 50 South LaSalle Street Chicago IL 60675 USA Beneficiary Bank ABA #: 071000152
Customer Account #: 98175 Swift Code: CNORUS44
5. Proof of organisation information should be composed as follows:
 - Fax the acceptable Proof of Right (POR) documentation in English.
 - Articles of Incorporation (English). Please translate the first page and the last page into English.
 - Business License (English). Please translate the document using an accredited translation service.
 - Company charter Documents (English).
 - Partnership Papers (English).
6. In order to verify who you are, you must send your current telephone bill with the right notary letter to Verisign.

Please note that it is highly recommended that you maintain contact and drive the process with Verisign to obtain your ACS Publisher ID.