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.

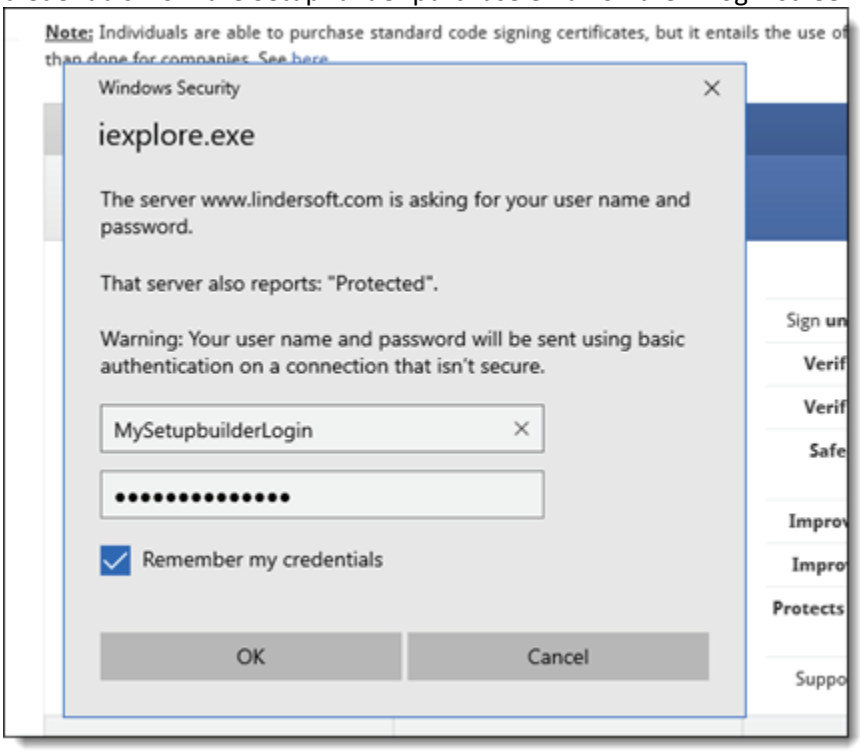
Some years ago, Dun & Bradstreet somehow listed me when I had a business landline. (No doubt they thought I'd buy something from them.) Some fewer years ago, I managed to log in and correct my information to reflect my current home phone number. This was fortunate.

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.

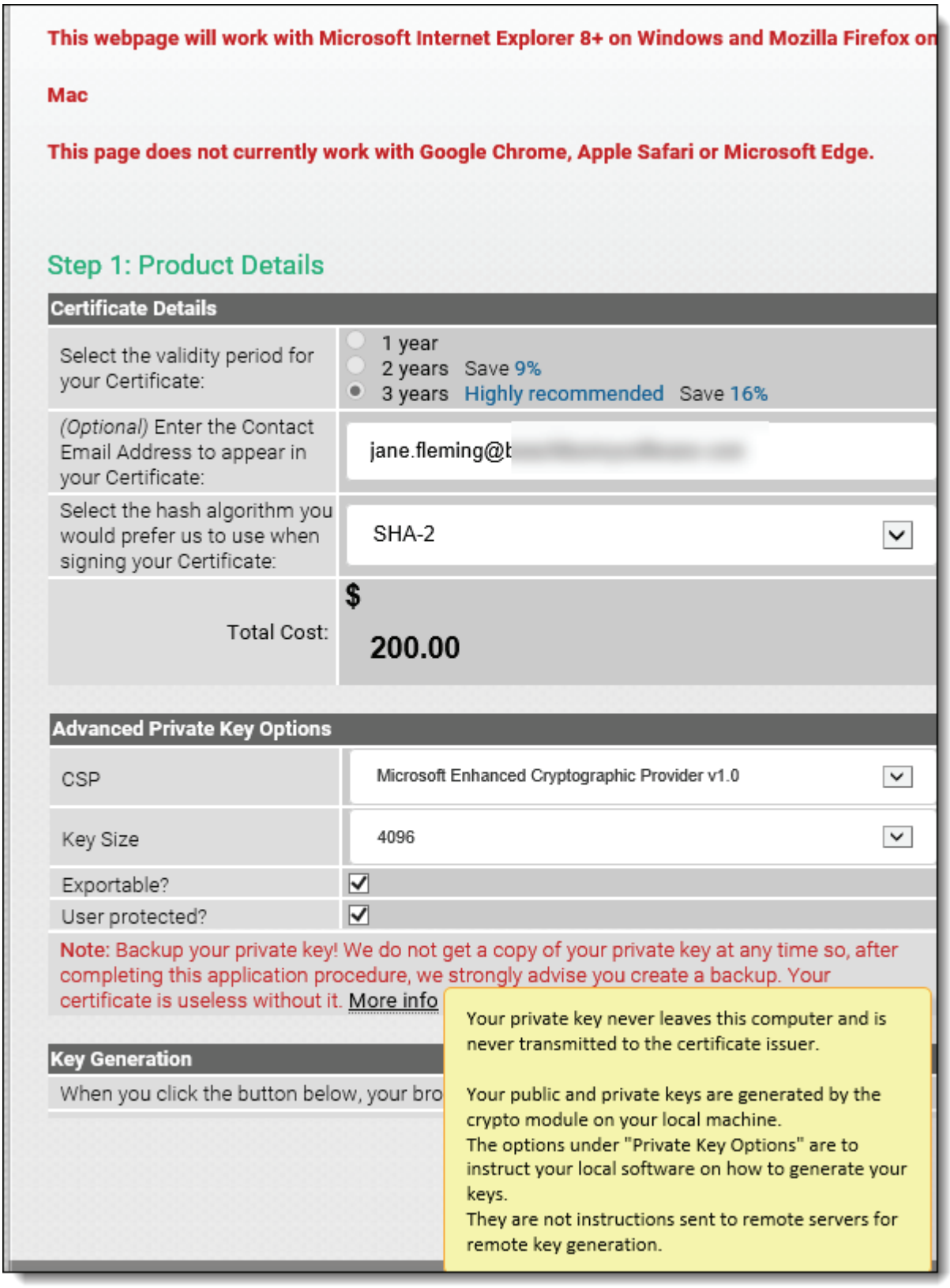
I, of course, opted to make the purchase using the SetupBuilder credentials that Friedrich provides with subscriptions. The cost through Lindersoft was 40% of what the Sectigo guy quoted me.

