How to Install DADDS Certificate so it is Recognized by LRGS Java

The Problem:

If your LRGS is configured to do PDT validation, it will try to download the latest PDT and channel file from DADDS.

This is enabled with the following "lrgs.conf" settings:

```
doPdtValidation=true
channelMapUrl=https://dcs1.noaa.gov/chans_by_baud.txt
pdtUrl=https://dcs1.noaa.gov/pdts_compressed.txt
```

As of October 2011, DADDS is using a Verisign Class 3 Certificate Authority which is not recognized by a Java. Thus when LRGS tries to download the PDT and CDT files from the above URLs, it will fail. You will see a message in lrgslog like this:

```
WARNING 2011/11/15-16:53:47 Cannot download PDT from
'https://dcs1.noaa.gov/pdts_compressed.txt': javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification
path to requested target
```

To get this to work, we must add the Certificate Authority to the trusted list used by Java.

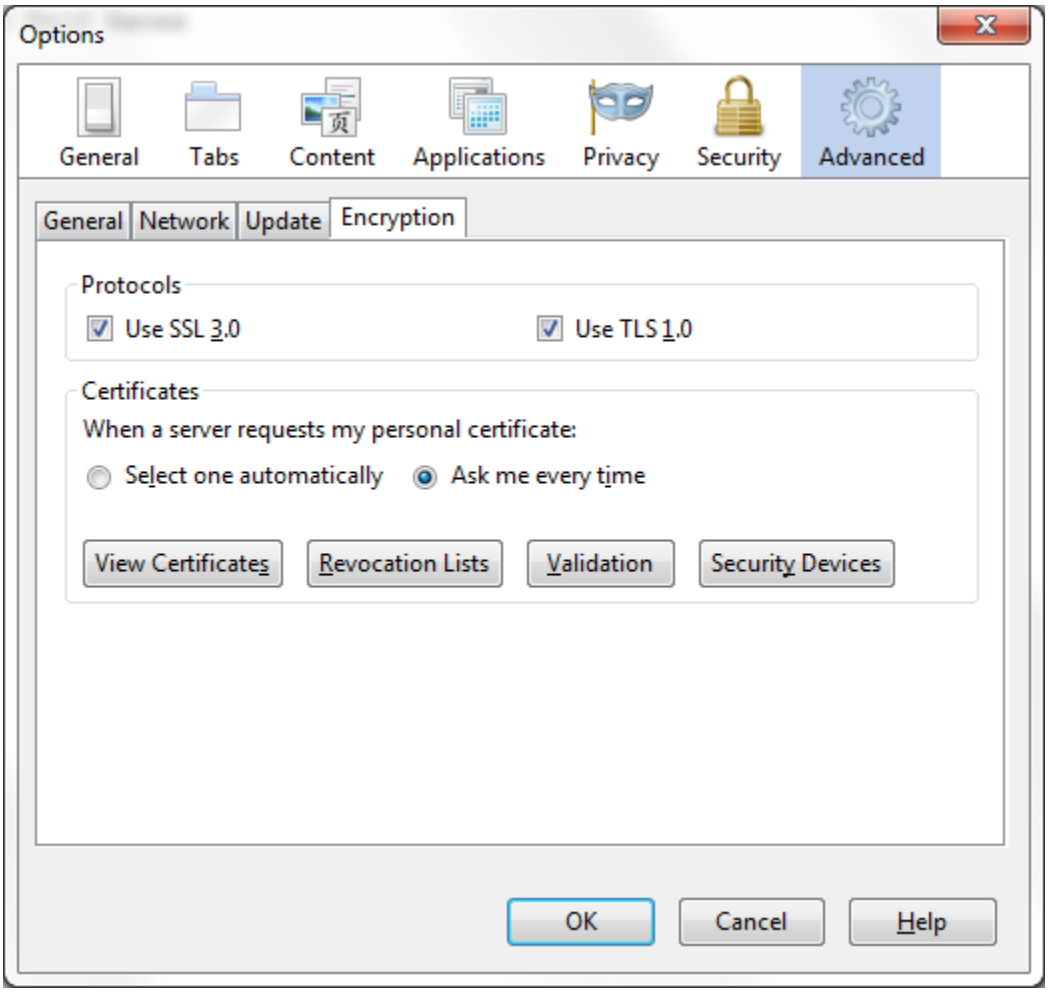
Step 1: Get the Certificate

The certificate must be stored as a binary "DER" file. We have saved it for you. Download it from:

