“Renewing” a Code-Signing Certificate - 2014

Time really does continue to go faster as I continue to get older.

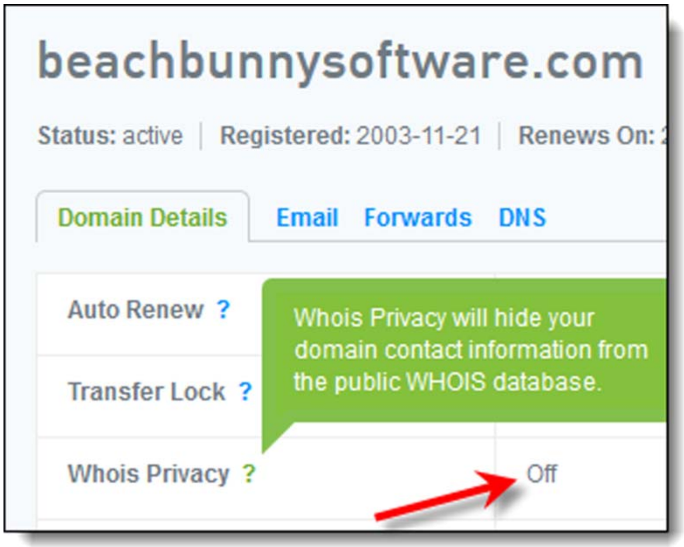
Really? Can it really be time to renew my code-signing certificate? AGAIN??

Yes. Sigh.

All right… let’s not quibble over terminology. One doesn’t actually “renew” an existing certificate. But since my previous certificate was also purchased through Lindersoft’s “deal”, I used the same credentials this time. And with a few strategically placed swift kicks, the whole process took about 16 hours. Plus a couple of days’ advance planning.

Part of the content of a code-signing certificate is an attestation that you are who you say you are.
How Comodo (or any other certificate issuing authority) decides to verify that is their choice.
In the past, I’ve been asked for a copy of a business license, bank statement in the business name, utility bill, phone bill, etc.
But I also recalled a delay from my purchase three years ago because my website’s WHOIS information was protected by my domain registrar’s privacy service.

So a couple of days before initiating the certificate process, I logged into my registrar and turned off the privacy settings for my domain. I did it a couple of days in advance to allow whatever to propagate. Was this necessary or helpful? Dunno.



beachbunnysoftware.com

Status: active | Registered: 2003-11-21 | Renews On: 2

Auto Renew ?

Transfer Lock ?

Whois Privacy will hide your domain contact information from the public WHOIS database.

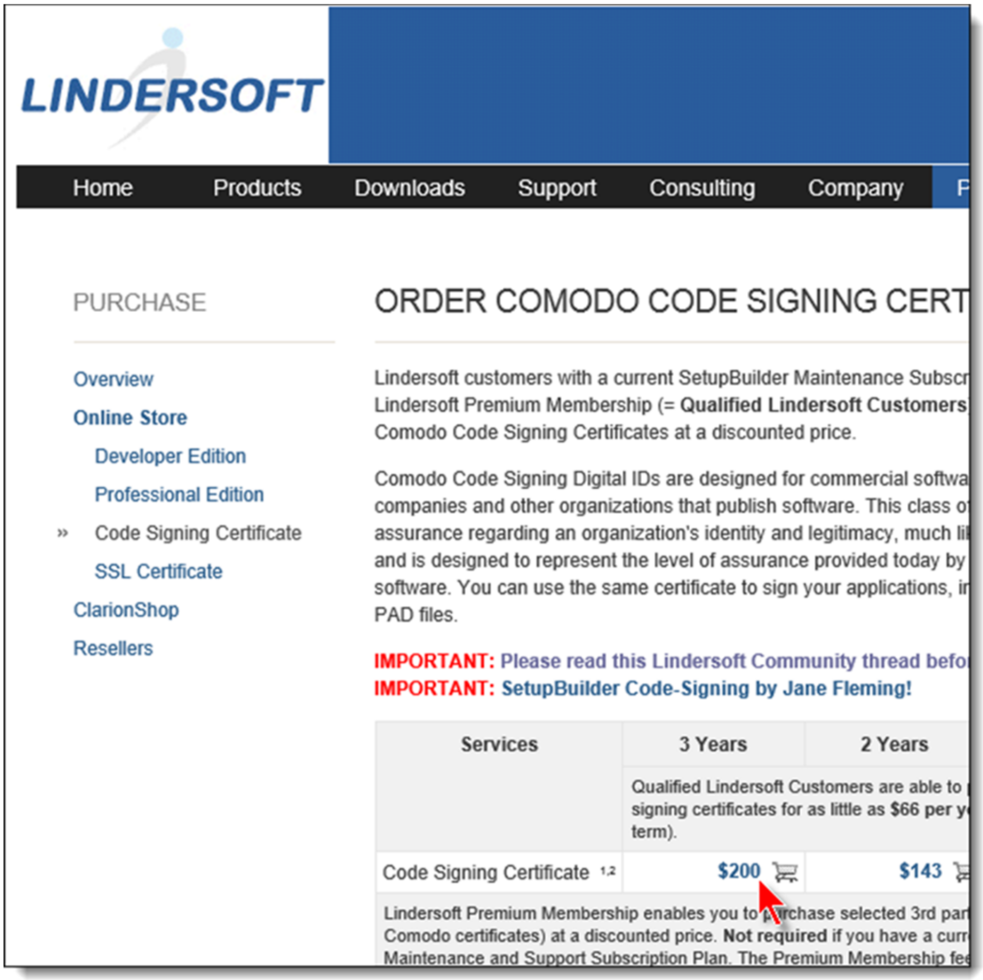
Whois Privacy ? Off

Figuring that Comodo might be processing this in Europe and that I would be working from home on Friday, I placed my order on Thursday evening Pacific time (USA). Based on my prior experience, I was expecting I’d need to receive a confirming phone call on my business phone number, and that number only rings at my residence.

I started by logging in to the Lindersoft website

In the past, the recommendation was to use Windows XP and Internet Explorer.
Feeling carefree and chipper, however, I opted to use a Windows 8.1 virtual machine. I did use IE, though, as that’s the only browser I have in that VM.

Began at the lindersoft.com website, selecting the 3 Years option:



ORDER COMODO CODE SIGNING CERT

Lindersoft customers with a current SetupBuilder Maintenance Subscr Lindersoft Premium Membership (= **Qualified Lindersoft Customers** Comodo Code Signing Certificates at a discounted price.

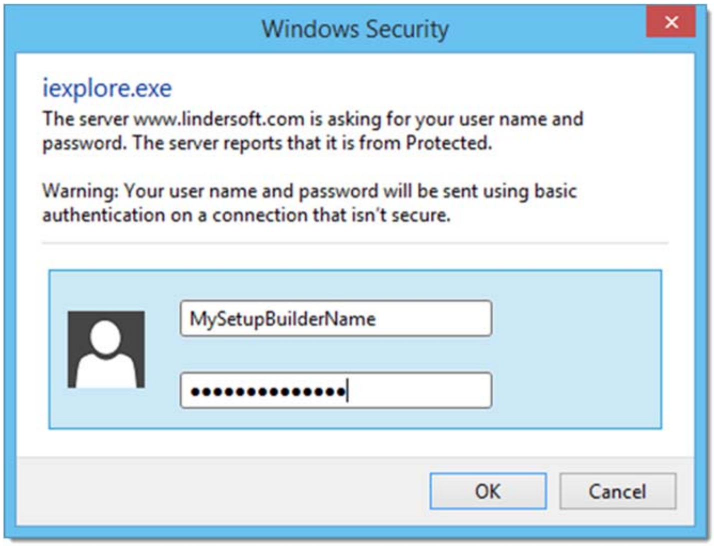
Comodo Code Signing Digital IDs are designed for commercial softwa companies and other organizations that publish software. This class o assurance regarding an organization's identity and legitimacy, much li and is designed to represent the level of assurance provided today by software. You can use the same certificate to sign your applications, i PAD files.

IMPORTANT: Please read this Lindersoft Community thread befo
IMPORTANT: SetupBuilder Code-Signing by Jane Fleming!

Services	3 Years	2 Years
	Qualified Lindersoft Customers are able to signing certificates for as little as **$66 per y** term).	
Code Signing Certificate 1,2	**$200**	**$143**

Lindersoft Premium Membership enables you to purchase selected 3rd par Comodo certificates) at a discounted price. **Not required** if you have a curr Maintenance and Support Subscription Plan. The Premium Membership fee

Logged in with the credentials that Friedrich sends out to current customers. It's the information at the bottom of the "there's a new SetupBuilder build available" emails.



iexplore.exe

The server www.lindersoft.com is asking for your user name and password. The server reports that it is from Protected.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

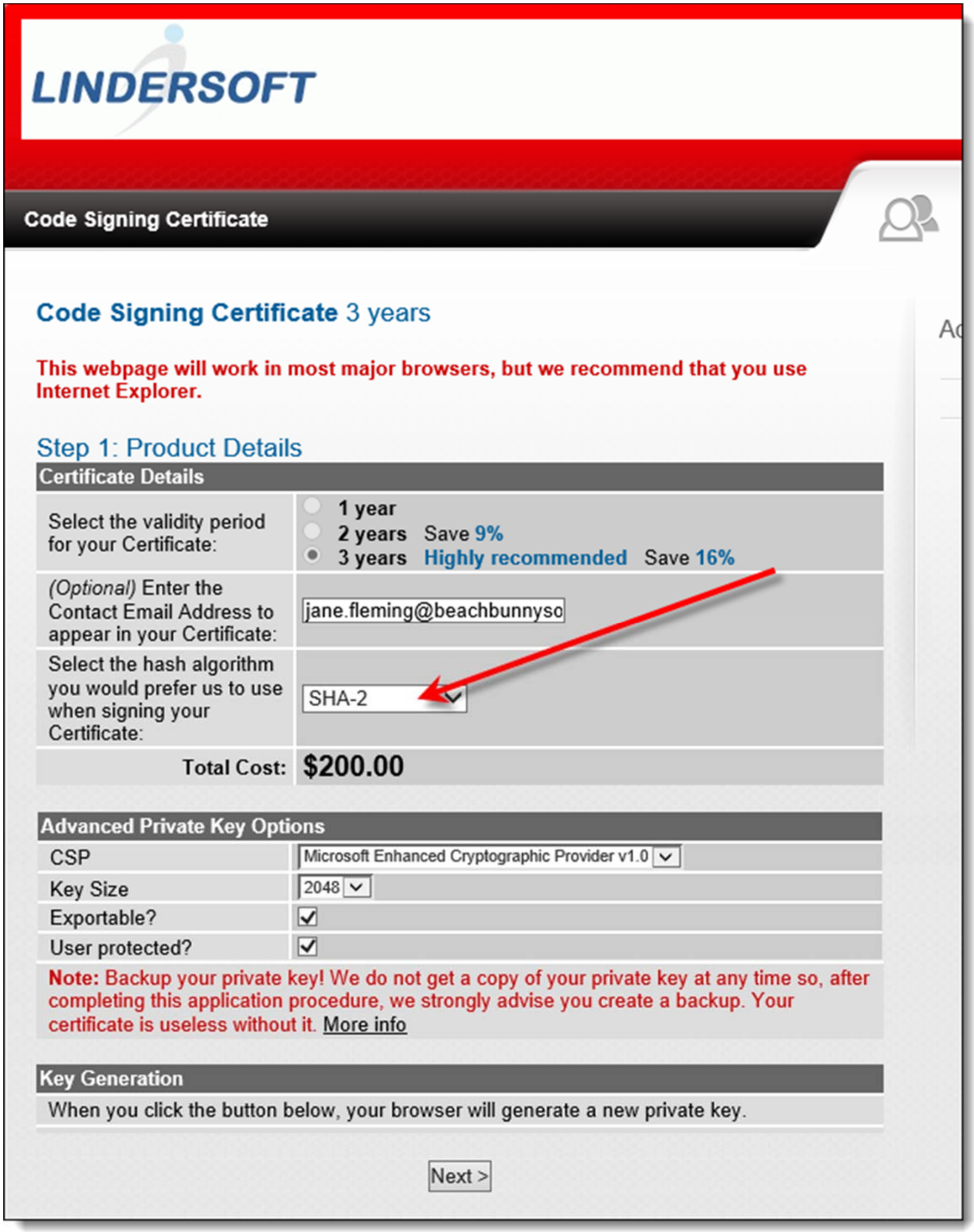
MySetupBuilderName

••••••••••••••

Now it was time to specify stuff and pay.