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…)

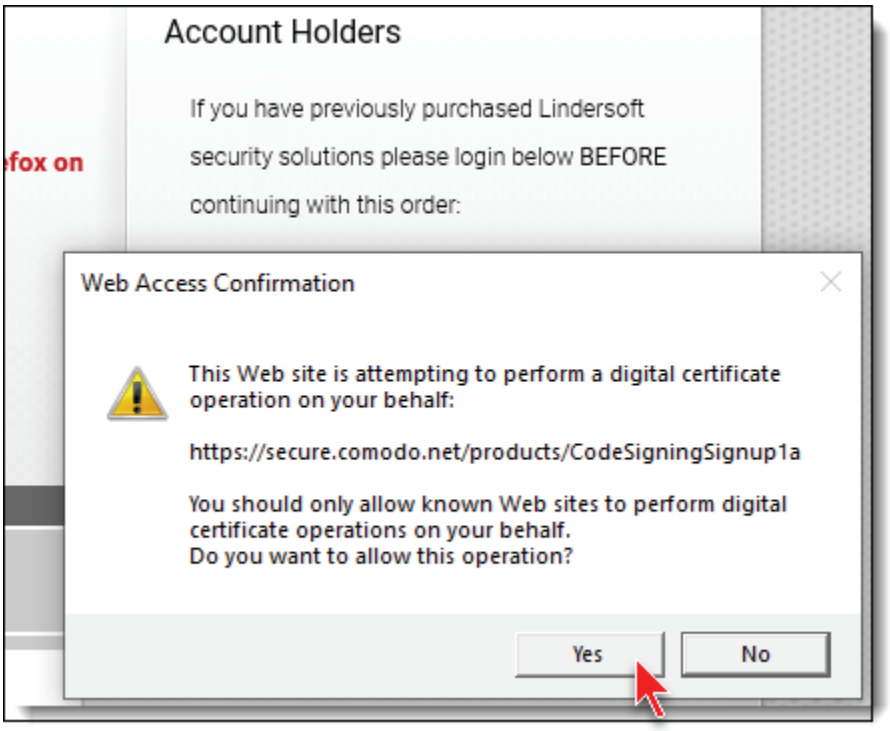
I used the link from the SetupBuilder purchase email, selected the 3-year certificate, and used the credentials from the SetupBuilder purchase email on the IE login screen:



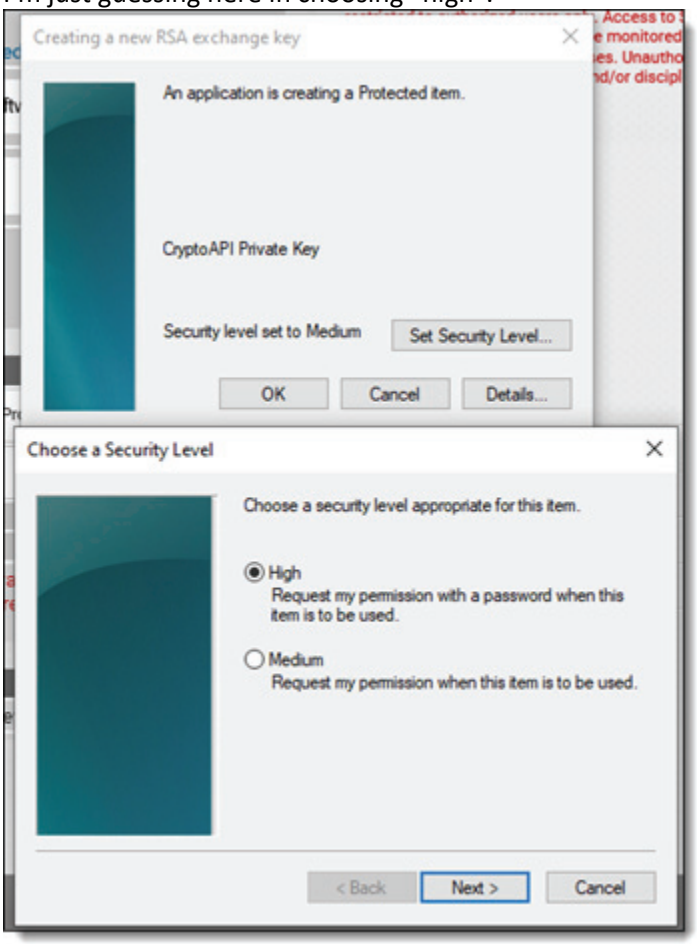
You want SHA-2, of course. (I don't know why SHA-1 is still a choice on the dropdown.) I picked a 4096-bit private key. You want the private key exportable. "User protected" means you will need to create a password now and then give that password again when you eventually export your certificate. So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



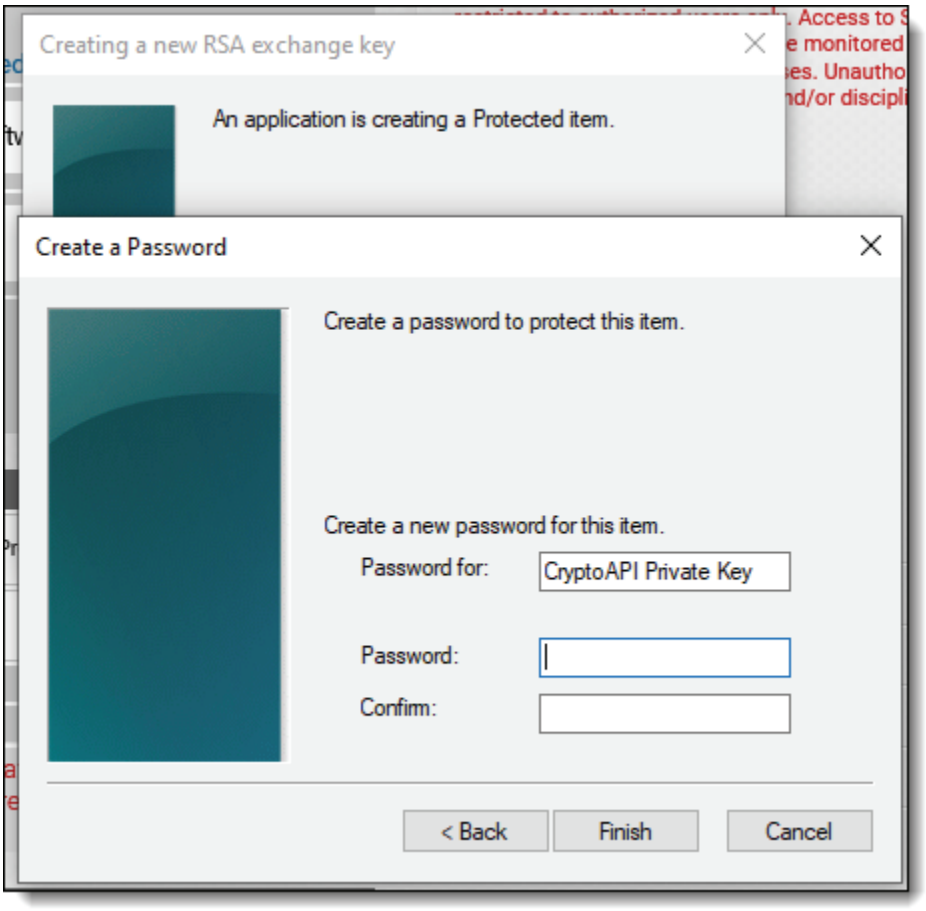
This is the part (well, part of the part) for which you need IE, with its hooks into Windows to generate your private key. If you've done the above step in Chrome, you'll get an error message.
I'll give a little sidebar info on this part (the private key stuff) at the end of this document.



