SECTIGO (Formerly COMODO) Code-Sign Certificate Adventure – February, 2020

These are just some scattered notes documenting my triennial trauma of purchasing a code-signing certificate. There will be less detail than in similar notes from previous years.

TL;DR bottom line – you will need a phone number they can look up under the name you're using for your certificate. And yes, you really DO need to do this process with Internet Explorer. And you will need to pick up your issued certificate using Internet Explorer ON THE SAME COMPUTER from which you placed the order.

In past years, I had found it advantageous to turn OFF the WHOIS privacy that my domain registrar provides for my website. I did that a few days ago, but WHOIS still didn't show my information. I was too lazy to check with the registrar's tech support to ask why it wasn't visible.

Some years ago, Dun & Bradstreet somehow listed me when I had a business landline. (No doubt they thought I'd buy something from them.) Some fewer years ago, I managed to log in and correct my information to reflect my current home phone number. This was fortunate.

To my surprise, I got an email about two weeks before the expiration of my current certificate from someone from Sectigo inviting me to renew. His boilerplate said they have a new website; my old credentials wouldn't work – I'd need to create new ones.

I, of course, opted to make the purchase using the SetupBuilder credentials that Friedrich provides with subscriptions. The cost through Lindersoft was 40% of what the Sectigo guy quoted me.

In the past, I've tried to think about what time it is in which time zone and to prepare myself mentally for the ordeal. It happened that yesterday, February 1, I looked at the clock, saw it was a bit past 3PM Pacific time on a Saturday, and thought "what the heck." A bit like just jumping into the ice water without long agonizing planning and debate. (Yes... I'd rather go to the dentist...)

I used the link from the SetupBuilder purchase email, selected the 3-year certificate, and used the credentials from the SetupBuilder purchase email on the IE login screen:

Note: Individuals are able to purchase stan than done for companies. See here	dard code signing certificates, but i	t entails the use of
Windows Security		×
iexplore.exe		
The server www.lindersoft.com is password.	asking for your user name and	
That server also reports: "Protect	ed".	
Warning: Your user name and na	ssword will be sent using basic	Sign un
authentication on a connection th	hat isn't secure.	Verif
		Verif
MysetupbuliderLogin	^	Safe
•••••		
		Improv
Remember my credentials		Impro
		Protects
ОК	Cancel	
		- Suppo

You want SHA-2, of course. (I don't know why SHA-1 is still a choice on the dropdown.) I picked a 4096bit private key. You want the private key exportable. "User protected" means you will need to create a password now and then give that password again when you eventually export your certificate. So remember it. The yellow box at the bottom of the screen comes from the More Info link.

This webpage will work with Microsoft Internet Explorer 8+ on Windows and Mozilla Firefox o		
Мас		
This page does not currently w	vork with Google Chrome, Apple Safari or Microsoft Ed	lge.
Step 1: Product 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:	jane.fleming@t	
Select the hash algorithm you would prefer us to use when signing your Certificate:	SHA-2	~
Total Cost:	\$ 200.00	
Advanced Private Key Options		
CSP	Microsoft Enhanced Cryptographic Provider v1.0	~
Key Size	4096	~
Exportable?		
User protected?		
Note: Backup your private key! we do not get a copy of your private key at any time so, after completing this application procedure, we strongly advise you create a backup. Your certificate is useless without it. More info Your private key never leaves this computer and is never transmitted to the certificate issuer. When you click the button below, your bro Your public and private keys are generated by the crypto module on your local machine. The options under "Private Key Options" are to instruct your local software on how to generate your keys. They are not instructions sent to remote servers for remote key generation.		

This is the part (well, part of the part) for which you need IE, with its hooks into Windows to generate your private key. If you've done the above step in Chrome, you'll get an error message. I'll give a little sidebar info on this part (the private key stuff) at the end of this document.