But one piece of “stuff” was different and unexpected.

There’s now a choice as to the hash algorithm to be used – SHA-1 or SHA-2.
A wee bit of google revealed that SHA-1 certificates are being deprecated (announced November 11, 2013
http://blogs.technet.com/b/pki/archive/2013/11/12/sha1-deprecation-policy.aspx)
So buying SHA-2 seemed the obvious choice.



Code Signing Certificate 3 years

This webpage will work in most major browsers, but we recommend that you use Internet Explorer.

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:	jane.fleming@beachbunnyso
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	2048
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

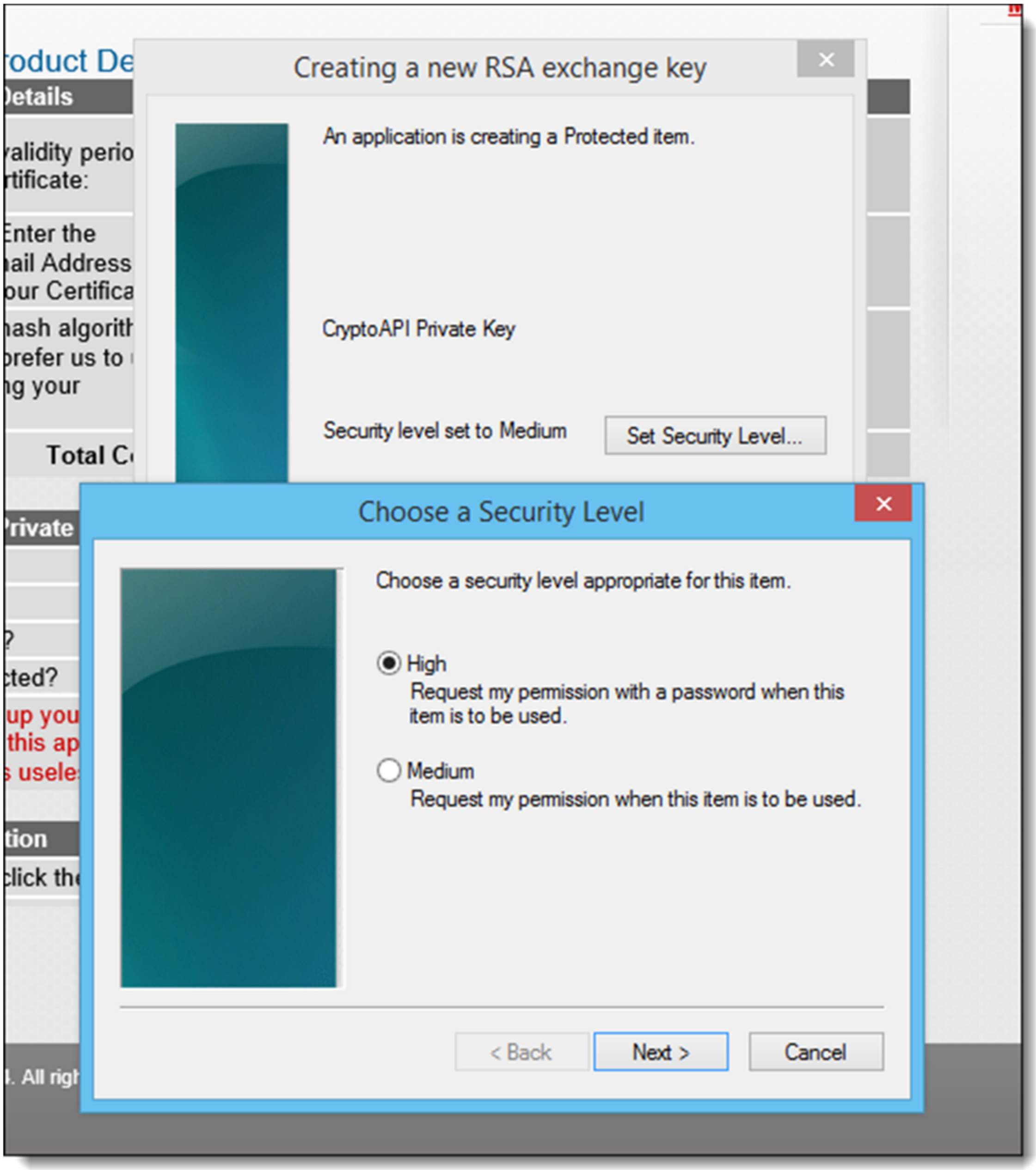
Key Generation

When you click the button below, your browser will generate a new private key.

The ordering page admonishes one to back up one's private key. However, I really didn't know how to do that… in that we no longer wind up with certificate files as we did in the old XP days.
I wound up making a snapshot of my virtual machine after I placed the order.

You definitely want to mark your private key as exportable.
I'm not sure what "user protected" involves, but marked that as well.

Perhaps that's why I got the next popup window.
DO REMEMBER THE PASSWORD YOU CREATE HERE!



Creating a new RSA exchange key

An application is creating a Protected item.

CryptoAPI Private Key

Security level set to Medium

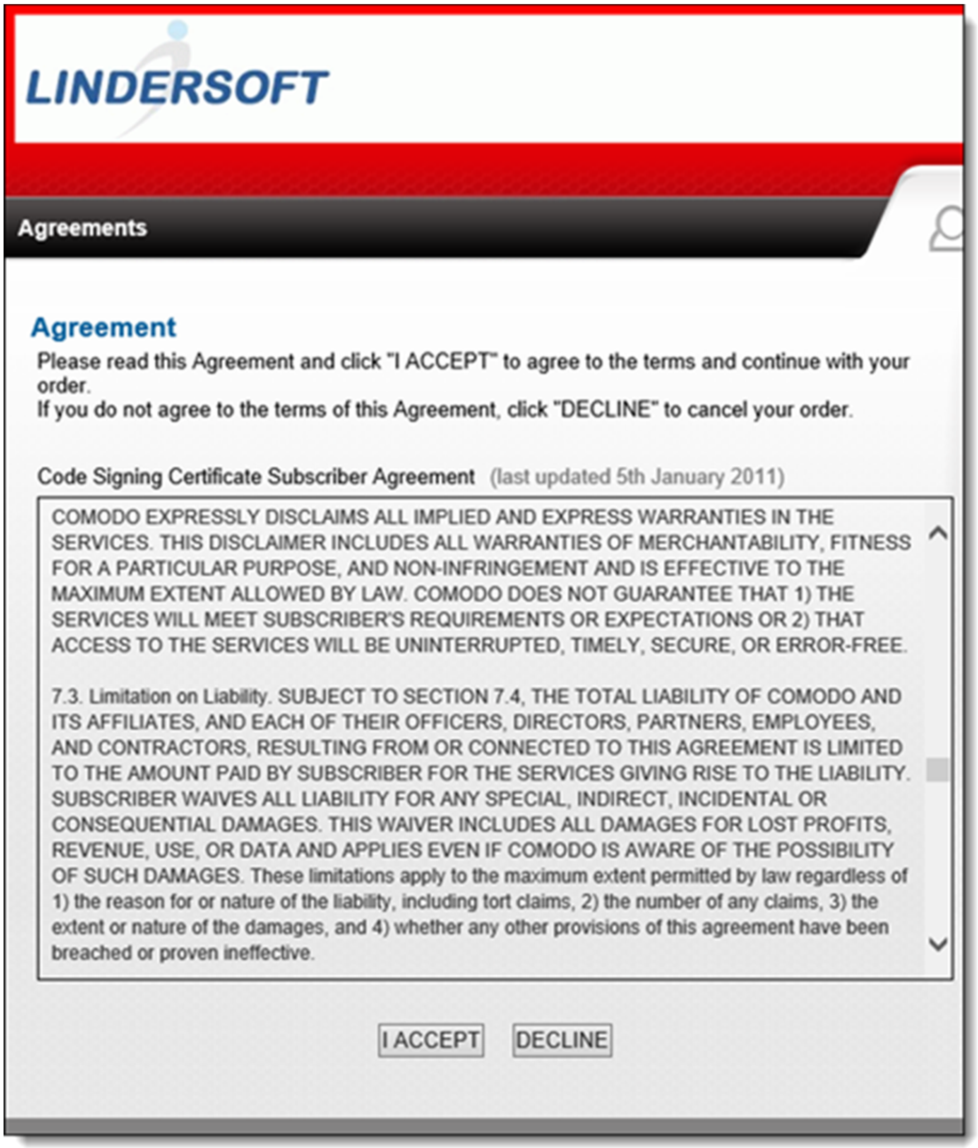
Choose a Security Level

Choose a security level appropriate for this item.

● High
Request my permission with a password when this item is to be used.

○ Medium
Request my permission when this item is to be used.

Does anybody actually read these things??



Agreement

Please read this Agreement and click "I ACCEPT" to agree to the terms and continue with your order.
If you do not agree to the terms of this Agreement, click "DECLINE" to cancel your order.

Code Signing Certificate Subscriber Agreement (last updated 5th January 2011)

COMODO EXPRESSLY DISCLAIMS ALL IMPLIED AND EXPRESS WARRANTIES IN THE SERVICES. THIS DISCLAIMER INCLUDES ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND IS EFFECTIVE TO THE MAXIMUM EXTENT ALLOWED BY LAW. COMODO DOES NOT GUARANTEE THAT 1) THE SERVICES WILL MEET SUBSCRIBER'S REQUIREMENTS OR EXPECTATIONS OR 2) THAT ACCESS TO THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE.