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



You will, obviously, want to remember this password.

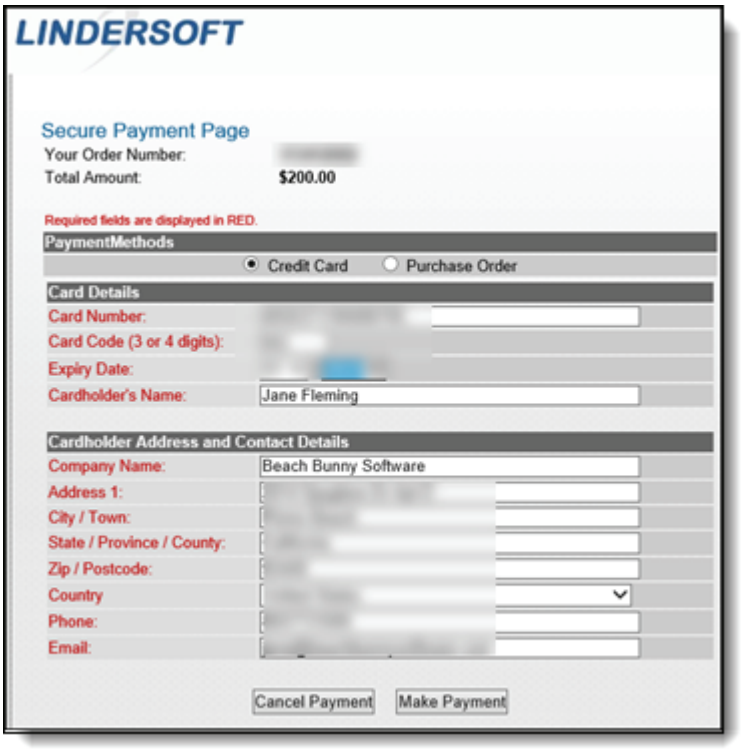


Next is a screen to enter your certificate information.
For USA people, do NOT use an abbreviation for your state. California (or whatever) needs to be spelled out.

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:

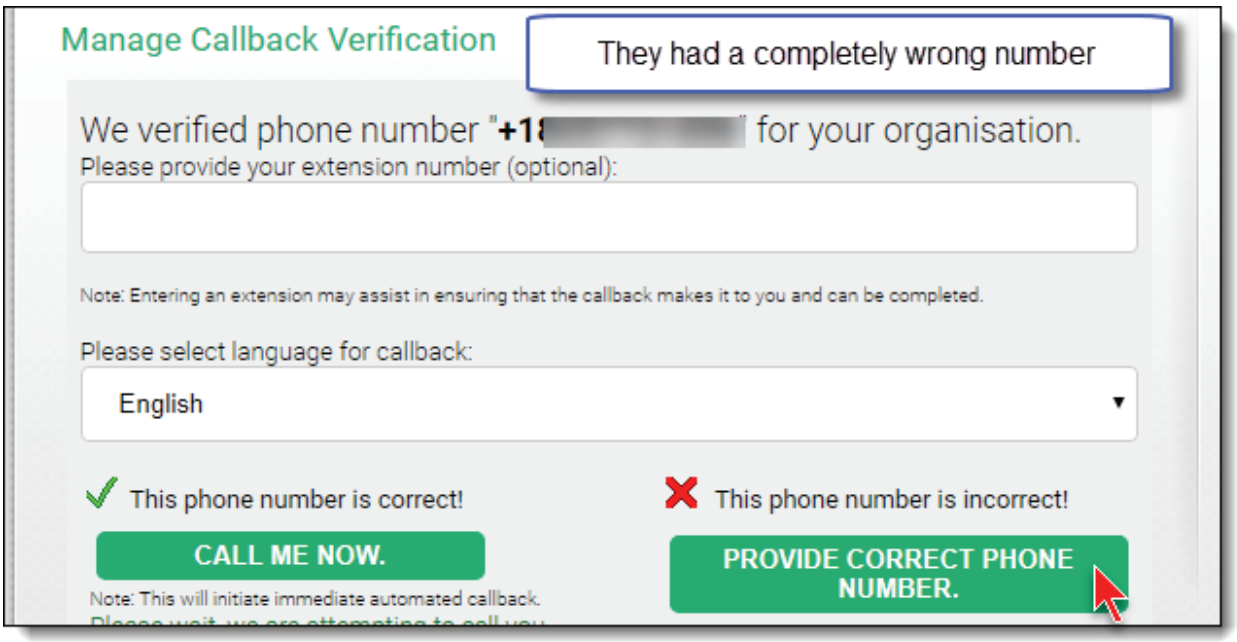


In past years I had created an "I've requested a certificate and not received it" support ticket immediately after completing the order process.

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.

