# *Frequently Asked Questions For CAISO Digital Certificates*

# Contents

# Questions

## Question #1: How can I get a new CAISO digital certificate?

The instructions for registering for a new CAISO digital certificate are located here:

http://www.caiso.com/Documents/InstructionsForRegisteringForYourNewDigitalCertificate.pdf

## Question #2: My certificate has expired. How do I get a new one?

The instructions for renewing your CAISO digital certificate are located here:

http://www.caiso.com/Documents/InstructionsForRenewingYourDigitalCertificate.pdf

## Question #3: I lost my certificate or changed computers. How do I get a new one?

If you followed the certificate installation instructions you should have created a back-up. For details see:

http://www.caiso.com/Documents/Instructions-SavingCopy-Certificate-WindowsXP.pdf

http://www.caiso.com/Documents/Instructions-SavingCopy-Certificate-Windows7.pdf

If you cannot locate the certificate and it cannot be recovered by your information technology staff, contact our support desk at HelpDesk@caiso.com or (888) 889-0450. You will receive an email with instructions and an incident number to input on the registration website in Common Name Field followed by the certificate name. See example registration on the following page.

## Question #4: I don't know the passphrase to download a certificate, so what should I do?

If you cannot remember the passphrase you entered when you registered for your certificate, contact our support desk at HelpDesk@caiso.com or (888) 889-0450. You will receive an email with instructions and an incident number to input on the registration website

## Question #5: I requested/renewed my certificate and I haven't received it, where is it?
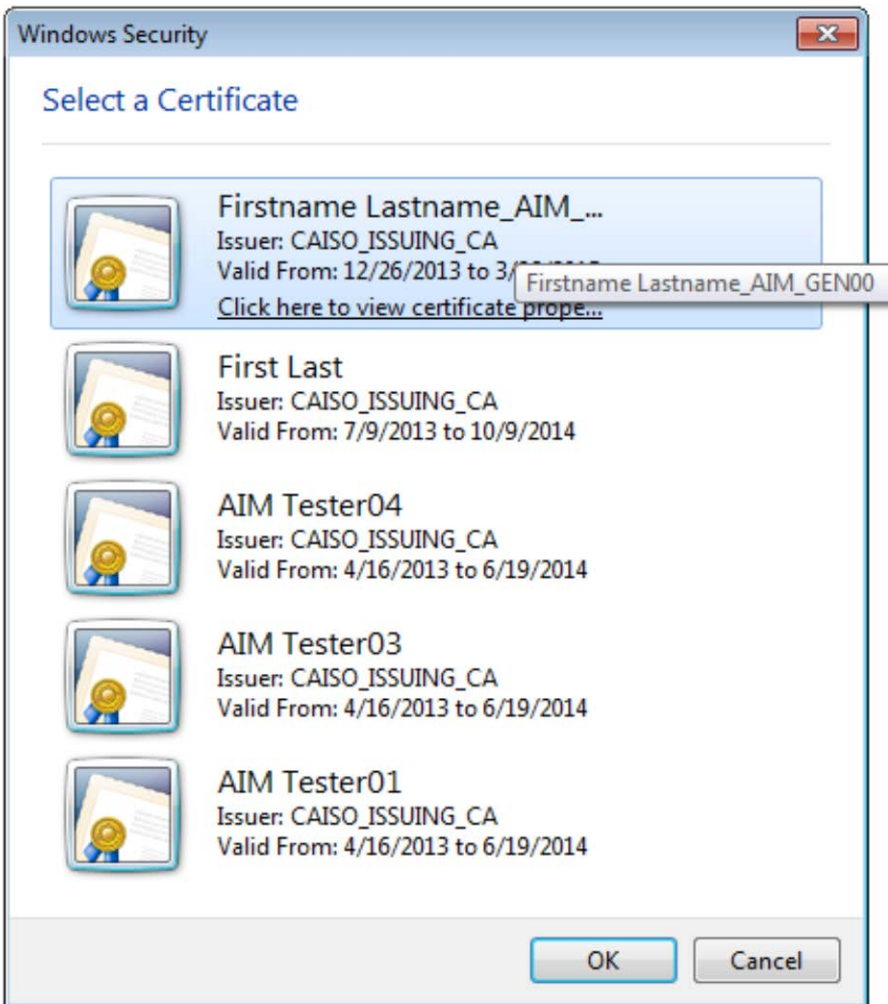
First, you must register for your certificate—see the answers to Question #1 and Question #2. Then, your registration must be validated and you should receive an email with instructions on how to receive your certificate from "do-not-reply@verizon.com" within two business days after you register. You should add "do-not-reply@verizon.com" to your email Safe Senders

