## SetupBuilder™ Code-Signing

© 2009 Jane Fleming

# **Table of Contents**

2

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

## 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, <u>Beach Bunny Software</u>. 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 <u>the Lindersoft website</u>. 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 <u>VeriSign</u> is going for USD \$995 or direct through <u>Comodo</u> for USD \$500.

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

4

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.

LINDERSOFT						
	Please do not use your browser's BACK and FORWARD butt					
Code Signing Certificate 3 years This webpage will work in most major bro Explorer. Stop 1: Product Dotails						
Certificate Details	_					
Select the validity period for your Certificate:	0 1 year 0 2 years 0 3 years	Save 9% Highly recommended Save 16%				
(Optional) Enter the Contact Email Address to appear in your Certificate:	anef@beachbunnysoftware.cc					
Total Cost: \$200.00 Be sure you save your certificate as a FILE. Accept the default 2048 key size.						
CSP	Microsoft Enhand	ed Cryptographic Provider v1.0 🗸				
Key Filename	O In the CSP	⊙ In the file: C:\mykey.pvk				
Key Size	2048 💌					
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" popup Click "Yes" to each one.						
<b>NOTE:</b> If you are saving your Private Key to a .PVK file, you will also be asked to ente 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 <u>Comodo support website</u> and register.

modo Windows Internet Explorer
C https://support.comodo.com/
agIt 🔁 🛃
C Comodo -
COMON Comodo Support Home   Trustfax Support Home
Support Center
Welcome to the Comodo Support home page. From here, you'll be able to find support information through our Knowledgebase and using our Troubles!
If you are not able to find answers to your questions If you would like to submit a ticket, please do so usi
Register Register a new account to submit new Tickets or manage subscriptions.

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

Ϲ·Ο·Ϻ·Ο·Ͻ·Ο					
Comodo Suppor	t Home   Trust	fax Support Home			
Support Cente	r » Ticket Lis	st » SSP-			
> required do	cumentation	attached			
Tieles Basell					
Ticket ID:	SSP-		Department:	Validation Escalated	ł
Status:	Closed		Priority:	Critical	-
Created On:	17 Aug 2008	03:34 AM	Last Update:	17 Aug 2008 05:00	AM
					-
Order Inform Order Number Name: *	oation OR Domain	10000			
Problem Des Brief problem	Problem Description Brief problem description: I have ordered my certificate, but not yet received it				
Conversation					
Jane Flem	ing				USER
Posted On:	: 17 Aug 2008	03:34 AM			
Copies of city	business lice	nse and bank sta	atement attache	ed.	
Attachments BeachBun BeachBun	nySoftware.jpg nySoftwareban	(218.30 KB) k.jpg (325.47 KB)			

7

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.

ecurity Services				
LINDERSOFT				
Please do not use your browser's BACK and FORWARD buttons				
Code Signing Certificate				
Step 5: Installation				
Please ensure that you are collecting your Certificate on the same computer that you requested it from.				
If you are using Internet Explorer, you may see a number of "Potential Scripting Violation" or "Web Access Confirmation" popups. Click "Yes" or "OK" to each one.				
NOTE: Please remember that we strongly advise you to backup your Private Key, because your Certificate is useless without it!				
Windows Internet Explorer				
This Certificate could not be installed. Please ensure that - this is the same computer and web browser from which you applied for your Certificate. - you have not deleted your Private Key. - you have not already installed your Certificate. OK				

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<sup>™</sup> 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 <u>available at this link</u>.