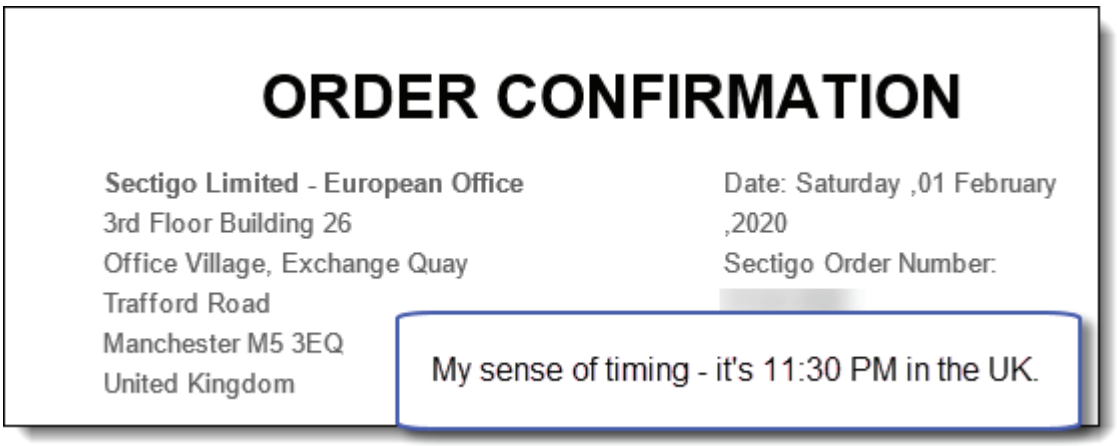


Sectigo's FAQ says "Phone numbers must be verified through a third party database or through an online source that receives information directly from a telecommunications provider". Be advised….

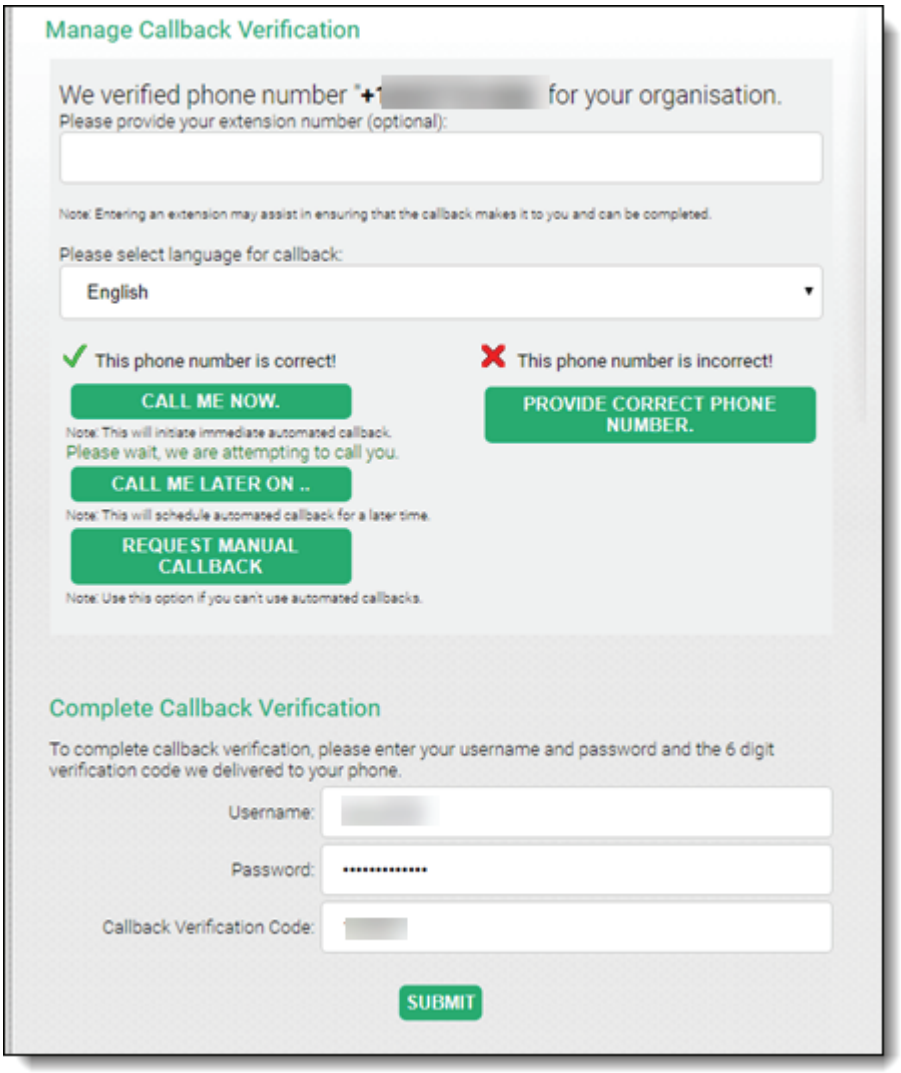
Not being the most patient person (have I said that already?), I clicked the "provide correct phone number" and told them to use the one from Dun & Bradstreet.

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.



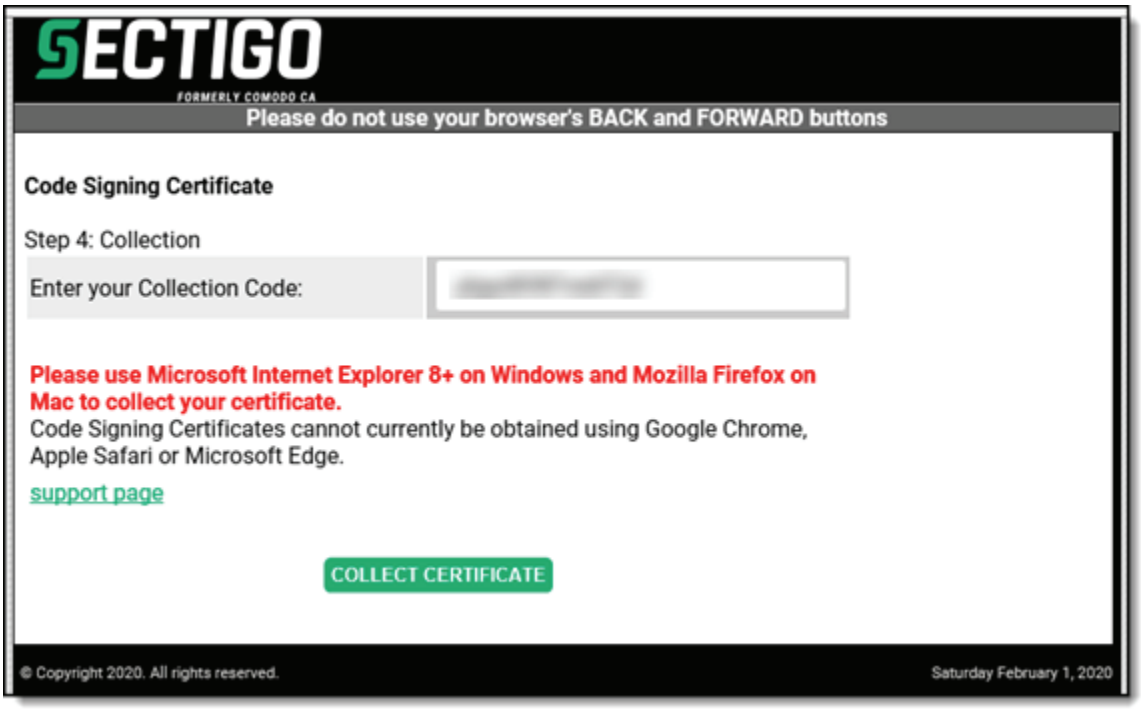
The kind lady said they had sorted my phone number to the correct one and they'd re-send the email. They did, I clicked to get the call NOW, typed in the PIN I was given by their robot over the phone, clicked the Submit button, and that part of the process was done.