		Account Holders	
fox o	n	If you have previously purchased Lindersoft security solutions please login below BEFORE continuing with this order:	
	Web Aco	ess Confirmation	×
*		This Web site is attempting to perform a digital certificate operation on your behalf: https://secure.comodo.net/products/CodeSigningSignup1 You should only allow known Web sites to perform digital certificate operations on your behalf. Do you want to allow this operation?	a
		Yes No	

I'm just guessing here in choosing "high".

Creating a nev	v RSA exchange key X	e monitored
ftv	An application is creating a Protected item.	nd/or discipl
	CryptoAPI Private Key	
	Security level set to Medium Set Security Level	
Pre	OK Cancel Details	
e	Choose a security level appropriate for this item High Request my permission with a password whitem is to be used. Medium Request my permission when this item is to be 	en this be used.
	< Back Next >	Cancel

You will, obviously, want to remember this password.

ed	Creating a new RSA exchange key X	 Access to 9 e monitored ses. Unauthored
ťv	An application is creating a Protected item.	nd/or discipli
	Create a Password	×
	Create a password to protect this item.	
Pr	Password for: Crypto API Private Key	
	Password:]
e	< Back Finish C	ancel

Next is a screen to enter your certificate information.

For USA people, do NOT use an abbreviation for your state. California (or whatever) needs to be spelled out.

At the bottom of the user information screen is a place for a user name and password.

I put the same user name and password I had used with Comodo in the past and it complained that that user name was already in use. So I created a new one.

Then on to the summary/pay screen:

Secure Payment Pag Your Order Number: Total Amount:	e \$200.00		
PaymentMethods	ED.		-
	Credit Card	O Purchase Order	
Card Details			
Card Number:			
Card Code (3 or 4 digits):			
Expiry Date:			
Cardholder's Name:	Jane Fleming		
Cardbolder Address and	Contact Details		
Company Name:	Beach Bunny S	Software	
Address 1:		The second se	
City / Town:	Î.		
State / Province / County:	F		
Zip / Postcode:	F		
Country		×	
Phone:	P		
Email:			
	Cancel Paymen	d Make Payment	

In past years I had created an "I've requested a certificate and not received it" support ticket immediately after completing the order process.

Not being the most patient person, I tried creating a ticket AND phoning Sectigo's customer service number. I didn't get a human on the phone on this first attempt.

Within a half hour, I received an email with a link to initiate a callback.

Unfortunately, the phone number they showed was one I'd never seen before.

Manage Callback Verification	They had a completely wrong number
We verified phone number "+1 Please provide your extension number (option	for your organisation.
Note: Entering an extension may assist in ensuring that the Please select language for callback:	e callback makes it to you and can be completed.
English This phone number is correct!	This phone number is incorrect!
CALL ME NOW.	PROVIDE CORRECT PHONE

Sectigo's FAQ says "Phone numbers must be verified through a third party database or through an online source that receives information directly from a telecommunications provider". Be advised....

Not being the most patient person (have I said that already?), I clicked the "provide correct phone number" and told them to use the one from Dun & Bradstreet.

And at the same time replied to the support ticket with a screen shot of my listing from the Dun & Bradstreet website.

And phoned their customer support number again. I got an answer this time. Although I'd dialed a US number, my sense was that the lady was elsewhere. An impression reinforced by the "European Office" shown on the order confirmation.



The kind lady said they had sorted my phone number to the correct one and they'd re-send the email. They did, I clicked to get the call NOW, typed in the PIN I was given by their robot over the phone, clicked the Submit button, and that part of the process was done.

Manage Callback Verificat	ion		
We verified phone numb Please provide your extension nur	er "+1 for your organisation. nber (optional):		
Note: Entering an extension may assist in er	suring that the callback makes it to you and can be completed.		
Please select language for callbac	*		
English	•		
This phone number is correct	t! X This phone number is incorrect!		
CALL ME NOW. Note: This will initiate immediate automate Please wait, we are attempting to CALL ME LATER ON	d callback. c call you.		
Note: This will schedule automated callback for a later time. REQUEST MANUAL CALLBACK			
Note. Use this option if you can't use autor	rated calloacks.		
Complete Callback Verific	ation		
To complete callback verification, p verification code we delivered to yo	lease enter your username and password and the 6 digit ur phone.		
Username:			
Password:			
Callback Verification Code:			
	SUBMIT		

After 15 minutes or so I received an email saying my certificate was ready for pickup.