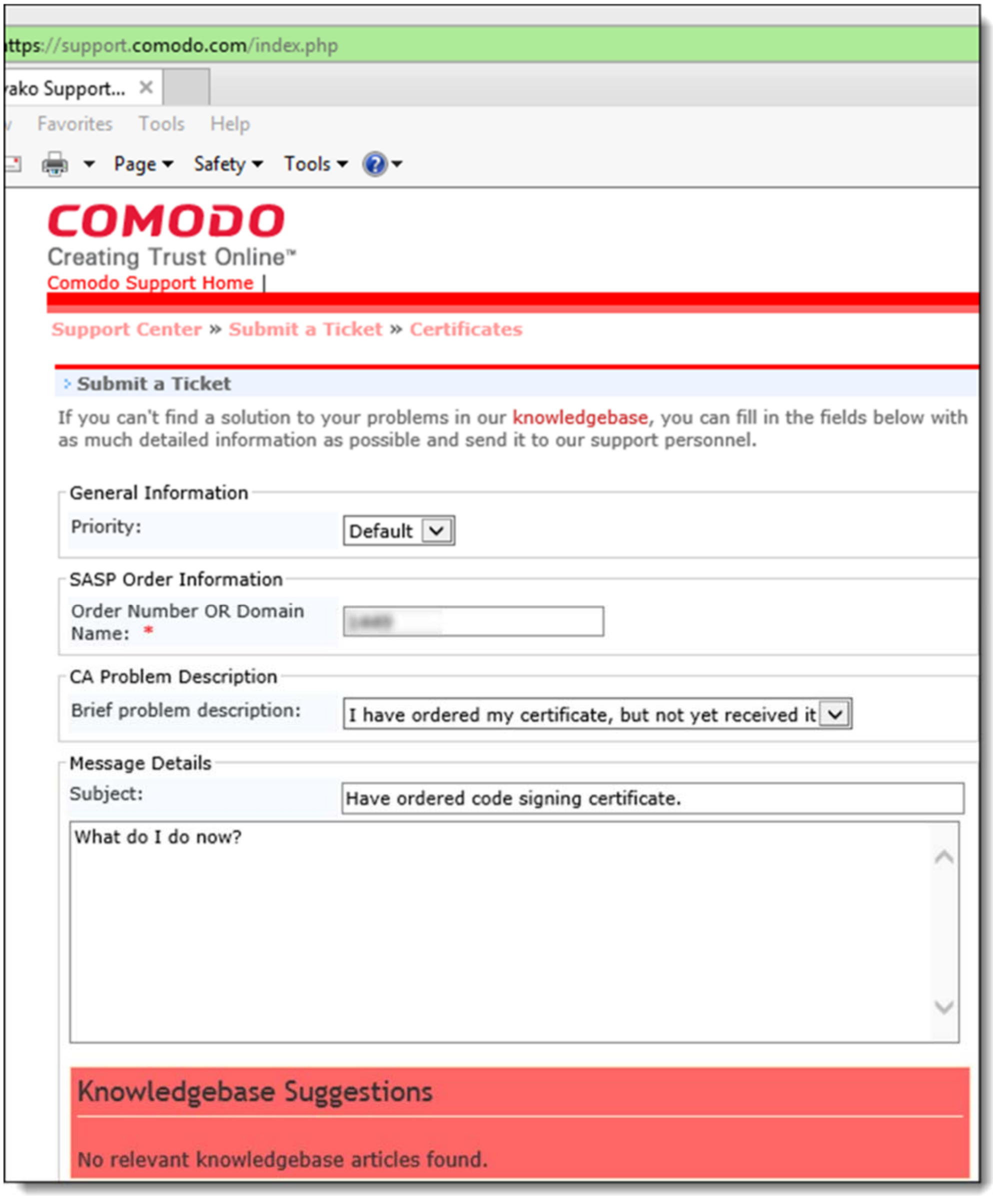
7.3. Limitation on Liability. SUBJECT TO SECTION 7.4, THE TOTAL LIABILITY OF COMODO AND ITS AFFILIATES, AND EACH OF THEIR OFFICERS, DIRECTORS, PARTNERS, EMPLOYEES, AND CONTRACTORS, RESULTING FROM OR CONNECTED TO THIS AGREEMENT IS LIMITED TO THE AMOUNT PAID BY SUBSCRIBER FOR THE SERVICES GIVING RISE TO THE LIABILITY. SUBSCRIBER WAIVES ALL LIABILITY FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES. THIS WAIVER INCLUDES ALL DAMAGES FOR LOST PROFITS, REVENUE, USE, OR DATA AND APPLIES EVEN IF COMODO IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. These limitations apply to the maximum extent permitted by law regardless of 1) the reason for or nature of the liability, including tort claims, 2) the number of any claims, 3) the extent or nature of the damages, and 4) whether any other provisions of this agreement have been breached or proven ineffective.

Paid.

Made a note of my order number.

Then immediately opened a support ticket.

No, it's not that I was expecting an instantaneous reply. But past experience has led me to think this is a good way to find out exactly what they need next.



Support Center » Submit a Ticket » Certificates

Submit a Ticket

If you can't find a solution to your problems in our knowledgebase, you can fill in the fields below with as much detailed information as possible and send it to our support personnel.

General Information

Priority: Default

SASP Order Information

Order Number OR Domain Name: * [redacted]

CA Problem Description

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

Message Details

Subject: Have ordered code signing certificate.

What do I do now?

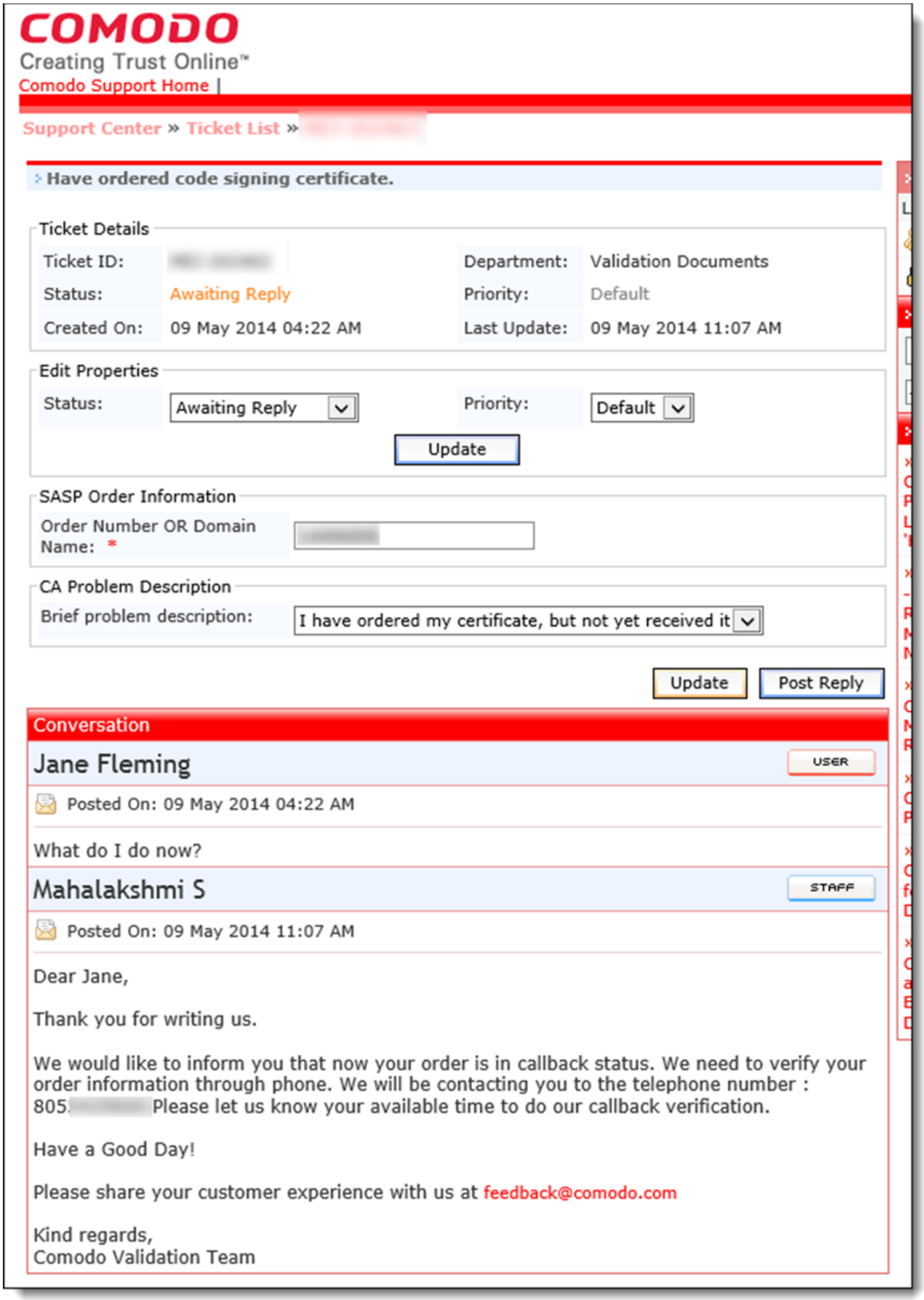
Knowledgebase Suggestions

No relevant knowledgebase articles found.

Friday morning, I checked the status of my ticket. Noticed that the creation time it shows is either UTC or European local time. (Because it shows "AM" rather than military time, I'm guessing the latter.)

The ticket only said they needed to phone my business number, and asked for an available time. I said "now" and updated the ticket.

Note that they specified my phone number, which apparently they found listed somewhere.



Have ordered code signing certificate.

Ticket Details

Ticket ID:	[redacted]	Department:	Validation Documents
Status:	Awaiting Reply	Priority:	Default
Created On:	09 May 2014 04:22 AM	Last Update:	09 May 2014 11:07 AM

Edit Properties

Status: Awaiting Reply | Priority: Default

SASP Order Information

Order Number OR Domain Name: * [redacted]

CA Problem Description

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

Conversation

Jane Fleming

Posted On: 09 May 2014 04:22 AM

What do I do now?

Mahalakshmi S

Posted On: 09 May 2014 11:07 AM

Dear Jane,

Thank you for writing us.

We would like to inform you that now your order is in callback status. We need to verify your order information through phone. We will be contacting you to the telephone number : 805[redacted]Please let us know your available time to do our callback verification.