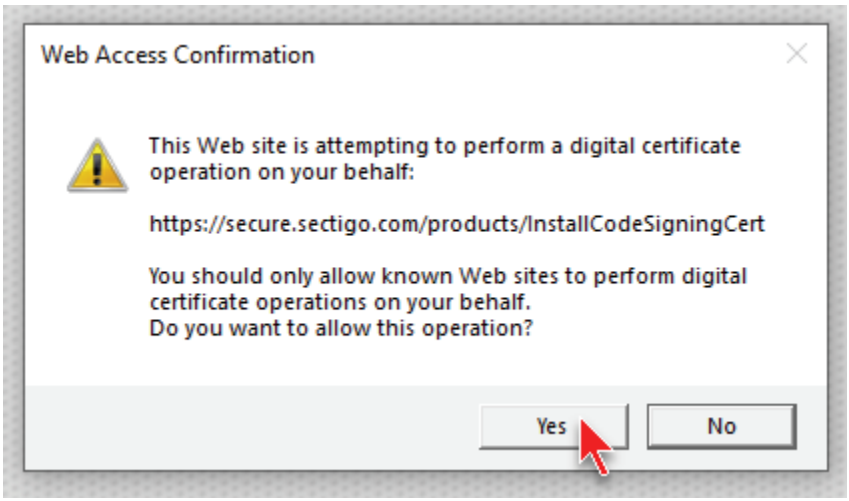
After 15 minutes or so I received an email saying my certificate was ready for pickup.

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.



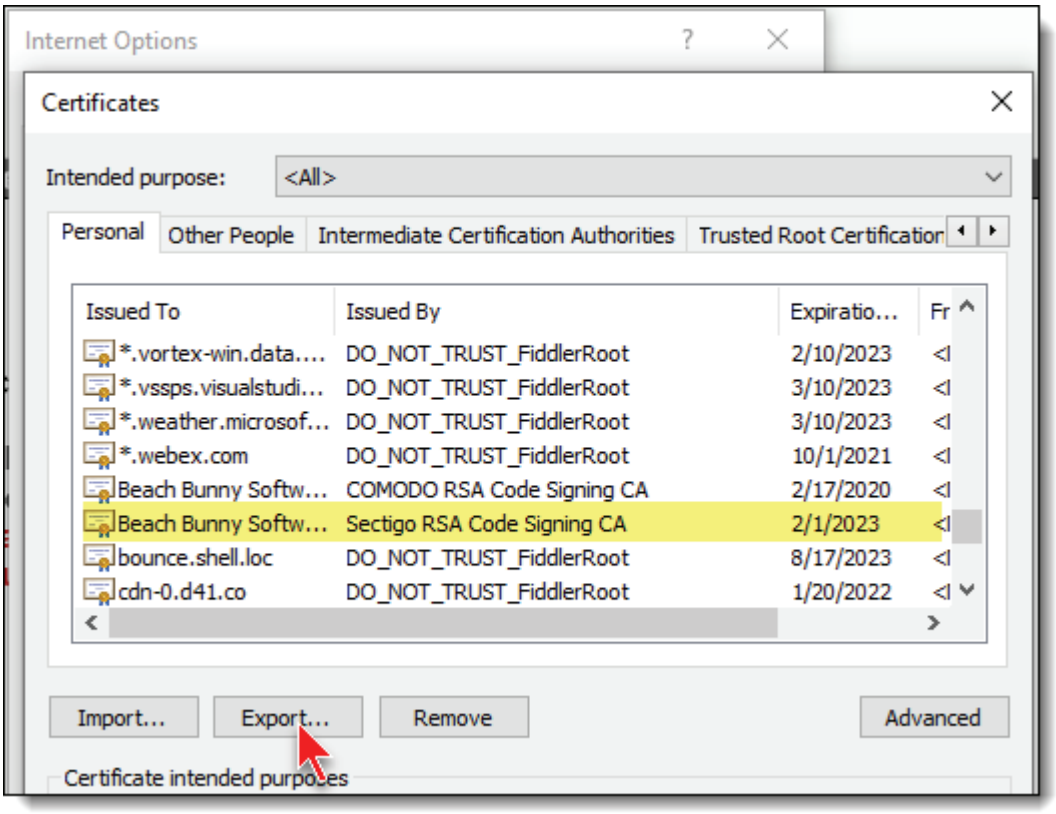
Now instead of offering to download, IE asked about installing the cert:



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.



