

# **SetupBuilder™**

## **Code-Signing**

© 2009 Jane Fleming

# Table of Contents

<b>Part I Introduction</b>	<b>3</b>
<b>Part II FAQ</b>	<b>3</b>
<b>Part III Buying A Certificate - The Lindersoft "Deal"</b>	<b>3</b>
<b>Part IV Getting the Tools</b>	<b>9</b>
1 Downloading the ISO.....	9
2 Extracting What You Need.....	10
3 Making Your PFX.....	14
<b>Part V Setting Up SetupBuilder</b>	<b>16</b>
<b>Part VI Code-Signing Your Installer</b>	<b>17</b>
<b>Part VII Code-Signing Your Application Files</b>	<b>18</b>

# 1 Introduction

This is material to supplement the presentation I gave on ClarionLive.com in May, 2009.

I'm not going to explain the "whys" of code-signing or manifests in this short article, but I'd like to go over briefly some of the items I touched on in the presentation.

While I used the latest beta version of SetupBuilder 7 for the presentation, the screen shots here are done with the current public version 6.9.

This document is Copyright © 2009 by Jane Fleming, [Beach Bunny Software](#).  
It may be freely distributed as long as it is distributed in its entirety and this notice is not removed.

Revised Saturday, May 30, 2009

# 2 FAQ

Verrrry briefly...

1. [I'm just getting my feet wet, so shouldn't I buy a 1-year certificate?](#) Dealing with the certificate purchase process has given more than a few people more than a few grey hairs. I really recommend buying a 3-year certificate.
2. [How many files can I sign with my certificate?](#) You can sign as many as you want. You can sign code created for you by contractors. Just bear in mind that you're putting your name as a guarantor on whatever you sign.
3. [On what operating systems can I code-sign?](#) I've signed projects using development machines running XP, Vista (32-bit and 64-bit) and Windows 7. You need to use an XP computer and Internet Explorer to go through the certificate purchase process. After that, you can copy your certificate files to any computer you wish.

# 3 Buying A Certificate - The Lindersoft "Deal"

If you look at the price of code-signing certificates, you wouldn't be the first person to joke that this whole thing looks like a money tree for the certification companies. Their prices for signing certificates have doubled or tripled since Vista went into public release.

We're fortunate that Lindersoft has negotiated a special deal with one of the Certification Authorities - Comodo. Current pricing and ordering information is available through [the Lindersoft website](#). As of this writing, a three-year certificate costs USD \$200. You may say, "ouch", but check out the alternatives - a three-year certificate from [VeriSign](#) is going for USD \$995 or direct through [Comodo](#) for USD \$500.

You can sign as many files as you want to while your certificate is valid.

Here are some suggestions for buying your certificate through Lindersoft.

- If you have ever bought a certificate from Comodo before, do not use that account or that email address to buy your new certificate - create and use a new email address.
- Gather the documentation you'll need to prove your identity. When I bought my certificate in 2008, the requirements were any TWO of:
  - Articles of Incorporation (with address)
  - Government Issued Business License (with address)
  - Copy of a recent company bank statement (you may blacken out the Account Number)
  - Copy of a recent company phone bill
  - Copy of a recent major utility bill of the company (i.e. power bill, water bill, etc.) or current lease agreement for the company
- USE AN XP COMPUTER. DO NOT USE A VISTA COMPUTER! Be sure you will have access to THIS computer in a few days when your certificate is ready for pickup.
- USE INTERNET EXPLORER. DO NOT USE A DIFFERENT BROWSER!


**IMPORTANT:** Once you have collected your certificate, you will be able to do code-signing on any computer. But you will need to collect it **on the same XP computer** you use to purchase it.

Click the Order link on the Lindersoft website.

Enter your user name and password. NOTE: If you paste the user name from the Lindersoft email, Windows may add an extra space at the end. Be sure you don't have any extra space(s) after your user name.

If you're asked for permission to install a certificate enrollment application, say Yes.

Be sure you specify to get your certificate in a file, so you can easily move it to different computers as needed.



Please do not use your browser's BACK and FORWARD buttons

**Code Signing Certificate 3 years**  
This webpage will work in most major browsers including Internet Explorer.

Be sure you select 3 years. You don't want this hassle every year.

Step 1: Product Details

**Certificate Details**

Select the validity period for your Certificate:

☐ 1 year  
☐ 2 years Save 9%  
☒ 3 years **Highly recommended** Save 16%

(Optional) Enter the Contact Email Address to appear in your Certificate:

Total Cost:

**\$200.00**

Be sure you save your certificate as a **FILE**. Accept the default 2048 key size.

**Advanced Private Key Options**

CSP

Microsoft Enhanced Cryptographic Provider v1.0

Key Filename

☐ In the CSP? ☒ In the file:

Key Size

Exportable?

☒

User protected?

☐

**NOTE:** After completing this signup process, we strongly advise you to backup your Private Key, because your Certificate is useless without it!

**Key Generation**

When you click the button below, you will see one or more "Potential Scripting Violation" popups. Click "Yes" to each one.

**NOTE:** If you are saving your Private Key to a .PVK file, you will also be asked to enter a "Private Key Password". It is vital that you remember this Password, because your Private Key cannot be used without it!