Click Here to Install Silverlight United S				
Microsoft <sup>®</sup>		🔎 Web 🖉 Live Search		
Download Center				
Download Center Home	Search All Downloads 🔹	Go Advanced Search		
Product Families Windows Office	Windows SDK for Wind	ows Server 2008 and .NET		
Servers Busines O-Luison Develo Windov MSN Games Windows Mobile	Framework 3.5 Brief Description ISO Image The Windows SDK for Windows Server® 2 tools designed to help you develop Window On This Page	008 and .NET Framework 3.5 provides documentation, vs applications using both native (Win32®) and manag		
All Downloads Download Categories Games	<u>Ource Details</u> <u>System Requirements</u> <u>Related Resources</u>	<u>Overview</u> <u>Instructions</u> <u>What Others Are Downloading</u>		
DirectX Internet Windows Security & Updates Windows Media	Download Quick Details			
Drivers Home & Office Mobile Devices Mac & Other Platforms System Tools Development Resources	File Name: Version: Date Published: Language: Download Size:	6.0.6001.18000.367-KRMSDK_EN.iso 6.1 2/5/2008 English 1330.0 MB		
Download Resources	Estimated Download Time:	Dial-up (56K) 🔻 54 hr 3 min		

#### 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.

E SDK_6.0.6001.18000.367-KRMSDK_EN.iso - WinRAR						
File Commands Tool	File Commands Tools Favorites Options Help					
Add       Extract To         Double-click the Setup folder.       Info         Image: SDK_6.0.6001.18000.307-KKIMSDK_EIN.ISO - ISO 13340 UDF archive, unpacked size 1,393,263,20						
Name 🏠						
🚇						
License						
Setup						
Autorun.inf						
DrivacyStatement tyt						

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

E SDK_6.0.6001.18000.367-KRMSDK_EN.iso - WinRAR						
File Commands Tools Favorites Options Help	Open the SDK .iso file.					
	Then double-click this .cab file	e. 🕴				
Add Extract To Test View Delete Find Wizard In	ito Virusscan					
SDK_6.0.6001.18000.367-KRMSDK_EN.iso\Setup - ISO 13346 UDF ar	chive, unpacked size 1,393,263,202 bytes					
Name 🗘 Size Packed Type						
WinSDKSamples-x86_WinSDKcab	614,820	614,820 WinRAR archive				
WinSDKTools-amd64_WinSDKcab 190,406 WinRAR archive						
WinSDKTools-ia64_WinSDKcab 197,225 WinRAR archive						
WinSDKTools-WinSDKTools-amd64.0.cab	10,909,378	10,909,378 WinRAR archive				
WinSDKTools-WinSDKTools-common.0.cab	5,118,201	5,118,201 WinRAR archive				
WinSDKTools-WinSDKTools-ia64.0.cab 15,653,969 15,653,969 WinRAR archive						

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

WinSDKTools-WinSDKTools-common.0.cab - WinRAR						
File Commands Tools Favorites Options Help Extract capicom.	dl					
Add Extract To Test View Delete Find Wizard Info	VirusScan					
🗈 📔 WinSDKTools-WinSDKTools-common.0.cab - CAB archive, unpacked siz	🗈 🛯 📚 WinSDKTools-WinSDKTools-common.0.cab - CAB archive, unpacked size 13,886,658 bytes					
Name 🗘	Size	Packed T	Туре			
🔒		F	olde			
apatch_exe.AEA58F39_E3D0_469E_80DD_C07820ABF050	40,960	? F	File A			
capicom_dll.970E4F94_546F_49F3_BF1F_18BE6B938B02	510,976		File 9			
Carloson and DTAFGAFT FC08 ADSC 07F8 562F688AP6AF	20.992	2 F	ile D			

And also signtool.exe and pfk2pfx.exe



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

WinSDKTools-WinSDKTools-common.0.cab - WinRAR					
File Commands Tools Favorite	es Options Help				
Add Extract To Test	Right-click. Then select to extract.	Info V			
🗈 🗎 WinSDKTools-WinSDK	lools-common.0.cab - CAB archive,	unpacked size 1			
Name 🔂					
🎴					
apatch_exe.AEA58F39_E3D0_469E_80DD_C07820ABF050					
capicom_dll.970E4F94_546F_49F Cert2Spc_exe.D7AE6AF7_EC98_4	Select all	Ctrl+A			
GertMgr_Exe.54E0133E_DC82_48	Extract to the specified folder	Alt+E			
checkv4_exe.C31AC45F_1731_4	Test archived files	UI+_T			