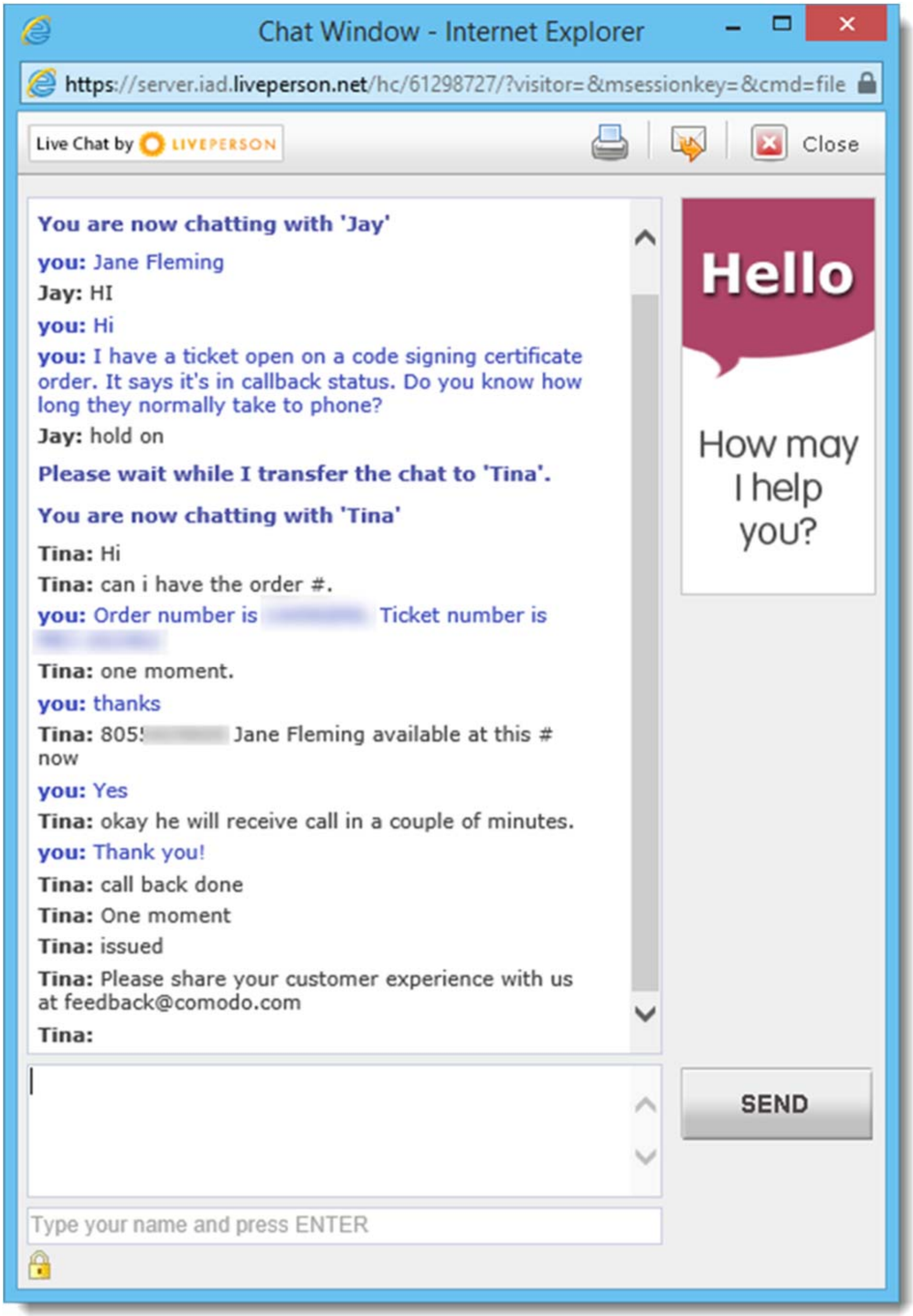
Have a Good Day!

Please share your customer experience with us at feedback@comodo.com

Kind regards,
Comodo Validation Team

Not one who does well at the “waiting for the phone to ring” game, after about an hour and a half I opened a chat window on Comodo’s support website.

And then received a phone call. Caller-ID just said “SKYPE CALLER”.


Chat Window - Internet Explorer
https://server.iad.liveperson.net/hc/61298727/?visitor=&msessionkey=&cmd=file
Live Chat by LIVEPERSON
Close
Hello
How may I help you?
SEND
Type your name and press ENTER

You are now chatting with 'Jay'

you: Jane Fleming

Jay: HI

you: Hi

you: I have a ticket open on a code signing certificate order. It says it's in callback status. Do you know how long they normally take to phone?

Jay: hold on

Please wait while I transfer the chat to 'Tina'.

You are now chatting with 'Tina'

Tina: Hi

Tina: can i have the order #.

you: Order number is [redacted] Ticket number is [redacted]

Tina: one moment.

you: thanks

Tina: 805[redacted] Jane Fleming available at this # now

you: Yes

Tina: okay he will receive call in a couple of minutes.

you: Thank you!

Tina: call back done

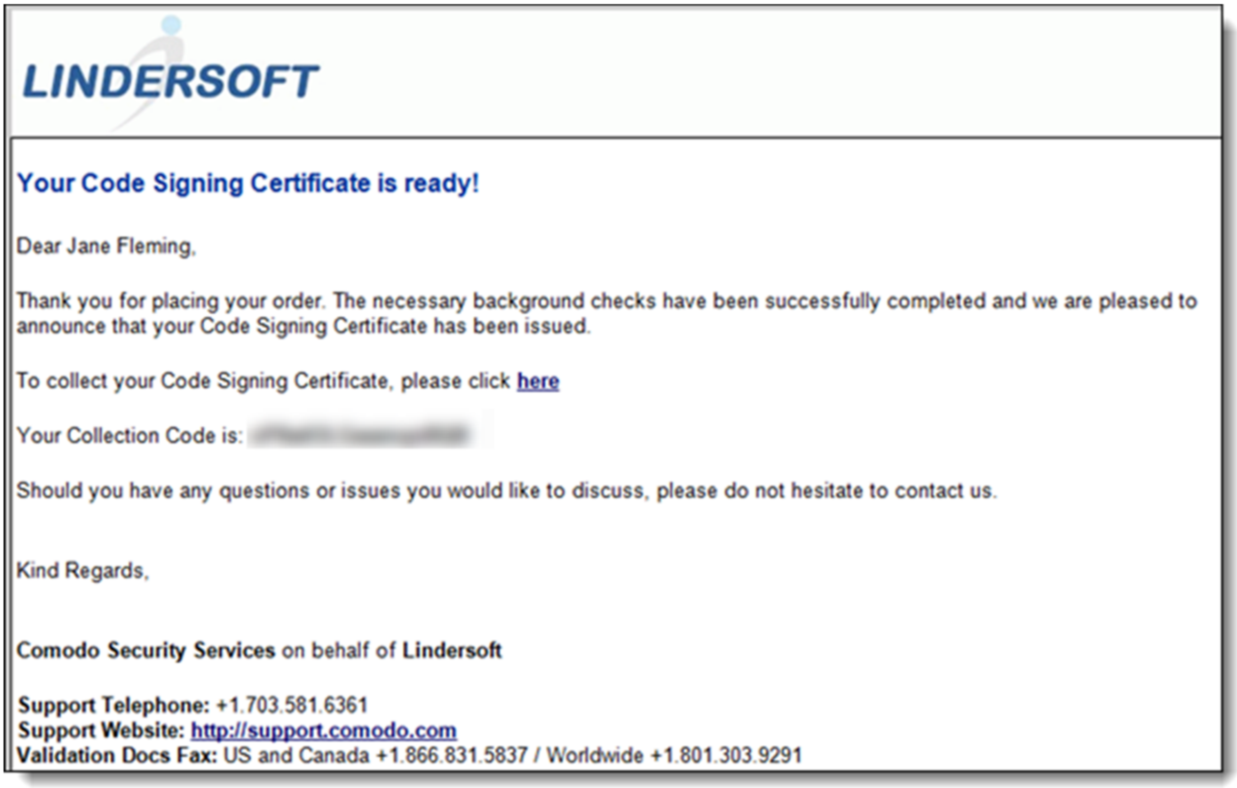
Tina: One moment

Tina: issued

Tina: Please share your customer experience with us at feedback@comodo.com

Tina:

Within the next hour, I received an email with a collection code.



Your Code Signing Certificate is ready!

Dear Jane Fleming,

Thank you for placing your order. The necessary background checks have been successfully completed and we are pleased to announce that your Code Signing Certificate has been issued.

To collect your Code Signing Certificate, please click here

Your Collection Code is: [redacted]

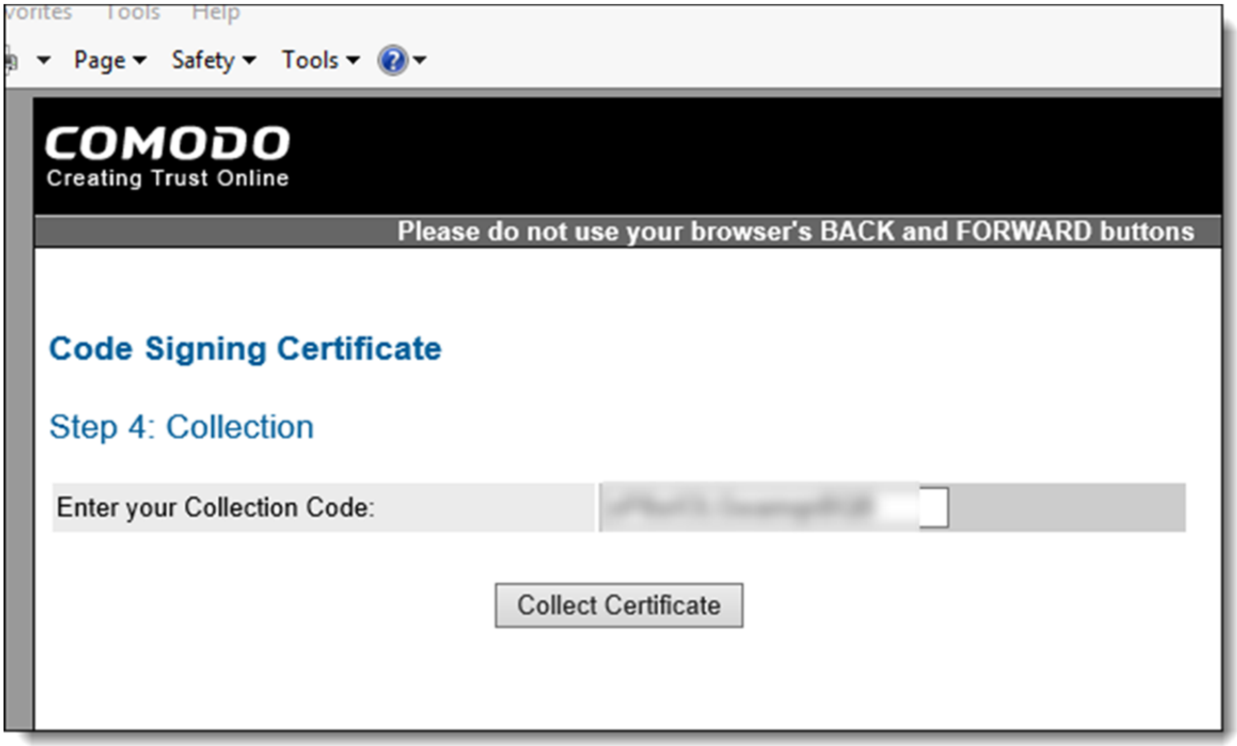
Should you have any questions or issues you would like to discuss, please do not hesitate to contact us.

Kind Regards,

Comodo Security Services on behalf of **Lindersoft**

Support Telephone: +1.703.581.6361
Support Website: http://support.comodo.com
Validation Docs Fax: US and Canada +1.866.831.5837 / Worldwide +1.801.303.9291

I opened the link in Internet Explorer on the virtual machine I had used to create the certificate request.