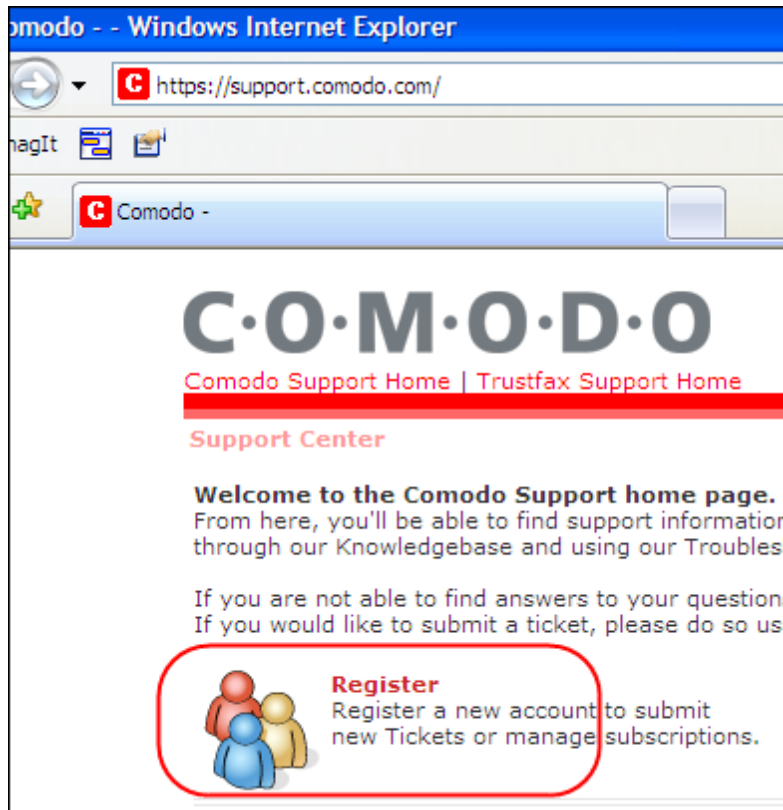
Next >

Proceed through the rest of the sales screens.

A short while after you place your order, you should get a confirmation from Comodo requesting your documentation.

Although some of the emails say you can email the documentation, you can't. They require it to be FAXed or attached to a support ticket.

To submit a support ticket, first go to the [Comodo support website](https://support.comodo.com/) and register.



After you've registered, log in with your new user name. Create a support ticket and attach the documents.

# C·O·M·O·D·O

[Comodo Support Home](#) | [Trustfax Support Home](#)

[Support Center](#) » [Ticket List](#) » [SSP-123456](#)

> required documentation attached

**Ticket Details**

Ticket ID:	SSP-123456	Department:	Validation Escalated
Status:	Closed	Priority:	Critical
Created On:	17 Aug 2008 03:34 AM	Last Update:	17 Aug 2008 05:00 AM

**Order Information**

Order Number OR Domain Name: \*

**Problem Description**

Brief problem description: I have ordered my certificate, but not yet received it

Update

Post Reply

**Conversation**


**Jane Fleming**


USER

Posted On: 17 Aug 2008 03:34 AM

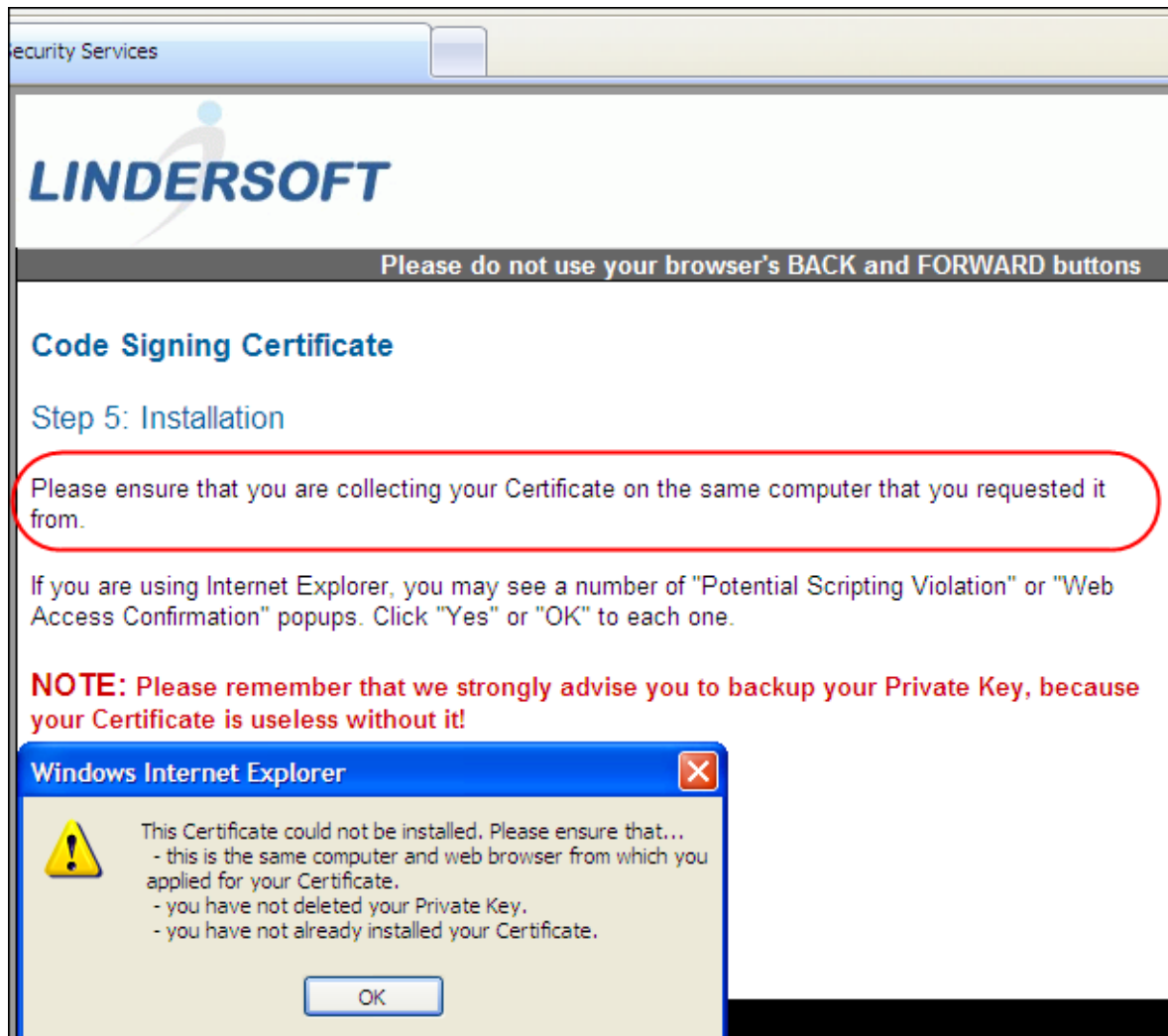
Copies of city business license and bank statement attached.