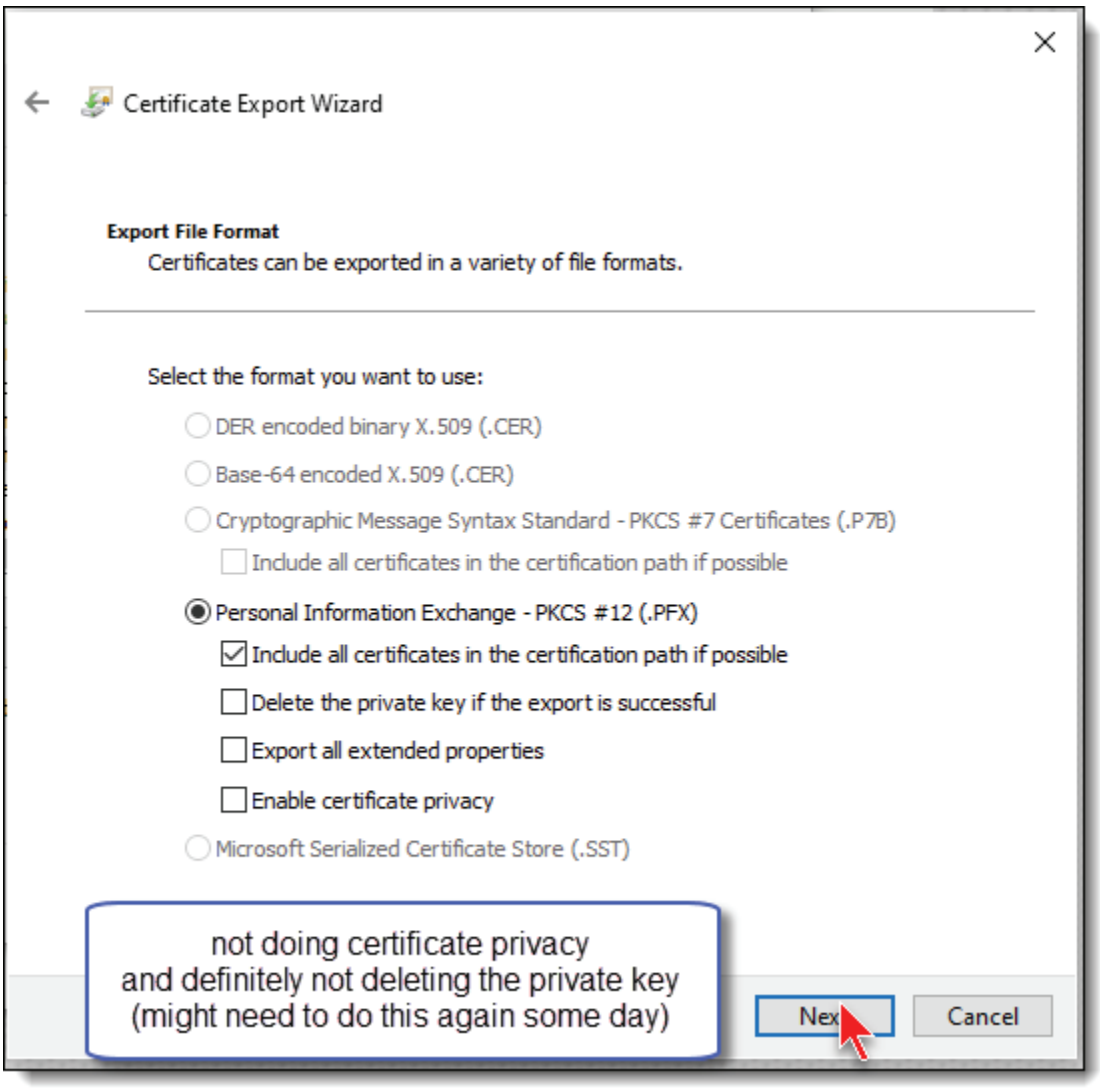
This is mostly the same process as it's always been.

YES export the private key.

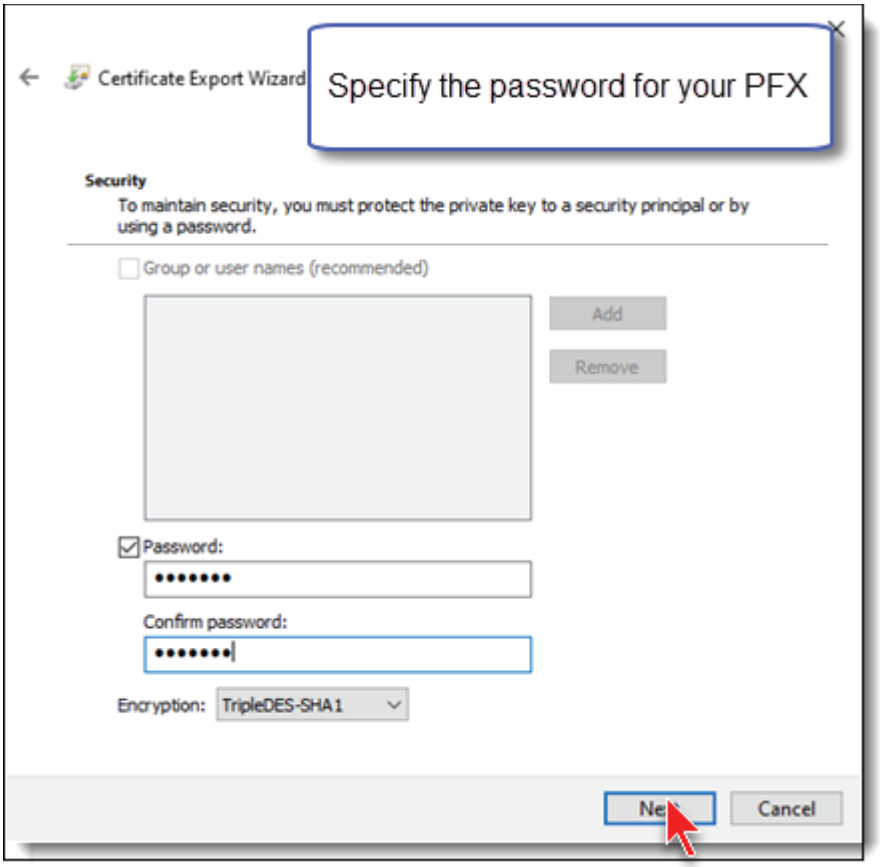
“Certificate privacy” is an option I’d not seen before. A quick google told me I didn’t need that.

“Include all certificates in the certification path” is necessary.

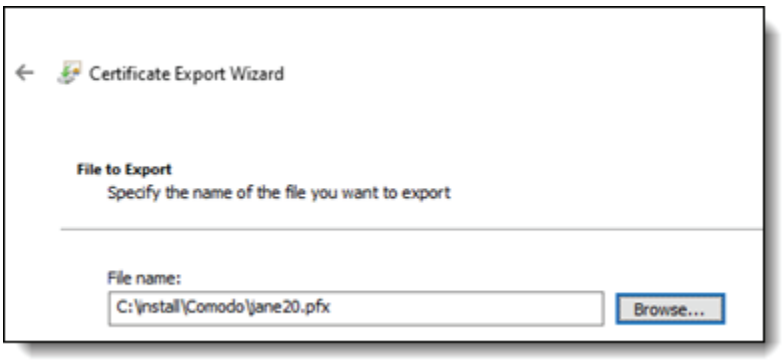
Deleting the private key is not something I’d do unless attacked by Martians on a Thursday during a Tsunami.