List. 3 Check your junk email folder and search for the email. If you did not receive it or cannot locate it, contact our support desk at HelpDesk@caiso.com or (888) 889-0450.

**Question #6: Certificate names are truncated in the Select a Certificate pop-up window. How do I view the full names of my certificates?**

To see the full name on a certificate in the Select a Certificate pop-up window when accessing CAISO systems, just hover the mouse over the truncated name and the full name will appear, or click the "Click here to view certificate properties" link under the certificate.

Example Pop-up Window:

**Certificate registration issues using the Cybertrust website**
**Error #1**

*A message appears during the registration processes indicating, "The period between start/end is greater than the span allowed in the policy"*



**Certificate Request**

**CMA Certificate**

| | |
|---|---|
| Common Name | |
| Not After * | 7/21/2016 8:52 AM |
| Maximum Span | 15 months |
| Email Address | |
| Key Algorithm | RSA |
| Pickup Passphrase | •••••••• |
| Pickup Passphrase Confirmation | •••••••• |

**Messages**

The period between start/end is greater than the span allowed in the policy.

Submit

\* Dates should be in the format: **M/d/yyyy h:mm a**
The current date and time is: 4/21/2015 8:52 AM

**Potential Cause #1**

This is a known issues during time changes throughout the year (**spring, fall**).

**Solution**

A change to the not after date by adding **one day** should enable the user to complete the registration process.
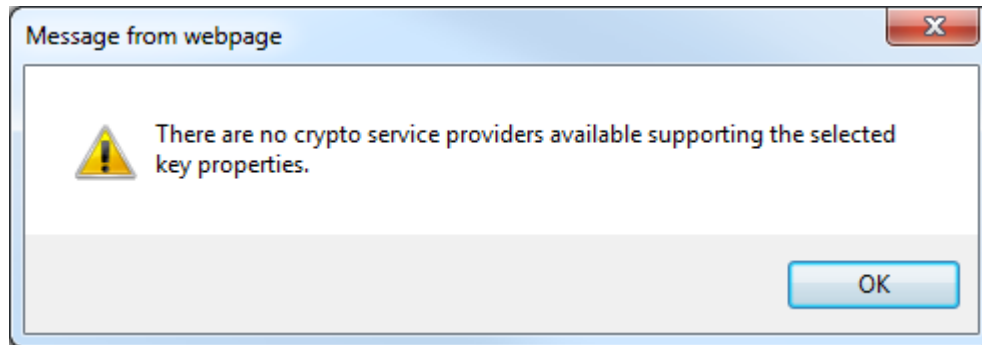
**Potential Cause #2**

The user leaves the website open for an extended period of time or tries to refresh the session.

**Solution**

Log off and clear the cache/cookies from browser. Restart the session and retry.

### Error #2

*During the registration process, the user receives a message from the webpage indicating, "There are no crypto service providers available supporting the selected key properties"*
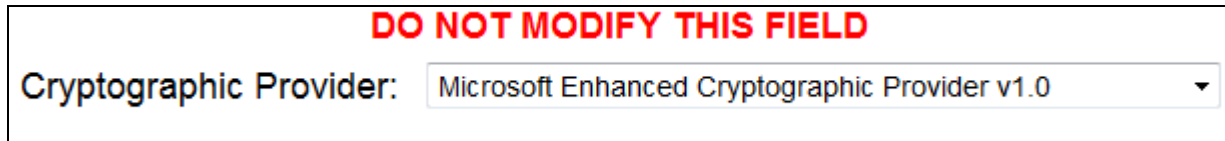


### Potential Cause #1

This is a known issue with Internet Explorer.