**Attachments**

 [BeachBunnySoftware.jpg](#) (218.30 KB)

 [BeachBunnySoftwarebank.jpg](#) (325.47 KB)

Once you're notified that your certificate is available, be sure to use the **same XP computer** to collect it. Otherwise, you'll get an error.



Once you have collected your certificate files, make copies, burn at least one copy onto a CD, and safeguard both the certificate files and your password that you created when you ordered the certificate. You won't be able to sign your files without the password.

At this point, you can use your certificate files on any Windows computer and no longer need to stick with the XP machine you used for the ordering process.



## 4 Getting the Tools

Unfortunately, Microsoft doesn't allow third-party vendors to distribute the current code-signing tools. SetupBuilder™ comes with Microsoft's old SignCode.exe tool installed, but SignCode.exe has some issues and may pop up a window that grabs focus when you're in the middle of doing something else.

SignTool.exe is the new code-signing tool. It and the pvk2pfx.exe tool that you'll also need are available as part of the (free) downloadable SDK from the Microsoft website.

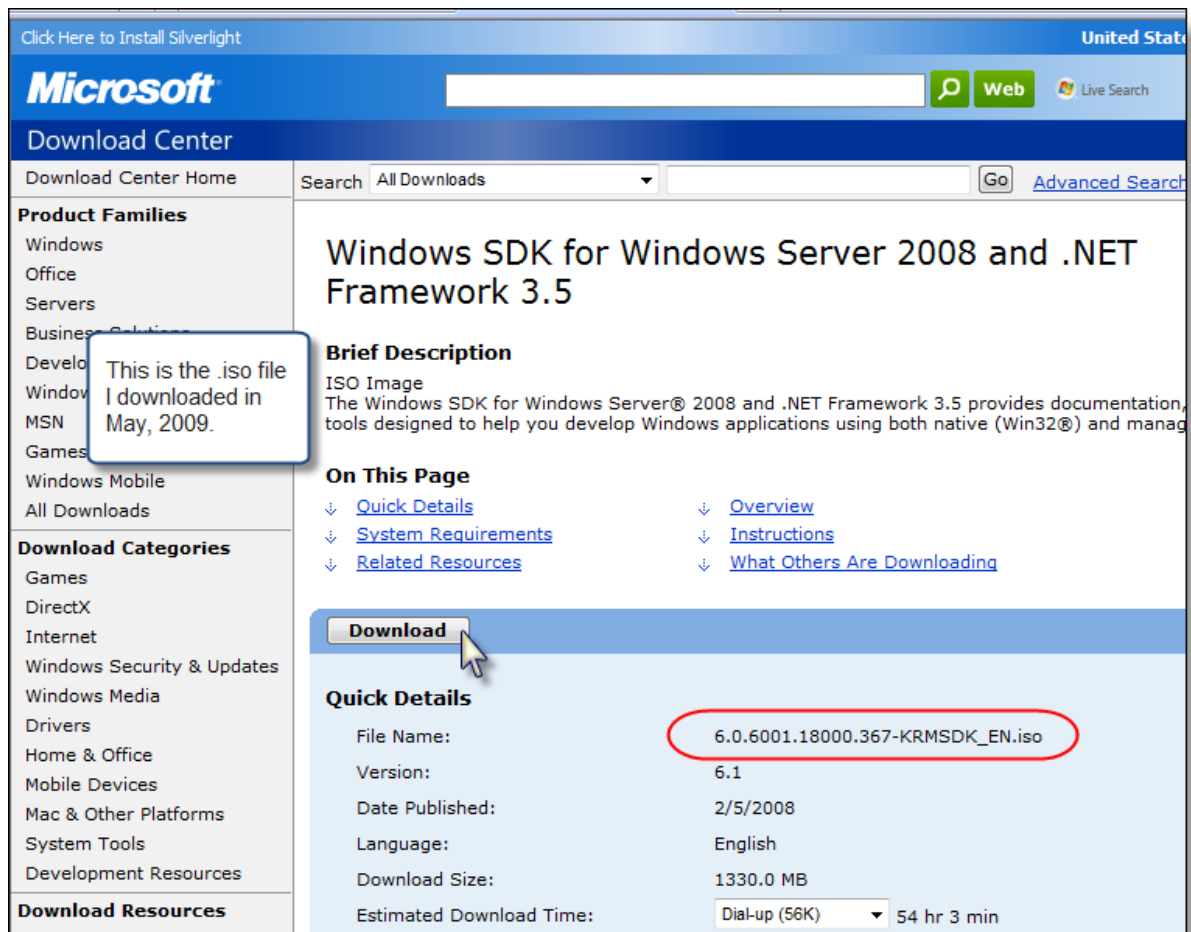
There are probably other ways to go about this, but what I'm going to illustrate involves

1. Downloading the SDK .ISO file from Microsoft (You could use this file to burn a DVD if you wanted)
2. Using WinRAR to extract the few needed files from the .ISO file
3. Creating a .PFX file to use with SetupBuilder™

### 4.1 Downloading the ISO

Search for the current SDK (Software Development Kit) on the Microsoft website.