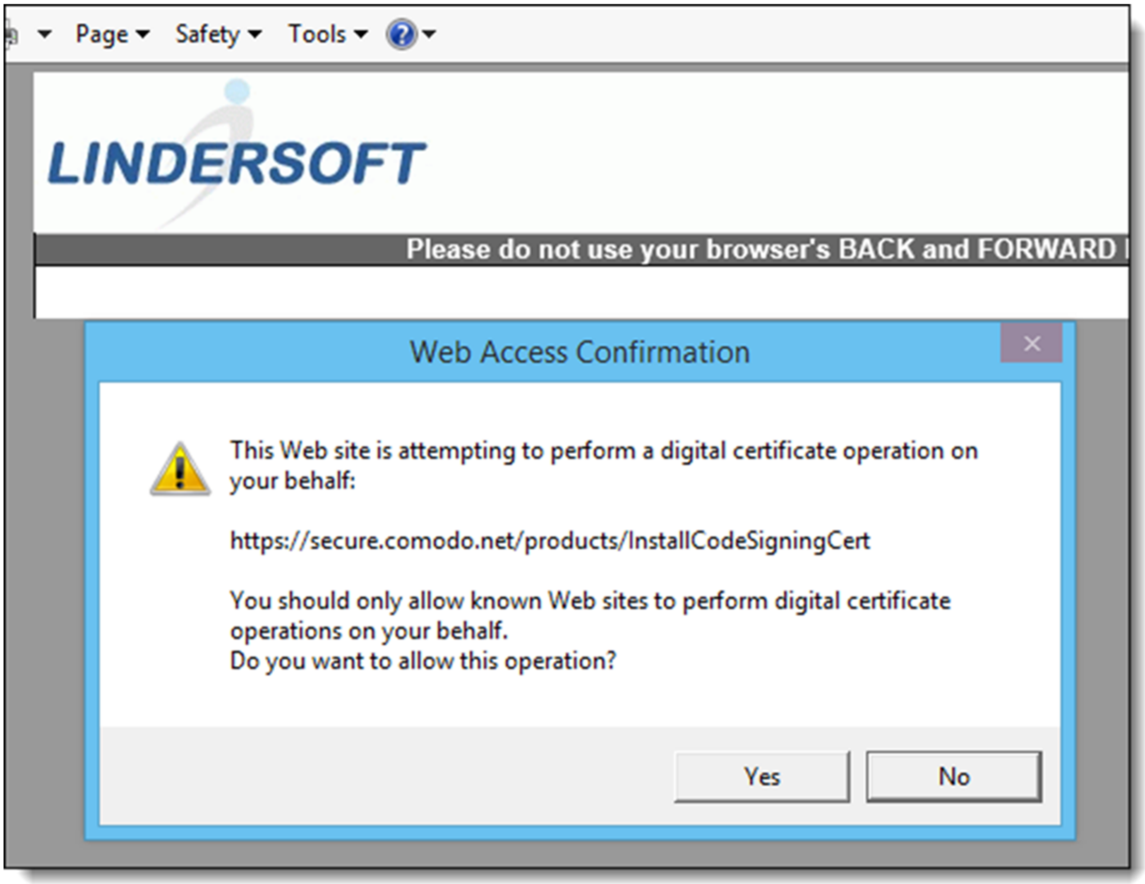


Please do not use your browser's BACK and FORWARD buttons

Code Signing Certificate

Step 4: Collection

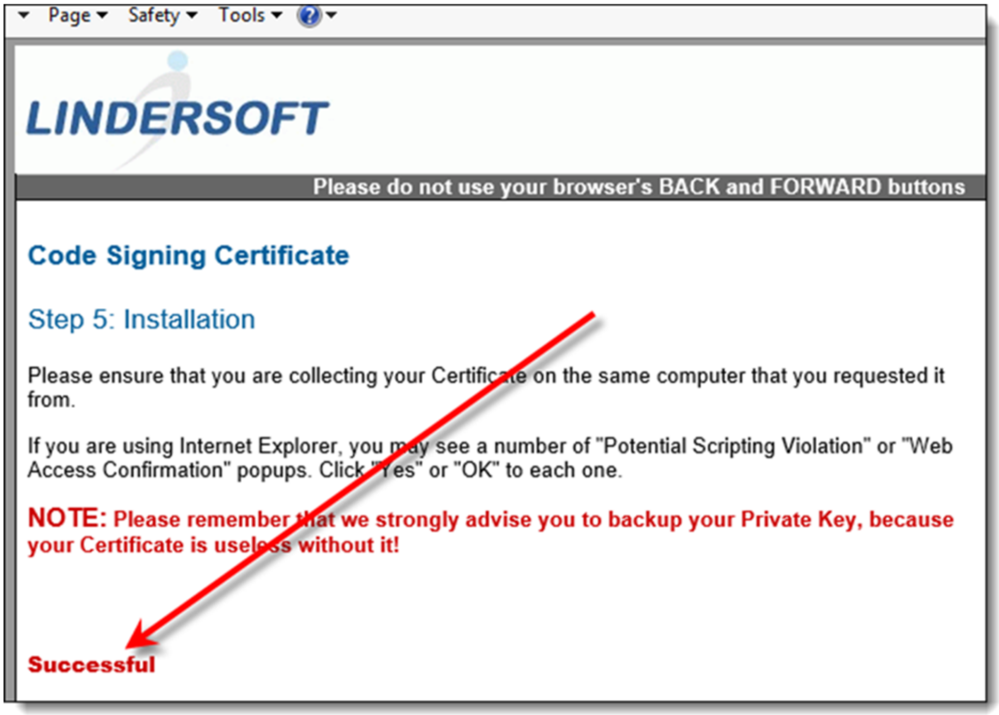
Enter your Collection Code: [redacted]



This Web site is attempting to perform a digital certificate operation on your behalf:

https://secure.comodo.net/products/InstallCodeSigningCert

You should only allow known Web sites to perform digital certificate operations on your behalf.
Do you want to allow this operation?



Code Signing Certificate

Step 5: Installation

Please ensure that you are collecting your Certificate on the same computer that you requested it from.

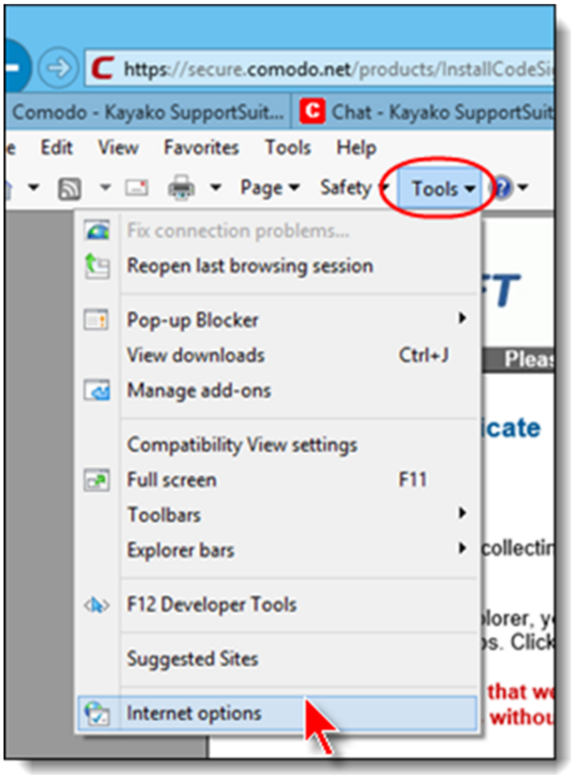
If you are using Internet Explorer, you may see a number of "Potential Scripting Violation" or "Web Access Confirmation" popups. Click "Yes" or "OK" to each one.

NOTE: Please remember that we strongly advise you to backup your Private Key, because your Certificate is useless without it!

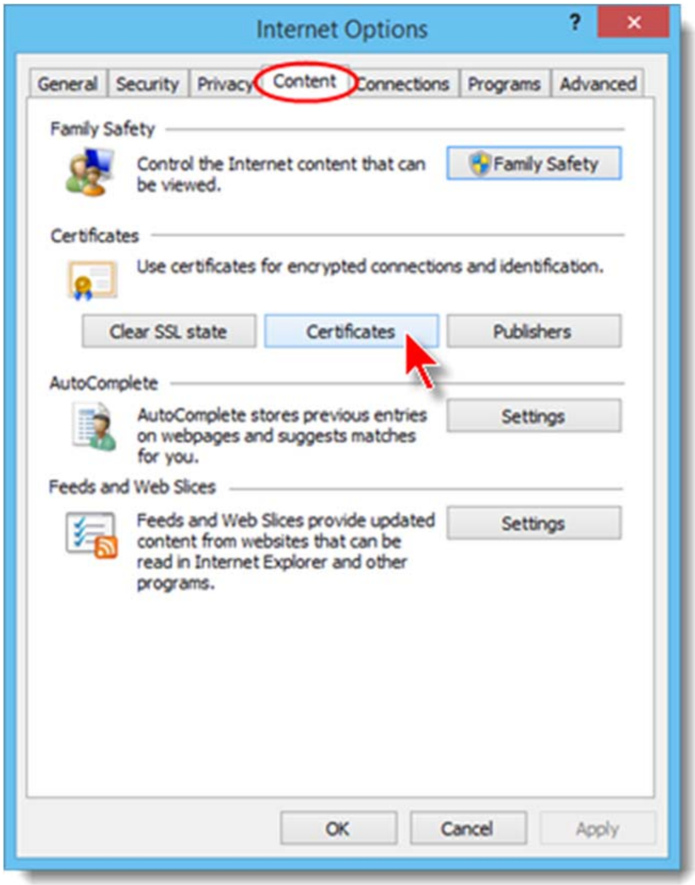
Successful

After the certificate downloaded into Windows, the next task was to export it to a file that I can back up and use with SetupBuilder or with batch files in my development environment.

Within IE, **Tools** then **Internet options** to begin.


https://secure.comodo.net/products/InstallCodeSi
Comodo - Kayako SupportSuit...
Chat - Kayako SupportSuit
Edit
View
Favorites
Tools
Help
Page
Safety
Tools
Fix connection problems...
Reopen last browsing session
Pop-up Blocker
View downloads Ctrl+J
Manage add-ons
Compatibility View settings
Full screen F11
Toolbars
Explorer bars
F12 Developer Tools
Suggested Sites
Internet options

Then click the **Content** tab, and the **Certificates** button.



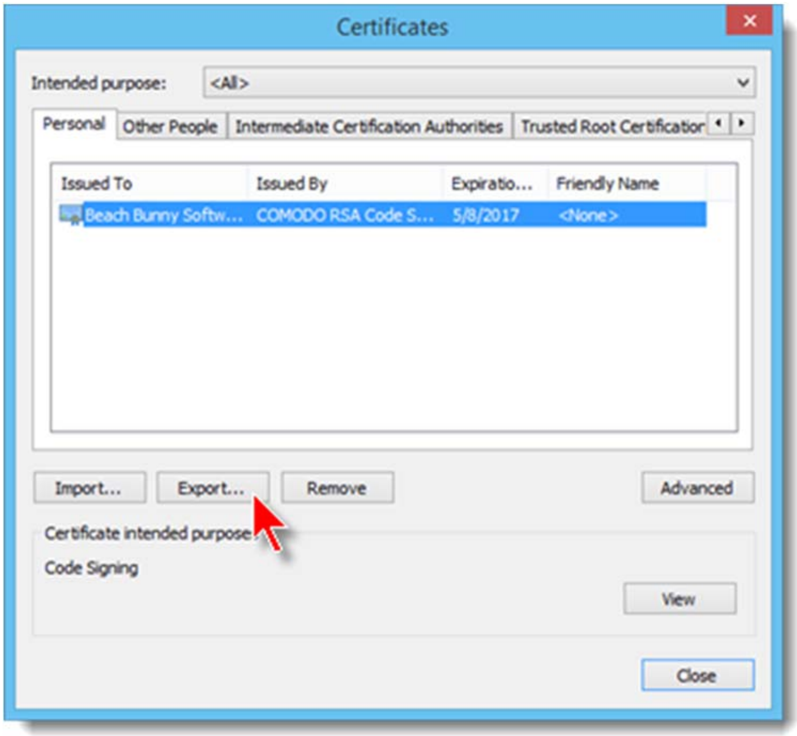
Control the Internet content that can be viewed.

Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

Highlight my lovely new certificate and click **Export**.



Certificates

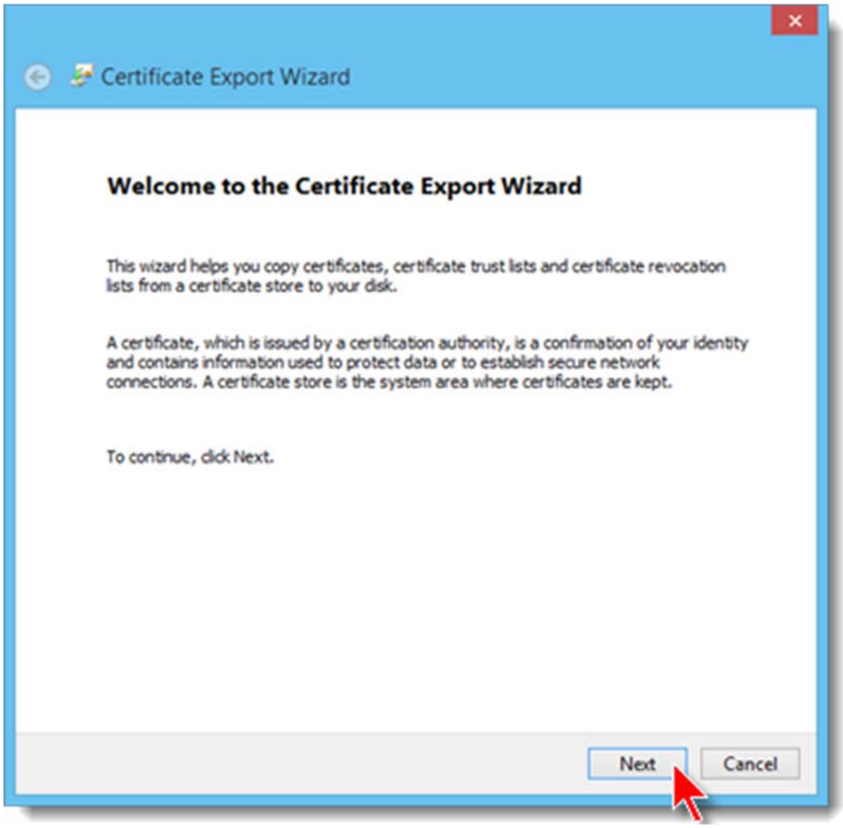
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Beach Bunny Softw...	COMODO RSA Code S...	5/8/2017	<None>

Certificate intended purposes

Code Signing

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Import...
Export...
Remove
Advanced
View
Close



Certificate Export Wizard

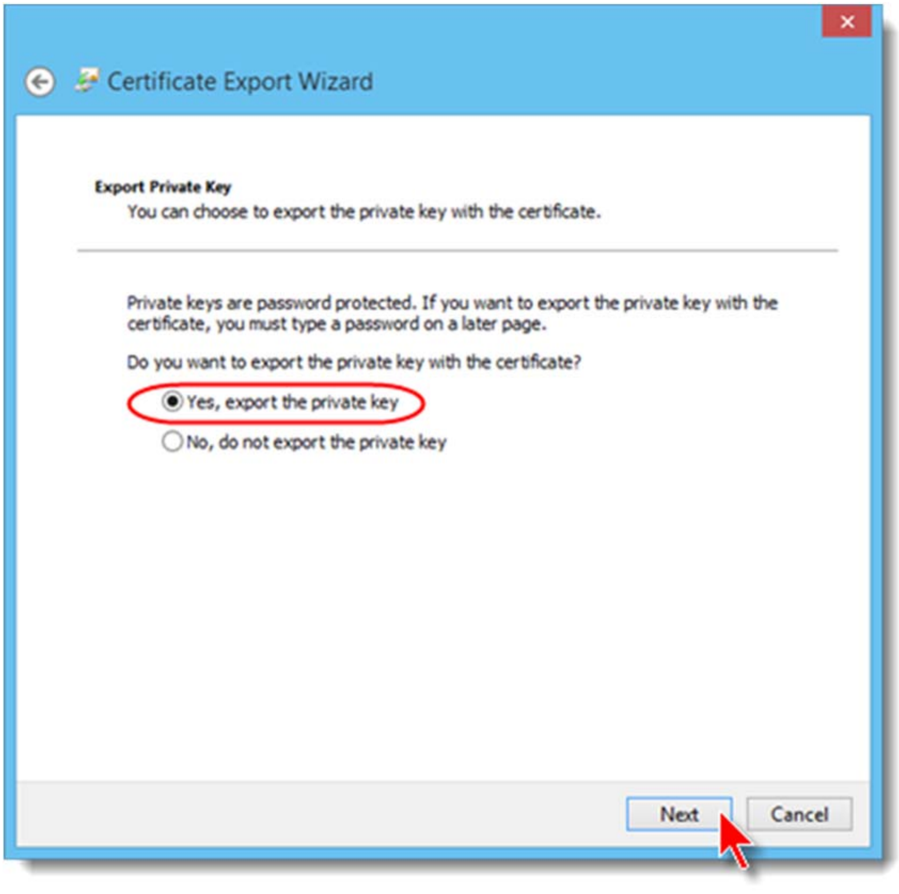
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Yes, I want to export the private key.



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

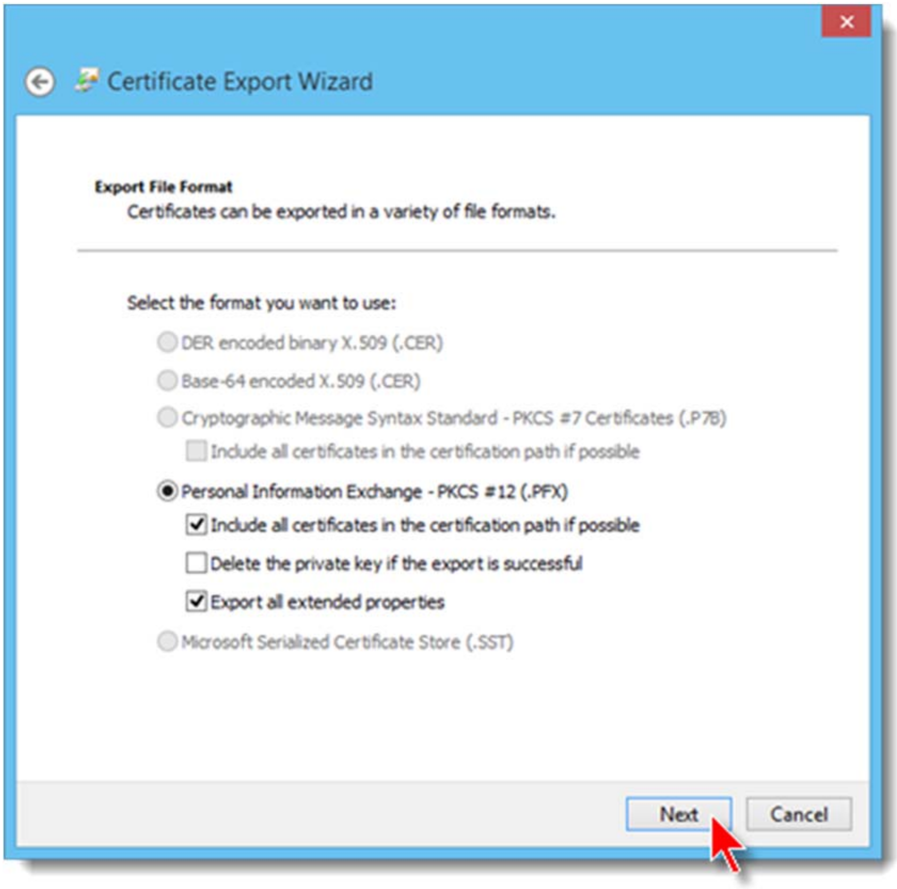
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

I do NOT want to delete the private key from its crypto hiding place on this machine.


Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

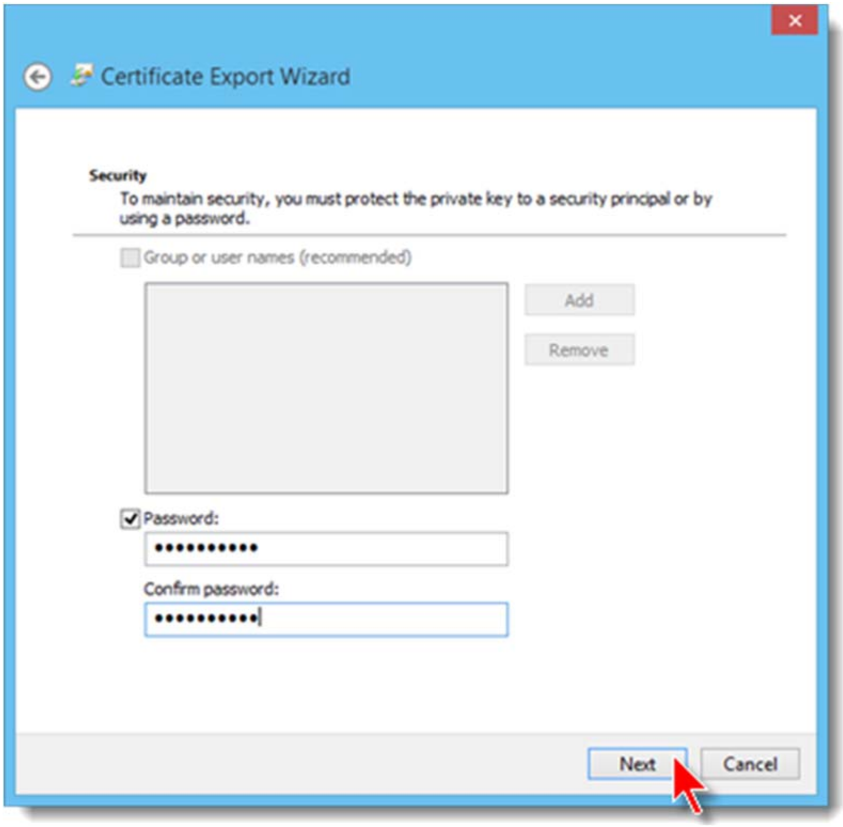
☑ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

☑ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

This is the password for this PFX file I'm creating – not the password I used when ordering the certificate.


Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

□ Group or user names (recommended)

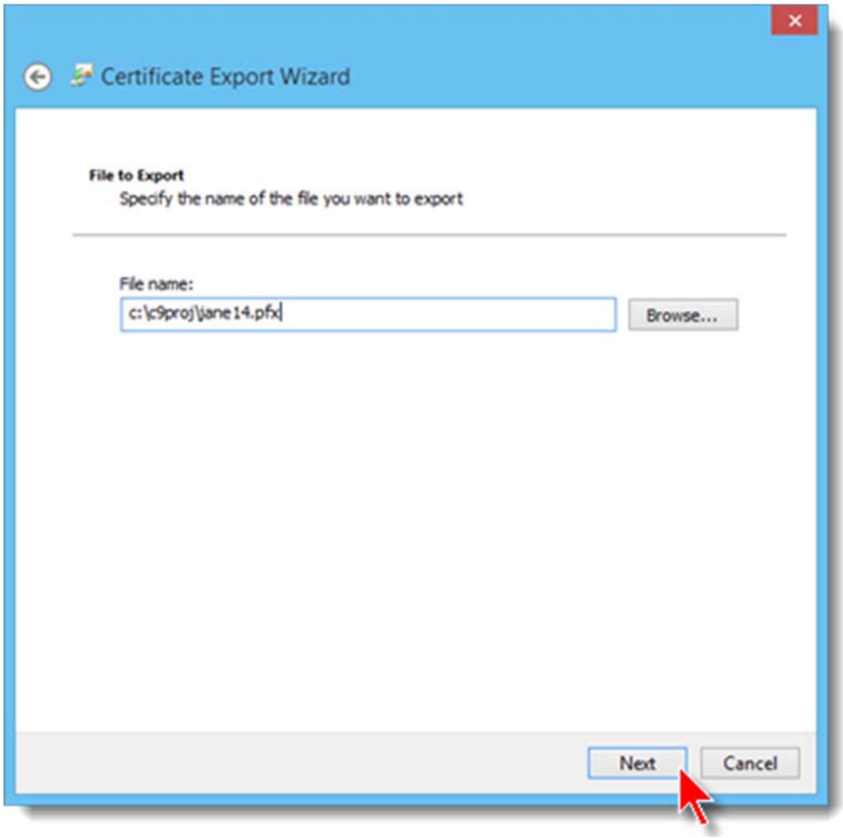
☑ Password:

••••••••••

Confirm password:

••••••••••

File name for the PFX file I'm creating.



Certificate Export Wizard

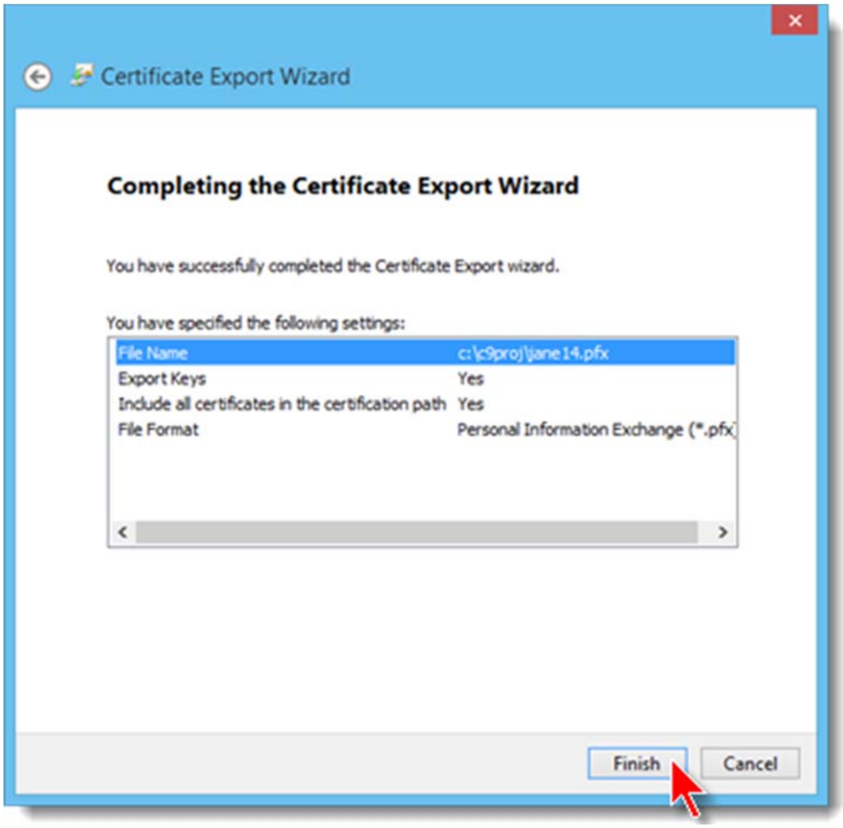
File to Export

Specify the name of the file you want to export

File name:

c:\c9proj\jane14.pfx

Confirm.



Certificate Export Wizard

Completing the Certificate Export Wizard

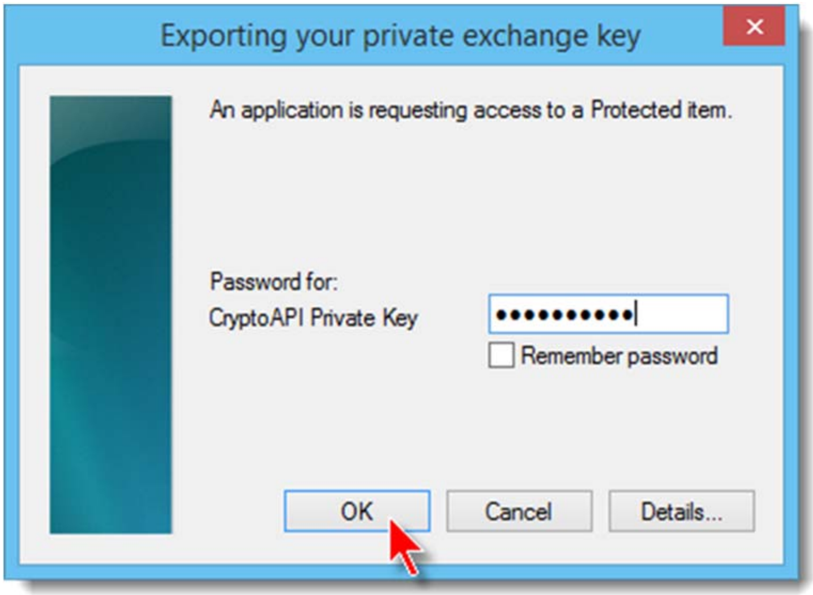
You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	c:\c9proj\jane14.pfx
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal Information Exchange (*.pfx)

But wait… remember that password I created when I was ordering the certificate?

Need to enter that now to complete the PFX file export.

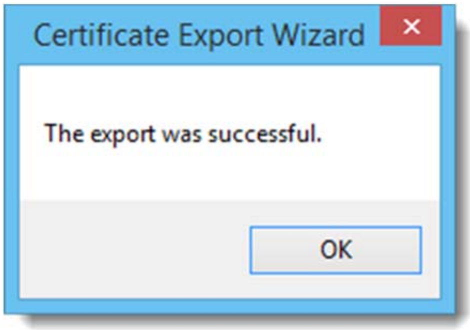


Exporting your private exchange key

An application is requesting access to a Protected item.

Password for:
CryptoAPI Private Key ●●●●●●●●●●●

□ Remember password



Certificate Export Wizard

The export was successful.

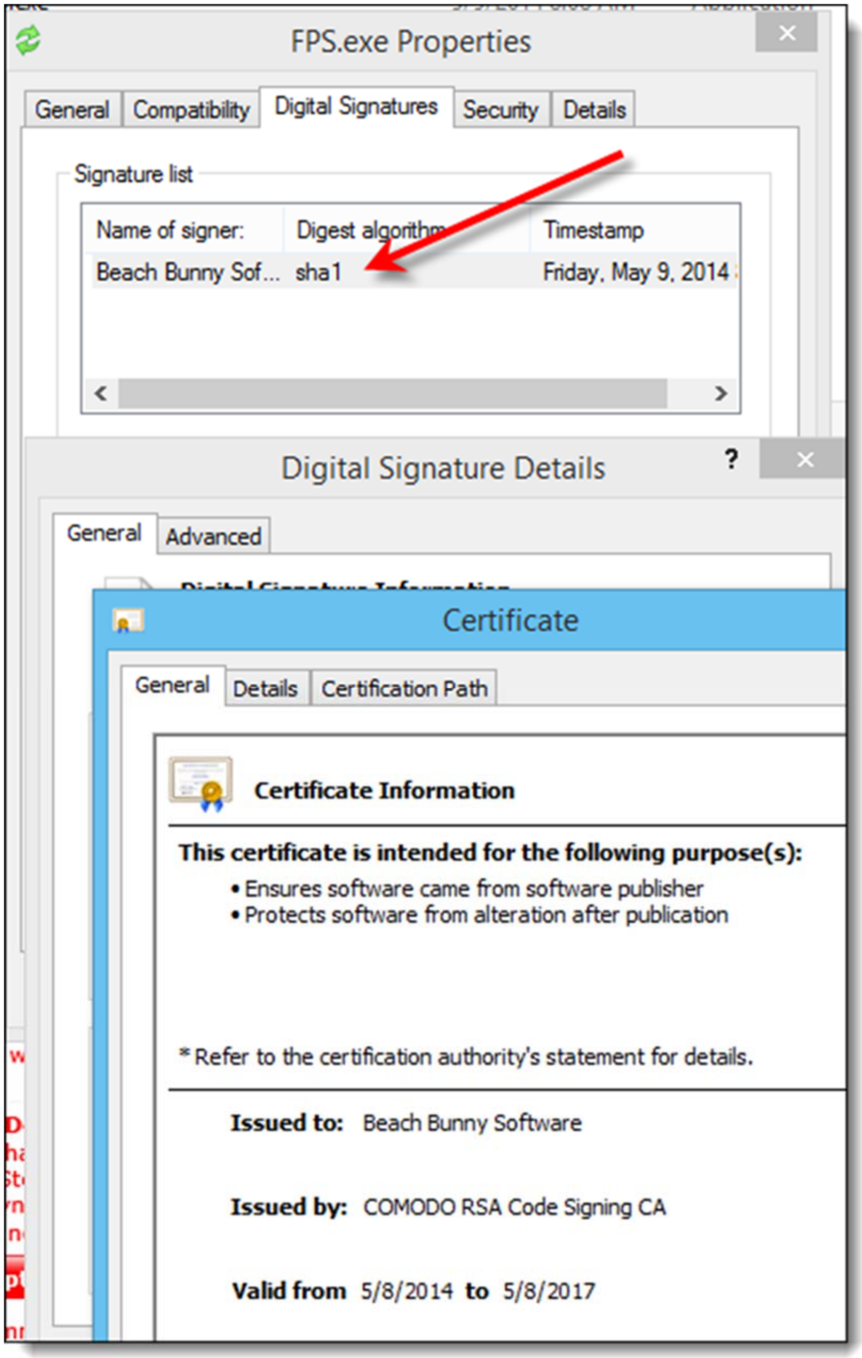
Well, that was easy. Now to start blasting out SHA-2 signatures.

But how will I tell?

I've found two ways. I think.
It turns out that Windows 8.x shows more information on the digital signature part of Program Properties than I've seen in Windows 7 or earlier.