### Solution#1

If the user is using Internet explorer, instruct the user to select the Microsoft Enhanced Cryptographic Provider v1.0



### Potential Cause #2

The user either does not have a Crypto Service Provider (**CSP**) running on their machine or does not have a provider supported by the Cybertrust website.

### Solution#2

Ask the user to consult their internal IT department or Windows Administrator.

Location:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\

The regedit utility can be used to discovery the key: Select the Start menu>Type regedit in Search programs and files>Press the Enter key>Go to the key above>"Microsoft Base Cryptographic Provider v1.0" should be listed at or near the top

**Certificate collection issues using the Cyber Trust website**

**Error #3**

*User states that the website freezes while trying to download the certificate.*



**Potential Cause**

The user is using a browser that is not supported by the Cybertrust website or there are intermittent connection issues between the site and the user.

**Solution**

The Cybertrust website supports Internet Explorer version 9 or below as well as Firefox Mozilla. A new session is recommended.

**Error #4**

*While trying to retrieve the certificate, the user enters the Transaction ID and Collection passphrase and received an error message which states, "The passphrase you entered was incorrect.*



**Potential Cause**

- The user may have CAPS or Num Lock on.

- The passphrase was entered incorrectly.

- The cybertrust website does not recognize the character entered or the passphrase was copied and pasted with hidden spaces.
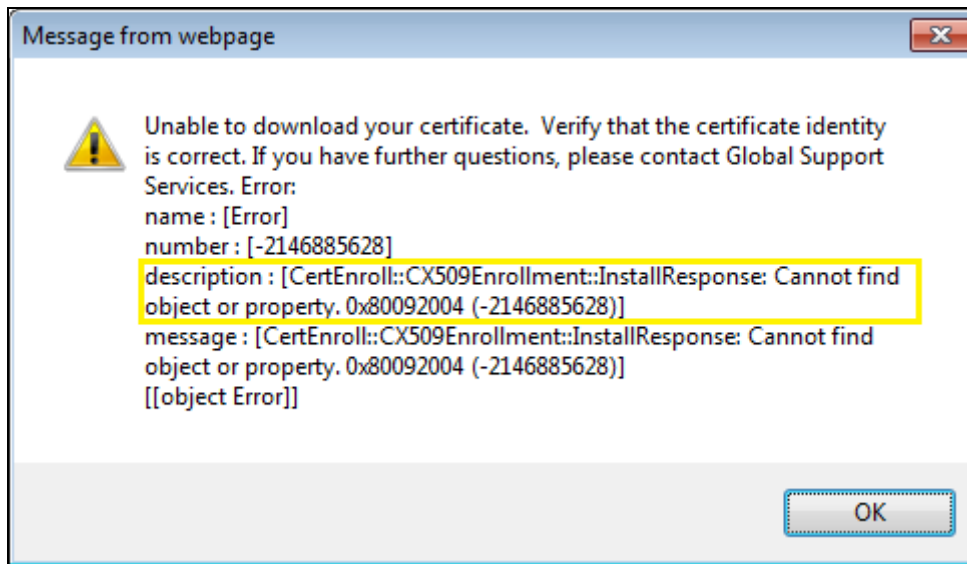
**Solution**

Verify the passphrase was entered manually on a notepad or text-edit before entering on the cybertrust website to verify the passphrase is correct since it's masked on the cybertrust website.

If the problem persists, create a ticket and send a new registration notice.

## Error #5

*The user receives a message from webpage while trying to <u>save the certificate in their browser</u> [download] indicating, "Install response: Cannot find object or property"*



## Potential Cause

The user is trying to download the certificate from a different computer than the one in which the certificate was originally registered on.

## Solution

Ask the user to try downloading the certificate from the same computer it was registered on.