As of May, 2009, the current version is [available at this link](#).



## 4.2 Extracting What You Need

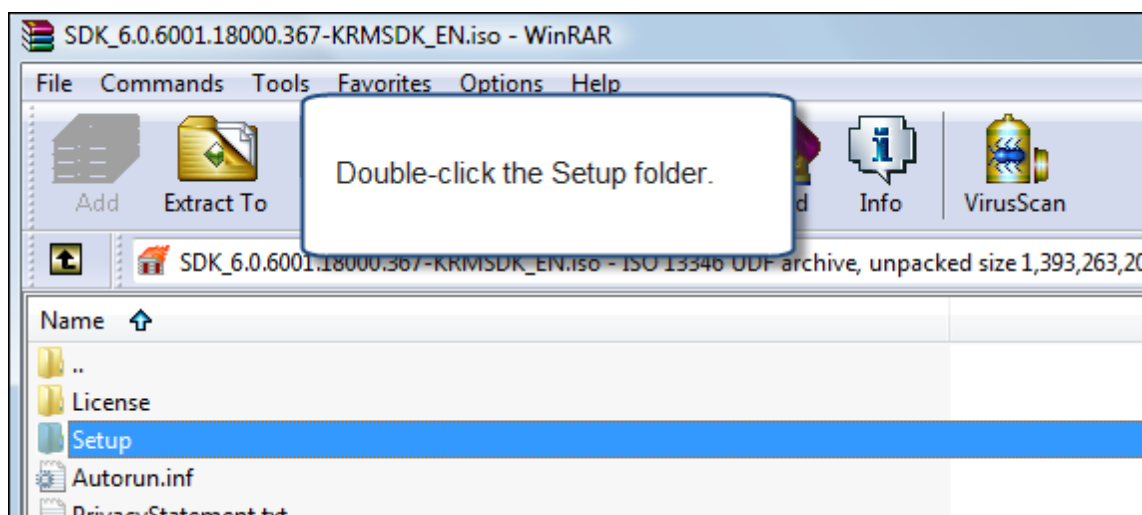
Depending on your operating system, you may or may not need the capicom.dll.

I'm going to suggest extracting it regardless, and either putting it into the folder with your code-signing tools or into C:\Windows\System32.

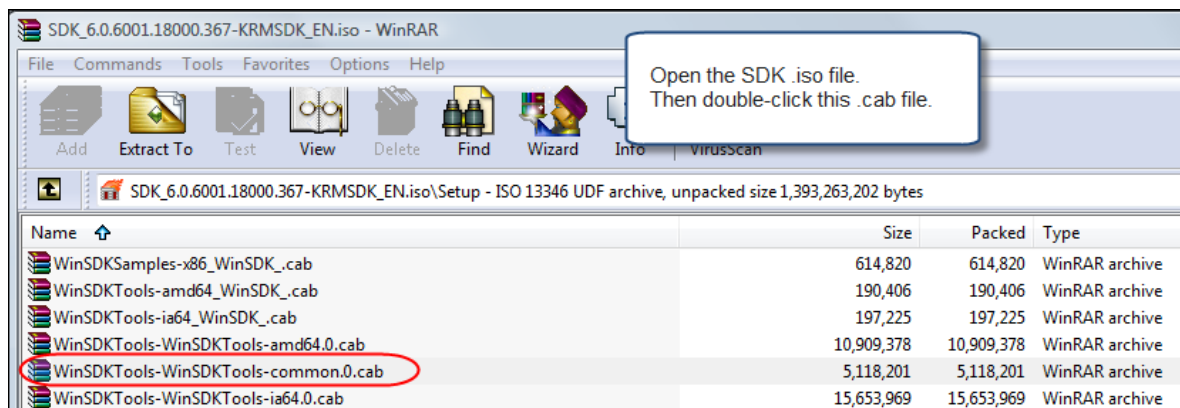
Because what you've downloaded is an ISO file, you could burn it to DVD, run the installation program, opt just to install tools, copy them elsewhere, and then delete the rest of the package.

What I'll show is using WinRAR to open the ISO and cherry-pick the few files you'll want. You could use some other ISO tool as well, of course.

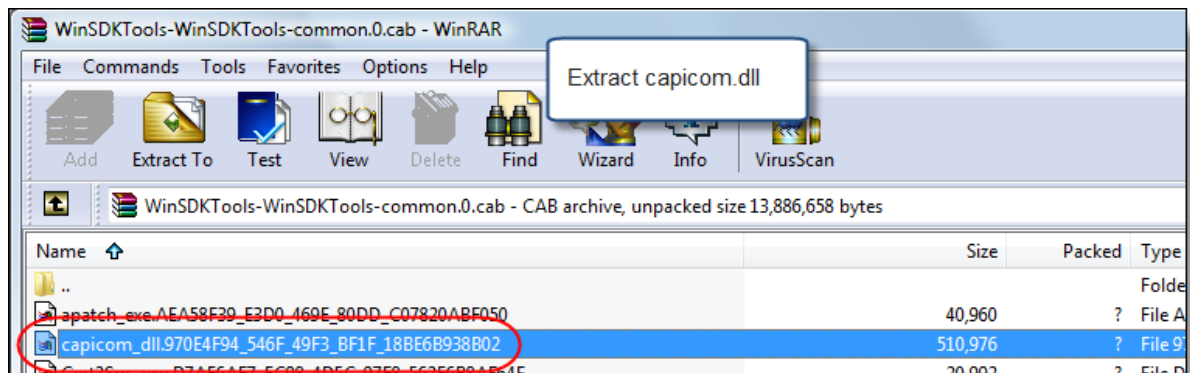
First, open the ISO you downloaded. Then open the **Setup** folder.