And you can also use signtool to show the signature properties.

My first effort led me to think I'd somehow specified the wrong certificate parameters after all.
The exe I signed with the new certificate showed "sha 1".



Name of signer:	Digest algorithm	Timestamp
Beach Bunny Sof...	sha1	Friday, May 9, 2014

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Beach Bunny Software

Issued by: COMODO RSA Code Signing CA

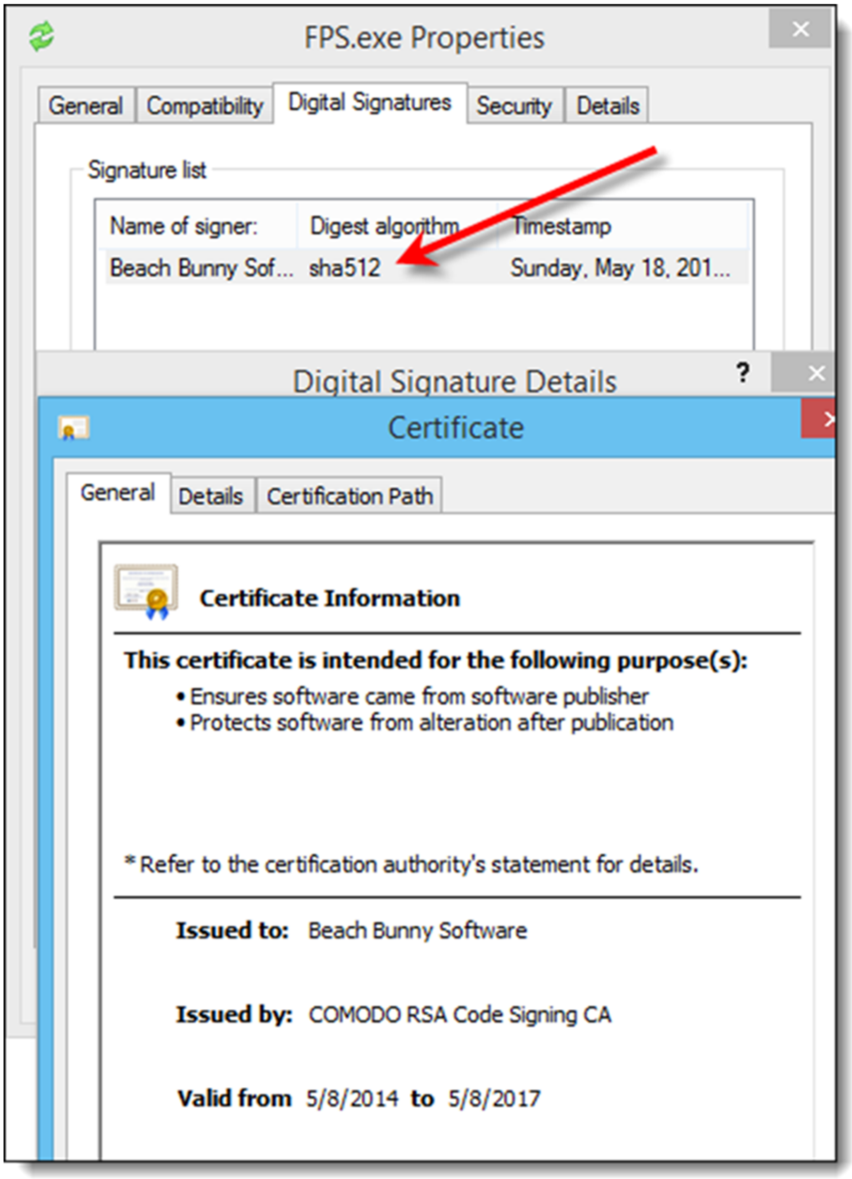
Valid from 5/8/2014 **to** 5/8/2017

Apparently, signtool happily defaults to SHA-1.

You don't actually tell it to use SHA-2 per se. Rather, you specify a longer key length. (Quoth Wikipedia, "SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256) designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS).")

So using the /fd switch with signtool, I specified SHA512.

Et voilà…



Name of signer:	Digest algorithm	Timestamp
Beach Bunny Sof...	sha512	Sunday, May 18, 201...

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Beach Bunny Software

Issued by: COMODO RSA Code Signing CA

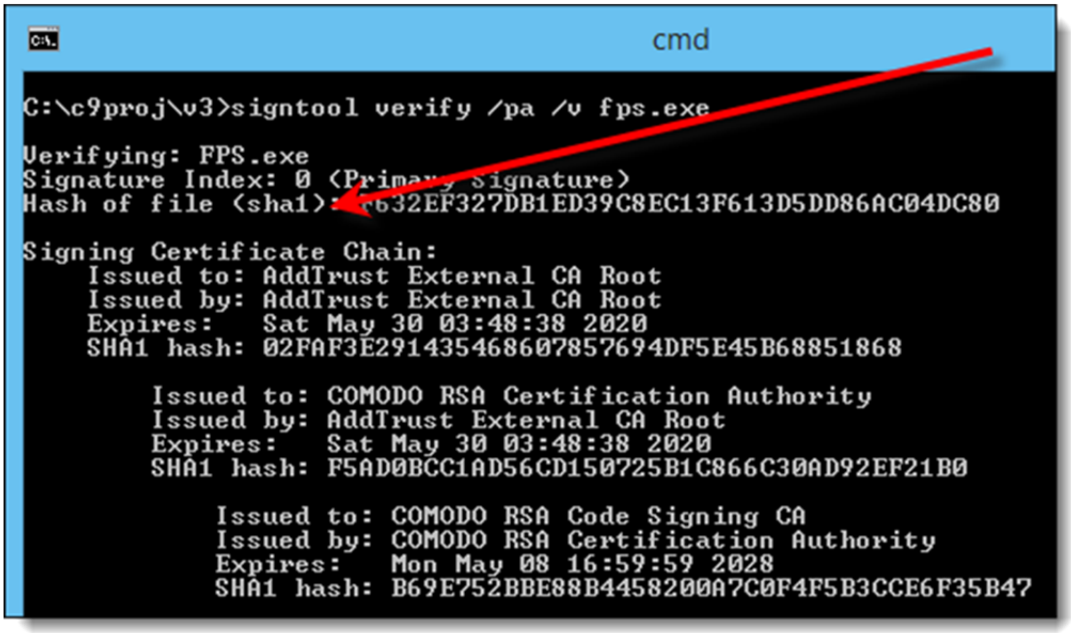
Valid from 5/8/2014 **to** 5/8/2017

This DOES seem to require a reasonably current version of signtool.exe.
I tried using the /fd switch with the 2006 vintage version of signtool that I had on one of my machines and it kicked sand in my face.

To check a file using signtool, run

```
signtool verify /pa /v FileNameToBeChecked
```

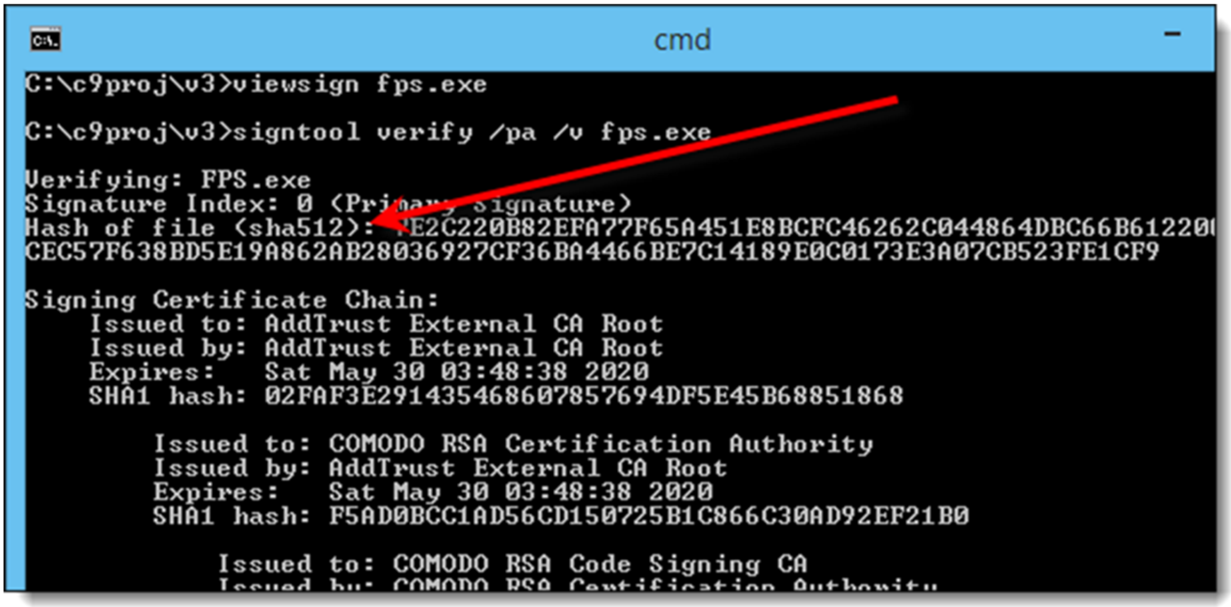
This shows my app signed without specifying the key length to use:



```
C:\c9proj\v3>signtool verify /pa /v fps.exe

Verifying: FPS.exe
Signature Index: 0 (Primary Signature)
Hash of file (sha1): [illegible]632EF327DB1ED39C8EC13F613D5DD86AC04DC80

Signing Certificate Chain:
    Issued to: AddTrust External CA Root
    Issued by: AddTrust External CA Root
    Expires:   Sat May 30 03:48:38 2020
    SHA1 hash: 02FAF3E291435468607857694DF5E45B68851868

        Issued to: COMODO RSA Certification Authority
        Issued by: AddTrust External CA Root
        Expires:   Sat May 30 03:48:38 2020
        SHA1 hash: F5AD0BCC1AD56CD150725B1C866C30AD92EF21B0

            Issued to: COMODO RSA Code Signing CA
            Issued by: COMODO RSA Certification Authority
            Expires:   Mon May 08 16:59:59 2028
            SHA1 hash: B69E752BBE88B4458200A7C0F4F5B3CCE6F35B47
```

And this shows the same app when it’s been signed using

```
/fd SHA512
```



```
C:\c9proj\v3>viewsign fps.exe

C:\c9proj\v3>signtool verify /pa /v fps.exe

Verifying: FPS.exe
Signature Index: 0 (Primary Signature)
Hash of file (sha512): [illegible]E2C220B82EFA77F65A451E8BCFC46262C044864DBC66B61220
CEC57F638BD5E19A862AB28036927CF36BA4466BE7C14189E0C0173E3A07CB523FE1CF9

Signing Certificate Chain:
    Issued to: AddTrust External CA Root
    Issued by: AddTrust External CA Root
    Expires:   Sat May 30 03:48:38 2020
    SHA1 hash: 02FAF3E291435468607857694DF5E45B68851868

        Issued to: COMODO RSA Certification Authority
        Issued by: AddTrust External CA Root
        Expires:   Sat May 30 03:48:38 2020
        SHA1 hash: F5AD0BCC1AD56CD150725B1C866C30AD92EF21B0

            Issued to: COMODO RSA Code Signing CA
            Issued by: COMODO RSA Certification Authority
```