## Potential Cause #2

The user is trying to download the certificate more than once

## Solution

The certificate can only be downloaded once.  If the user requires a copy of the certificate to use on a separate machine, direct them to the external website http://www.caiso.com/participate/Pages/ApplicationAccess/Default.aspx under sections: ISO System access>Application access request forms and application installation instructions> certificate installation instructions.

If the user never retrieved the certificate or cannot locate it, create a ticket and send out another registration notice.  CC: Certificate Requests

## Error #6

*The user is unable to download the certificate due to a message from the webpage indicating, "A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider"*



### Potential Cause

The root chain is not installed in the user's browser.

### Solution

Ask the user to follow the step 1. Listed on the collection notice.

**NOTE**: California ISO updated its certificate Trust chain between June 1st 2015 and June 17th 2015.  Please ensure the new chain has been installed.

The new chain can be found here:
http://www.caiso.com/Documents/SHA-2CyberTrustCAISO_Issuing_CA_TrustChainPKCS7.p7c

## Error #7

*The user is unable to download the certificate or register due to a long running script.*

## Potential Cause

The user is accessing the Cybertrust website using Internet Explorer 11.
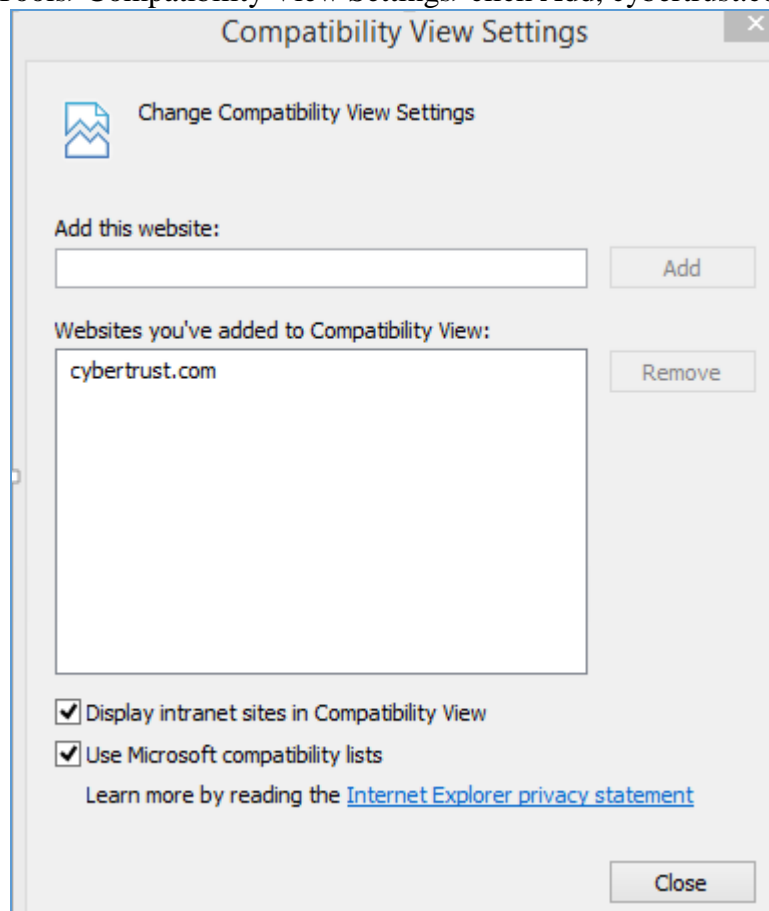
## Solution

Cybertrust does not currently support IE 11.  Ask the user to consult their internal IT department and downgrade to IE 10 or lower.

## Solution #2

As an interim fix, ask the user to complete the following steps:

1. In IE 11, click Tools>Compatibility View Settings>click Add, cybertrust.com



Next page>

2. Click Tools>Internet Options>Security>Trusted Sites>Sites, and add https://web.idm.cybertrust.com (see below)

Trusted Sites

**Trusted sites** ✕

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

`https://web.idm.cybertrust.com`    **Add**

Websites:

```
*.1800flowers.com
*.akamai.net
*.bombardier.com
*.centurylink.com
*._____.___
```

**Remove**

☐ Require server verification (https:) for all sites in this zone

**Close**