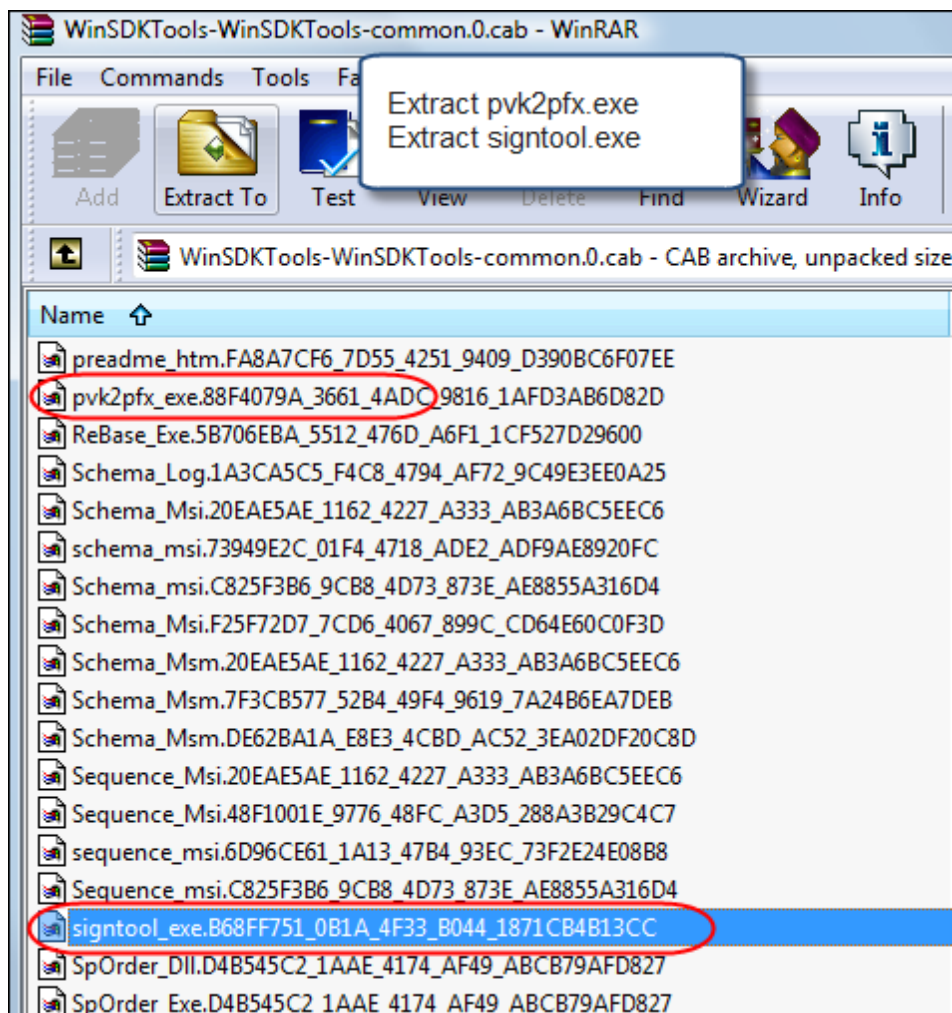
Within the **Setup** folder, double-click the .cab file shown.



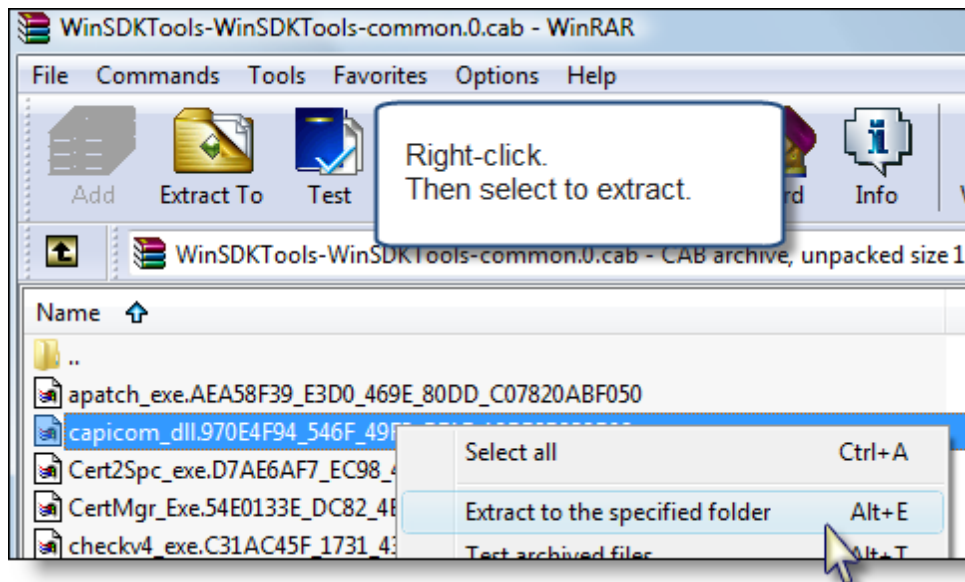
You're going to extract the capicom.dll file.