Like a dummy, I clicked the link in the email. Chrome is my default browser and offered to download BlahBlah.crt to my machine.

Because the certificate needs to mate up with the private key that remained on my computer, that would have been useless. (Or more work, as described later).

So I pasted the link into Internet Explorer and clicked the Collect Certificate button.



Now instead of offering to download, IE asked about installing the cert:



And there the certificate was on my machine. (You can get to this window from gear icon / Internet Options in IE, or Internet Options in Control Panel. Then click the Content tab, and then the Certificates button.)

All that remained to do was to export it to a PFX so SetupBuilder can access it for code-signing.

I highlighted the certificate and clicked Export.

ntended p	urpose: <	All>		
Personal	Other People	Intermediate Certification Authorities	Trusted Root Certifica	tion 1
Issued	То	Issued By	Expiratio	Fr ^
	ortex-win.data	DO_NOT_TRUST_FiddlerRoot	2/10/2023	<
*.v:	ssps.visualstudi	DO_NOT_TRUST_FiddlerRoot	3/10/2023	<
🔄 *.w	eather.microso	f DO_NOT_TRUST_FiddlerRoot	3/10/2023	<
- ⊑ ⊒*.w	ebex.com	DO_NOT_TRUST_FiddlerRoot	10/1/2021	<
Bea	ch Bunny Softv	COMODO RSA Code Signing CA	2/17/2020	<
Bea	ch Bunny Softv	Sectigo RSA Code Signing CA	2/1/2023	<
🔄 bou	nce.shell.loc	DO_NOT_TRUST_FiddlerRoot	8/17/2023	<
🔄 cdn	-0.d41.co	DO_NOT_TRUST_FiddlerRoot	1/20/2022	< >
<				>

This is mostly the same process as it's always been.

YES export the private key.

4	🚰 Certificate Export Wizard
	Export Private Key You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with certificate, you must type a password on a later page. Do you want to export the private key with the certificate?	

"Certificate privacy" is an option I'd not seen before. A quick google told me I didn't need that.

"Include all certificates in the certification path" is necessary.

Deleting the private key is not something I'd do unless attacked by Martians on a Thursday during a Tsunami.

← ,	ਓ Certificate Export Wizard	×
	Export File Format Certificates can be exported in a variety of file formats.	_
	Select the format you want to use:	
	O DER encoded binary X.509 (.CER)	
	Base-64 encoded X.509 (.CER)	
	Oryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
	Include all certificates in the certification path if possible	
	Personal Information Exchange - PKCS #12 (.PFX)	
	Include all certificates in the certification path if possible	
	Delete the private key if the export is successful	
	Export all extended properties	
	Enable certificate privacy	
	O Microsoft Serialized Certificate Store (.SST)	
	not doing certificate privacy and definitely not deleting the private key (might need to do this again some day)	ł

This is the password for my new PFX that will be needed for code-signing:

← 🛿 & Certificate Export Wizard S	specify the password for your PFX
Security To maintain security, you mus using a password.	t protect the private key to a security principal or by
Group or user names (reco	mmended)
	Add
	Remove
Password:	
•••••	
Confirm password:	
••••••	
Encryption: TripleDES-SHA1	~
	Ne

Give it a filename:

÷	🖉 Certificate Export Wizard
	File to Export Specify the name of the file you want to export
	File name: C:\install\Comodo\jane20.pfx Browse

Then the first password is needed – the one when I created the private key.

← 😺 Certificat	e Export Wizard This is the password when I originally created the private key.
Comp	leting the Certificate Export Wizard
You have	successfully completed the Certificate Export wizard.
You have File Nan Export I Include File For	specified the following settings: te C:\install\Comodo\jane20.pfx Keys Yes all certificates in the certification path Yes mat Personal Information Exchange (*.pfx)
Exporting	your private exchange key ×
	Password for: Crypto API Private Key ••••••• Remember password Cancel
	OK Cancel Details

Then sign something and check it out.