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

General Advanced Specify where to extract.				
C:\temp				
Update mode Extract and replace files Extract and update files Fresh existing files only		temp ⊕ dong ⊕ exam ⊕ hp n		
Overwrite mode		- q		

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

				X
Computer + Loc	al Disk (C:) 🕨 temp1 🗸	Search		م
🄄 Organize 👻 🏢 Views 👻 🚷	Burn	_		0
Favorite Links	Name	Date modified	Туре	Size
Documents	capicom_dll.970E4F94_546F_49F3_BF1F_18BE6B9	1/16/2008 5:21 PM	970E4F94_546F_49	
Pic	pvk2pfx_exe.88F4079A_3661_4ADC_9816_1AFD3A	1/16/2008 5:21 PM	88F4079A_3661_4	
Rename each of the files.	signtool_exe.B68FF751_0B1A_4F33_B044_1871CB	1/16/2008 5:21 PM	B68FF751_0B1A_4	

Done!

uter 🕨 Local Disk (C:) 🕨 temp1 🚽 😽 Search						
ws 🔻 🚯 Burn						
	Name	Date modified	Туре	Size		
	Scapicom.dll pvk2pfx.exe signtool.exe	1/16/2008 5:21 PM 1/16/2008 5:21 PM 1/16/2008 5:21 PM	Application Extens Application Application	499 KB 28 KB 110 KB		

#### 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.



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<sup>™</sup> 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

tupBuilder 6.9 [Developer Edition]					
w Project Build Debug Tools Help					
Options					
General Compiler Preferences Web Update FTP Profile Editor File Locations Langu					
Tell SetupBuilder where to find SignTool.exe (I put a copy into the SetupBuilder folder). NOTE: Use SignTool in place of the SignCode.exe that ships with SetupBuilder. Microsoft does not allow vendors to distribute SignTool, so you have to install it yourself.					
SignCode.exe or SignTool.exe Location:					
C:\Program Files (x86)\SB6\signtool.exe					
Credentials File:					
Private Key File:					

## 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<sup>™</sup> 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.

MiscJ.sb6 - SetupBuilder 6.9 [Developer Edition]					
General Information					
Specify whether to add a digital signature to the installer executable.					
○ No Digital Signature Enter the name.	and path of the PEX file				
Digital Signature     here, along with	its password, to code-				
Web URL: h sign the installer	: a the #code sign				
Descriptive Name: A application com	piler directive to code-				
TimeStamp URL: h sign the applicat distributing.	ion files you're				
Credentials File:					
Private Key File:	<u></u>				
PFX File (optional) C:\Virtual1\forscore\Jane.pfx					
Key Password: ********					

## 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<sup>™</sup> 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.

[ reacures ]						
! If features are enal Decomposition Code size Application						
! Warning: It is not Preprocessor: Code-sign Application						
	File Name:					
[ Setup Types ]	C:\Virtual1\test\MyExe.exe					
! If setup types are	Web URL:					
Embed manifest	http://www.beachbunnysoftware.com	Use the drop list to				
before signing app.	Descriptive Name:	select a time-stamp server, or type in				
::Derine Setup Type	My Test Application	another one.				
	TimeStamp URL:					
#embed UAC manifest i	http://timestamp.comodoca.com/authenticode					
<pre>tcode-sign applicat;</pre>	http://timestamp.comodoca.com/authenticode					
	http://timestamp.verisign.com/scripts/timstamp	p.dll				
[ User Interface ]	· · · · · · · · · · · · · · · · · · ·					
! Wizard dialog defin	d dialog defin Private Key File:					
Define Wizard Dialog						
Define Wizard Dialog Define Wizard Dialog	PFX File (optional):					
I The Wigard Loop die	C:\Virtual1\test\Jane.pfx					
Loop Wizard (Abort Di	Key Password:					
End	*******					
! Display progress di	Skip if file is already code-signed					
Display Setup Progres						
	En emanene					
1 Curren in challening						