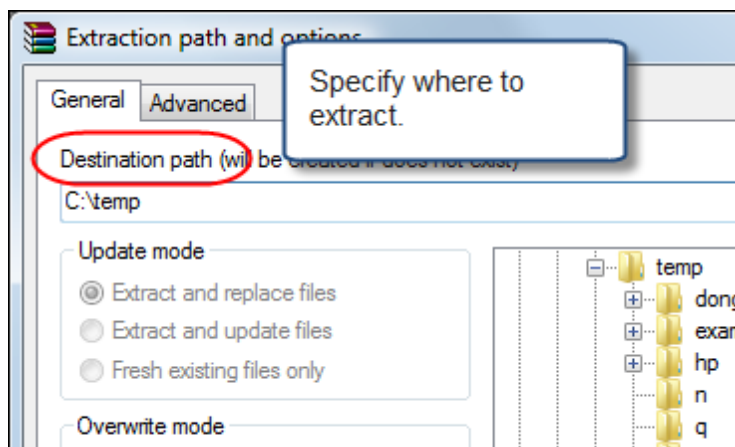
And also signtool.exe and pvk2pfx.exe



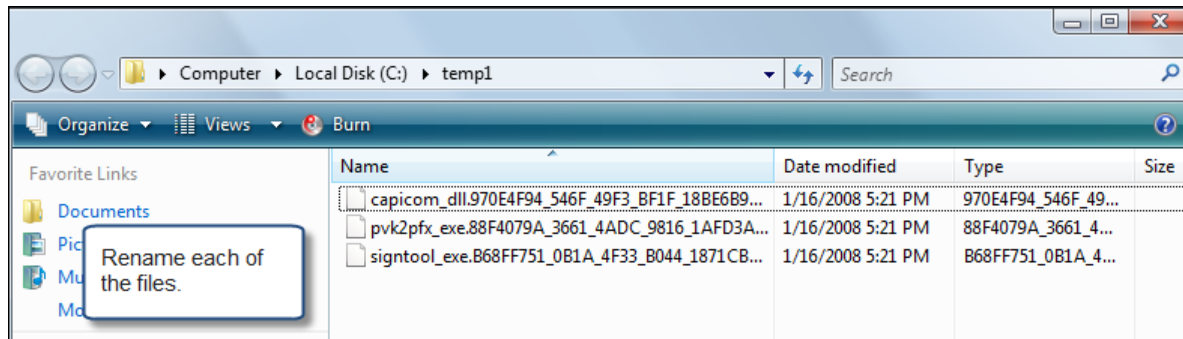
For each file, right-click and choose to extract.



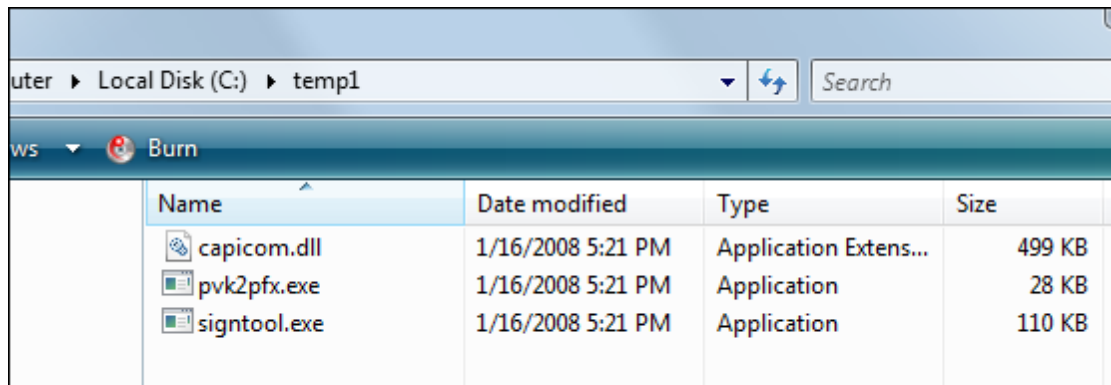
Select a place on your hard drive to stash the files.



Once they're extracted, you need to change the funky names to the real names.



Done!



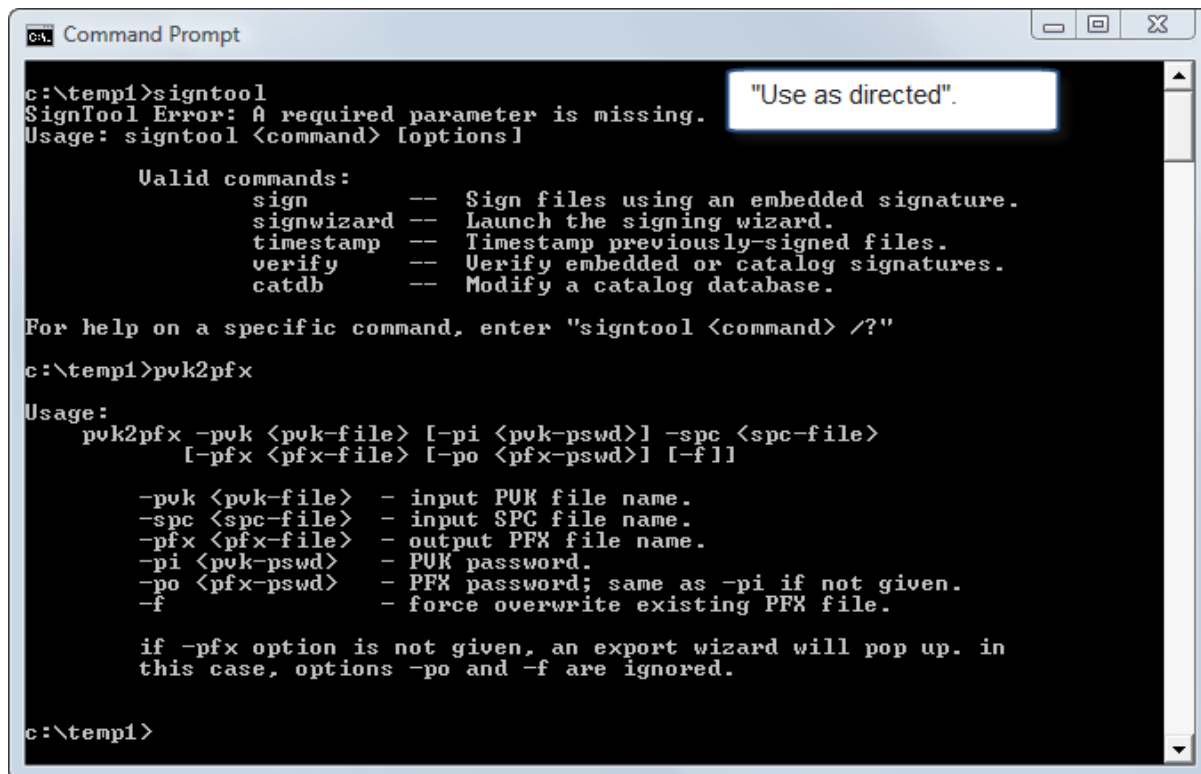
## 4.3 Making Your PFX

The files you've downloaded have a number of command-line options.