Start-to-finish was about two and a half hours from deciding to jump into the ice water to signing this test app.

↓ LdapDe	emo.exe Prop	erties		×				
Secu	urity	Details	Previous Versions					
Gene	ral	Compatibility	Digital Signatures					
Signatu	re list							
Name	Name of signer: Digest algorithm Timestamp							
Beac	h Bunny Sof	sha256	Saturday, February 1,	F	ilet			
Digital S	Digital Signature Details ?							
General	Advanced				M			
4	Digital Si This digital	gnature Informat signature is OK.	ion		op op op			
Sign	er information				pp			
Nar	me:	Beach Bunny Soft	ware		M			
E-m	E-mail: jane.fleming@beachbunnysoftware.com Signing time: Saturday, February 1, 2020 5:30:21 PM							
Sigr								
Sigi								
	View Certificate		-					
	Certificate							
G	eneral Detail	s Certification Path	1					
	Cer	rtificate Informati	on					
4	This certif • Ensu • Prot	for the following purpose rom software publisher Iteration after publication	:(s):					
* Refer to the certification authority's statement for details.								
	Issue	ed to: Beach Bunny	Software					
	Issue	ed by: Sectigo RSA	Code Signing CA					
	Valid	from 2/1/2020 to	2/1/2023					

SIDEBAR ON THE PRIVATE KEY / IE STUFF

Just a little insight into the private key and why you need to collect the certificate with IE on the same machine.

After placing my order and before getting my certificate, I looked in the Certificate Enrollment Requests pending on my computer. (MMC – add snap-in for certificates – point at current user).

What's in that folder is an incomplete certificate. "Subject" is blank. "Issued by" is [not available]. There's no certification path. In short, it's not yet a certificate. But does have the private key that was generated on my machine.

For giggles, I exported it to a PFX and used OpenSSL to extract the private key. This is not necessary, but I don't have a life.



Later, logging in to Sectigo's site I see I have access to download my issued certificate.

This is different from the "retrieve certificate" process described earlier. This is a zip file containing my signed certificate and the other certs in the chain. But since this whole ordering process does not send my private key to Sectigo, obviously the cert does not have the private key. Which would make it useless for signing something.

LINDERSOFT		I could download from here, but this will not have the private key.				<u>Logout</u>
Code Signing Certificate Options: Account Options: Management Welcome: Jane Fleming Beach Bunny Software CS Certificate Options Account Options						
SSL Product Type FQDN Order # (Date)	Valid From	Valid To	Serial Number Status (Date) Options		Managen	O MANAGEMENT
Code Signing Certificate (01-FEB-20)	02-FEB-20	01-FEB-23	Issued (02-FEB-20) equest Refund > Download as .zip	-		

The screen shot below shows what's in the downloaded zip file. Note the icon for the 13C0*.crt file (my cert; the others are part of the certification chain). It has a yellow seal in the lower right. This is the icon for a certificate that does not have a private key.

3C0CACD61C6BCA9F8815C9A698B64FD.crt	Security Certificate
🔄 AddTrustExternalCARoot.crt	Security Certificate
🔄 SectigoRSACodeSigningCA.crt	Security Certificate
USERTrustRSAAddTrustCA.crt	Security Certificate

In contrast, here's what's in the certificate as retrieved/installed using the same IE on the same computer where the private key was created. Notice that in addition to the certificate seal, there's a key icon in the upper left. This shows that the certificate includes the private key.

🛱 Beach Bunny Software	COMODO RSA Code Signing CA	2/17/2020
🛱 Beach Bunny Software	Sectigo RSA Code Signing CA	2/1/2023
<u> </u>	DO NOT TRUCT FLUE D	0/17/2022

Of course, if you've saved the private key as I did earlier it would be possible to use OpenSSL to combine that private key with the downloaded certificate from the zip file and make a PFX that could be used for code-signing. But that is left as an exercise for the reader.

And now I can look forward to three more years of peace in my life!

Jane Fleming / February, 2020