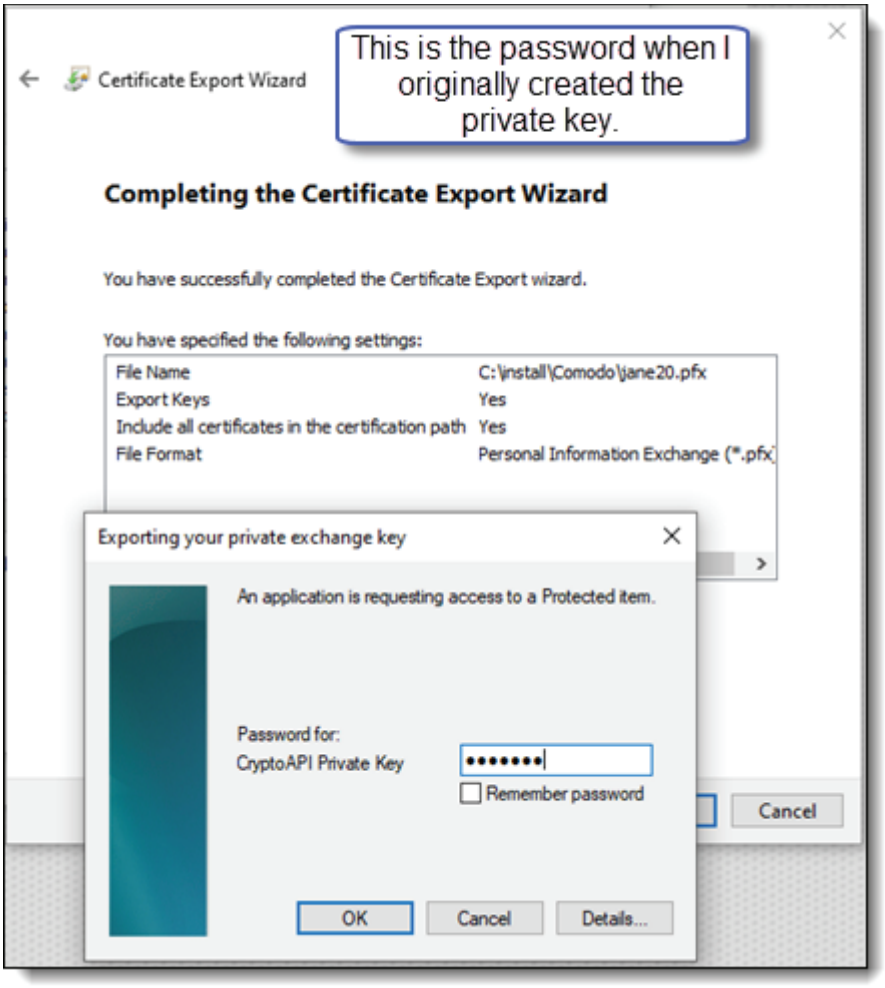
This is the password for my new PFX that will be needed for code-signing:



Give it a filename:

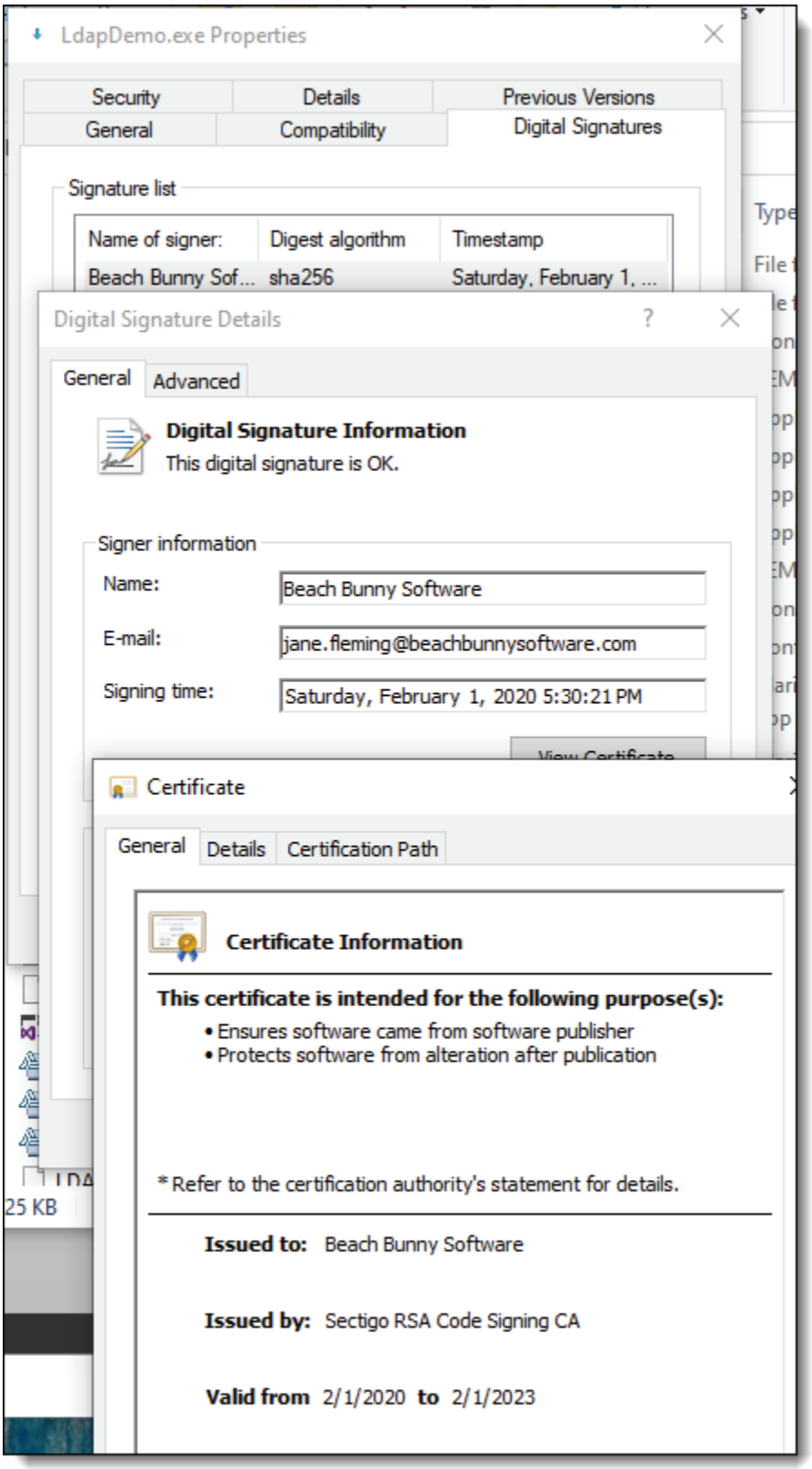


Then the first password is needed – the one when I created the private key.



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.