While `signtool.exe` can be used with a GUI, you need to use the **signwizard** command-line switch to invoke it.

You won't need any of that complexity once you have SetupBuilder™ set up properly, though.

Just running each of the two tools at the prompt shows the basics of their options. Signtool also has more detailed help as mentioned in the screen shot.



```
Command Prompt

c:\temp1>signtool
SignTool Error: A required parameter is missing.
Usage: signtool <command> [options]

Valid commands:
    sign          -- Sign files using an embedded signature.
    signwizard    -- Launch the signing wizard.
    timestamp     -- Timestamp previously-signed files.
    verify        -- Verify embedded or catalog signatures.
    catdb         -- Modify a catalog database.

For help on a specific command, enter "signtool <command> /?"

c:\temp1>pvk2pfx
Usage:
    pvk2pfx -pvk <pvk-file> [-pi <pvk-pswd>] -spc <spc-file>
               [-pfx <pfx-file> [-po <pfx-pswd>] [-f]]

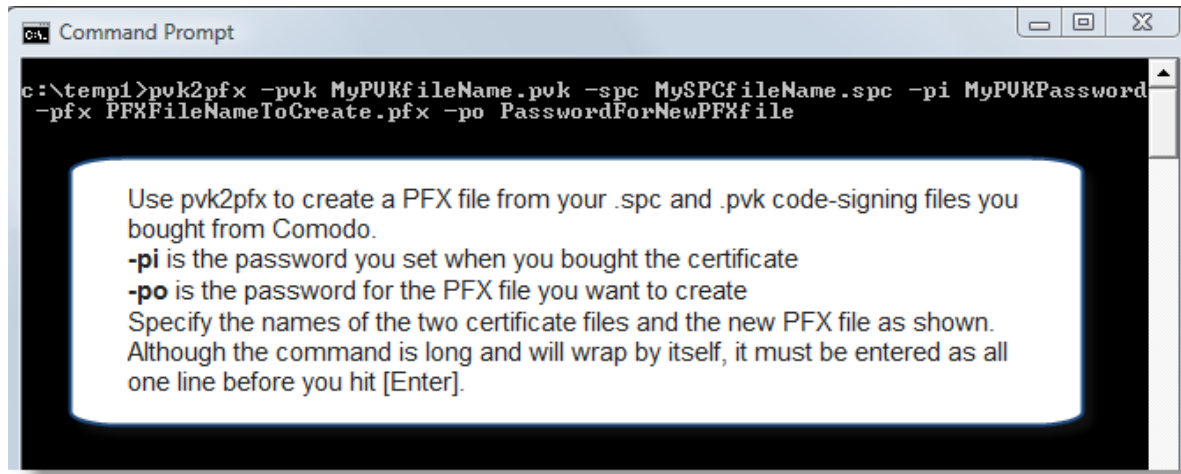
    -pvk <pvk-file>  - input PUK file name.
    -spc <spc-file>  - input SPC file name.
    -pfx <pfx-file>  - output PFX file name.
    -pi <pvk-pswd>   - PUK password.
    -po <pfx-pswd>   - PFX password; same as -pi if not given.
    -f              - force overwrite existing PFX file.

    if -pfx option is not given, an export wizard will pop up. in
    this case, options -po and -f are ignored.

c:\temp1>
```

"Use as directed".

To create your .PFX file, I'd suggest copying your certificate files (something.spc and something.pvk) into the same folder where you have pvk2pfx.exe installed. Then run the command as shown.