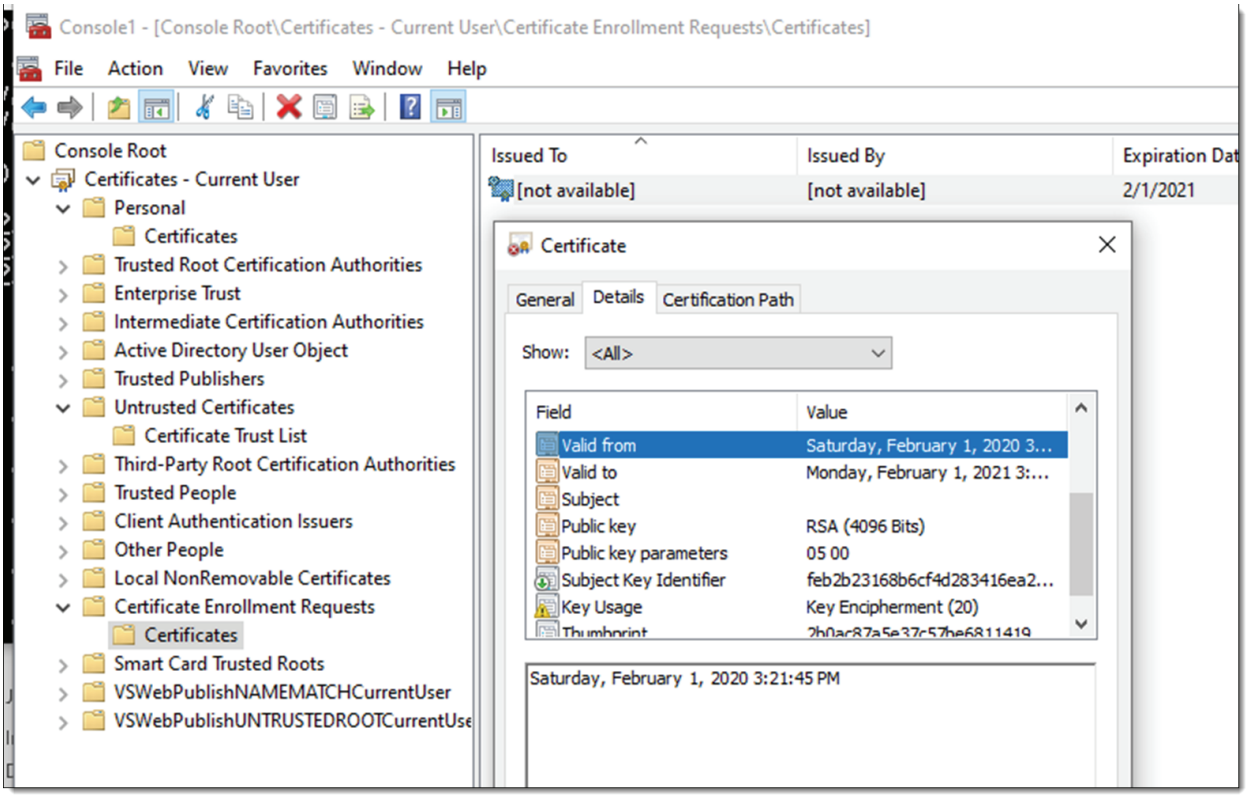
SIDEBAR ON THE PRIVATE KEY / IE STUFF

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).

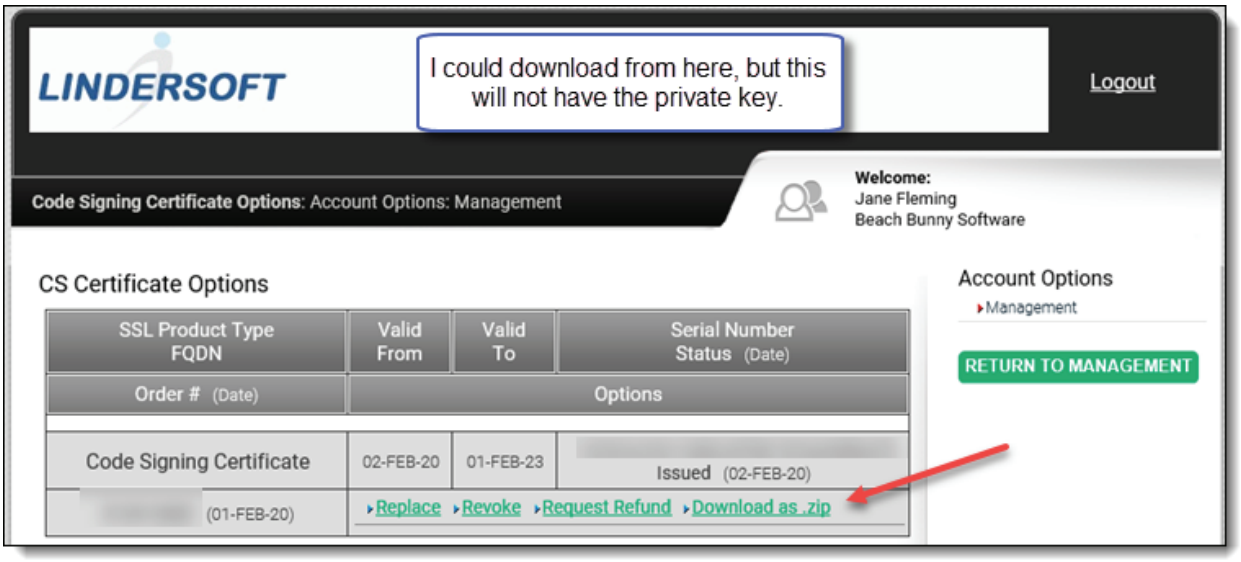
What's in that folder is an incomplete certificate. "Subject" is blank. "Issued by" is [not available]. There's no certification path. In short, it's not yet a certificate. But does have the private key that was generated on my machine.

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.



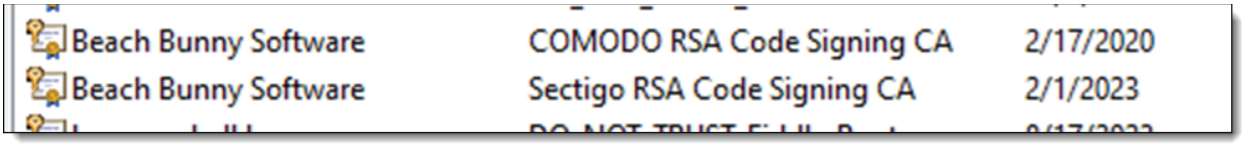
Later, logging in to Sectigo's site I see I have access to download my issued certificate.

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.



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.

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.



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