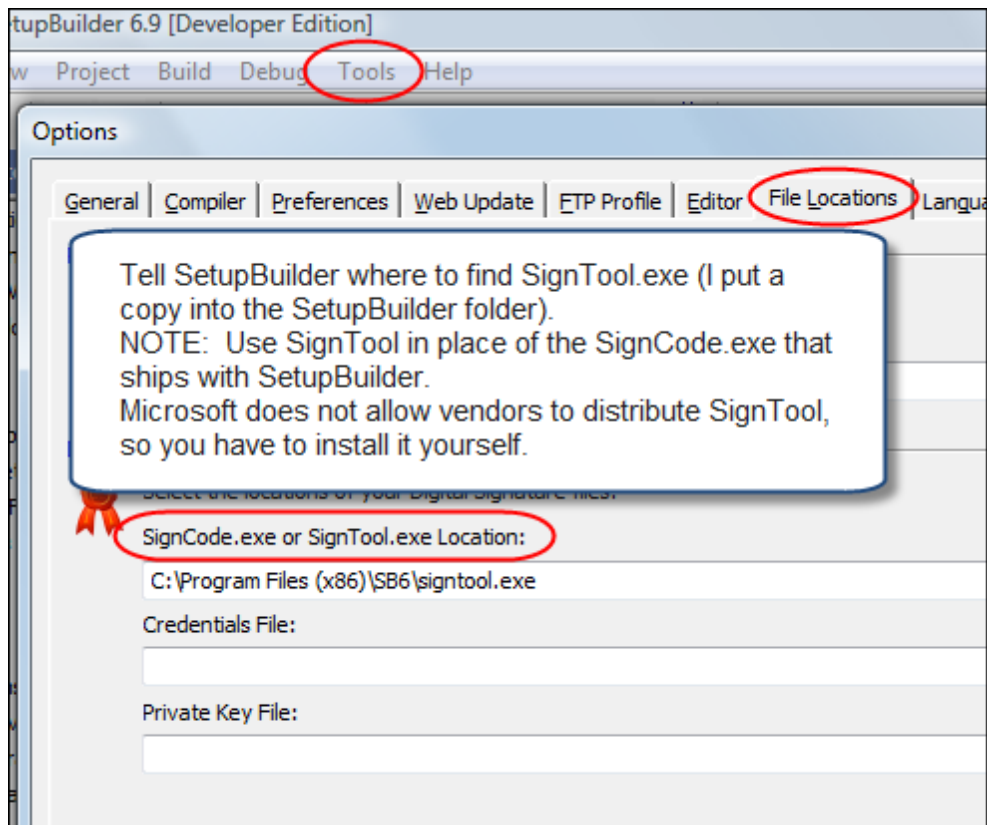


Here's a string you can copy and paste to get you started.

```
pvk2pfx -pvk mykey.pvk -pi janepassword -po mynewpass -spc mycert.spc -pfx Jane.pfx
```

## 5 Setting Up SetupBuilder

You'll need to tell SetupBuilder™ to use SignTool.exe instead of the SignCode.exe file that ships with it. Click on **Tools**, then **Options**, then select the **File Locations** tab and browse to the folder containing SignTool.exe



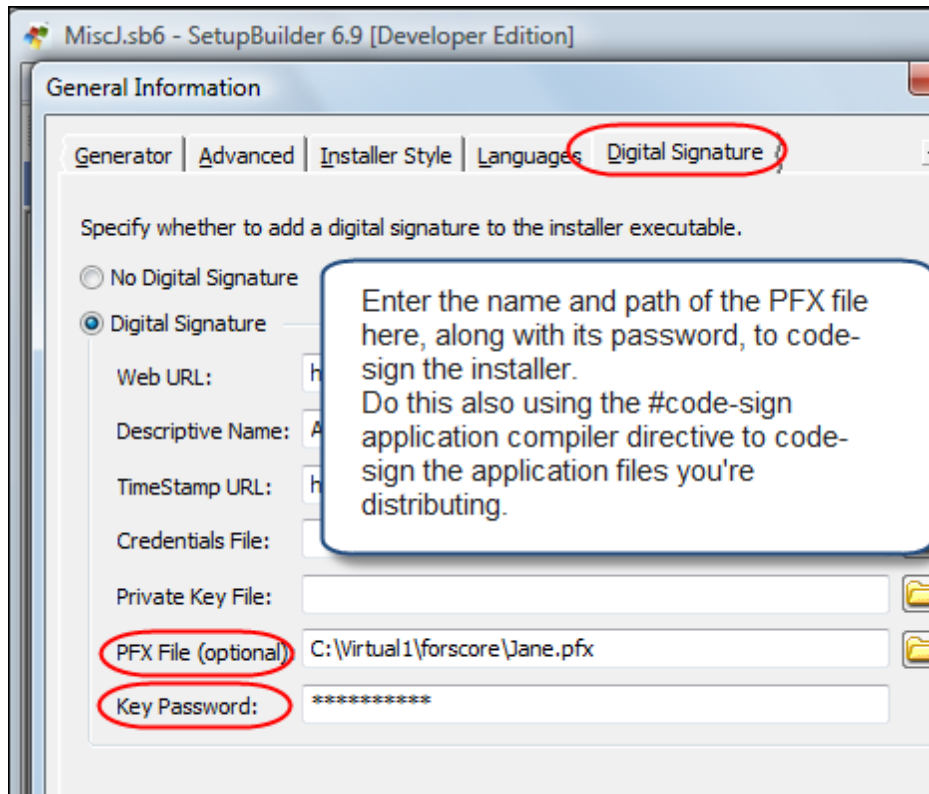


## 6 Code-Signing Your Installer

To code-sign your installer, click **Project**, then **Settings**, then scroll right until you get to the **Digital Signature** tab.

Enter the path to the PFX file and its password. Also fill in your web address and descriptive name as you want Windows to display it to your customers. And enter the URL for one of the code-signing timestamp servers. (See the SetupBuilder™ documentation for more information.)

Because you're using SignTool.exe and a PFX file, you don't need to enter anything in the **Credentials File** or **Private Key File** fields.

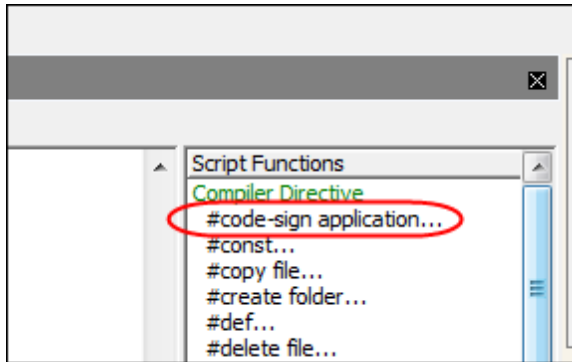


## 7 Code-Signing Your Application Files

The actual application file(s) that you distribute should be code-signed. I sign both EXE and DLL files.

You want to code-sign your file(s) after you have embedded a manifest, because the code-signing guarantees that the file hasn't been altered and inserting a manifest is definitely an alteration.

Use the **#code-sign application** Compiler Directive.



If you want your application file on your hard drive (not the copy compiled into the installer) to remain code-signed after the installer has been compiled, mark the **Permanent** check box. Otherwise, SetupBuilder™ will stash a copy of your original .EXE file, code-sign the file, compile the code-signed file into the installer, then restore the unsigned EXE to the folder on your hard drive.