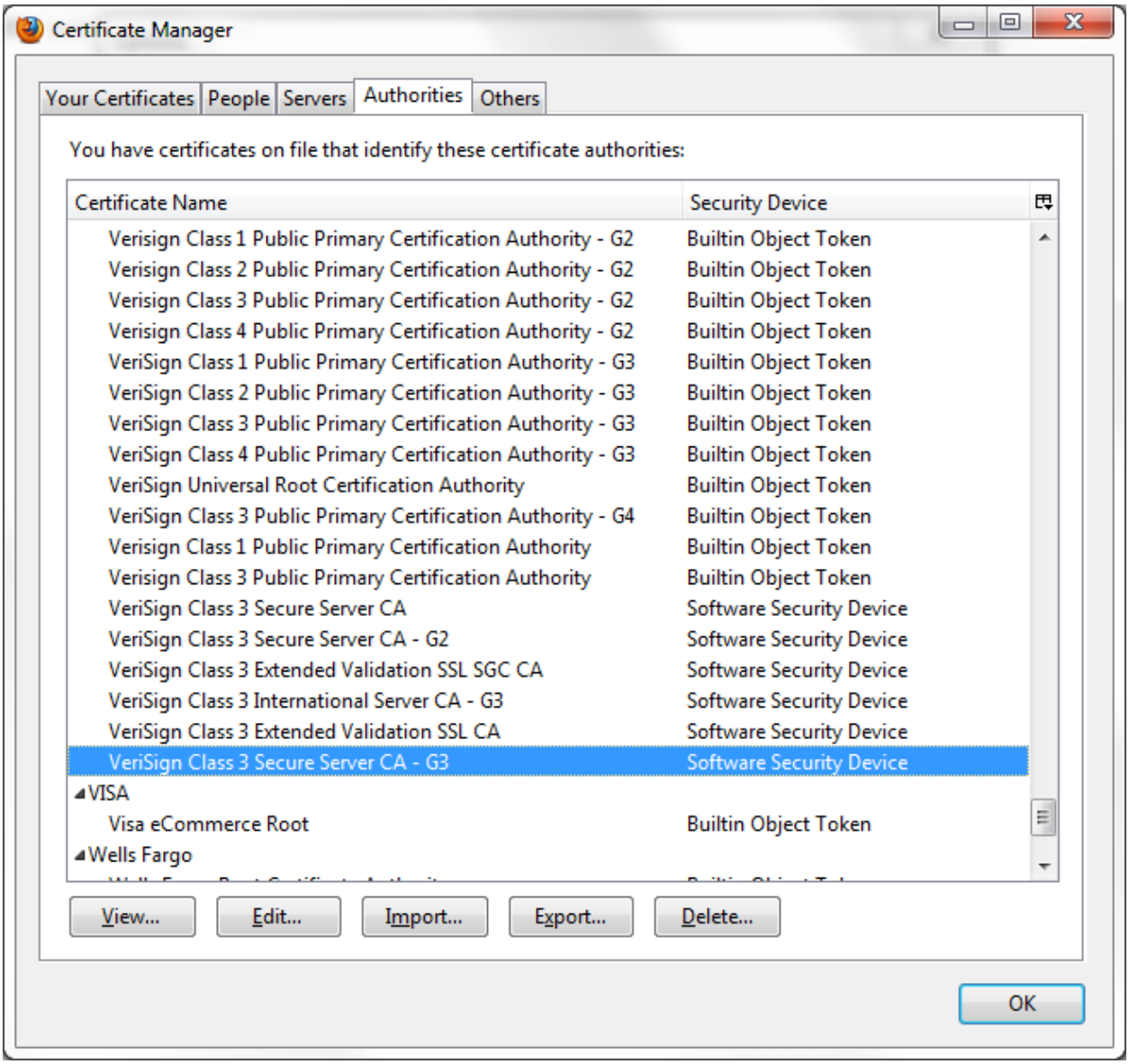
http://www.ilexengineering.com/download/VeriSignClass3SecureServerCA-G3.der

Or … you could export it from your browser like this:

- In firefox, go to one of the dcs1 URLs listed above. Accept the certificate if you get an exception.
- Go to the options dialog, Advanced Tab:



Click View Certificates, Authorities Tab, Find the indicated certificate and click Export… at the bottom:



For type, select X.509 Certificate (DER) and save the file.

Step 2: Install the Certificate into Java's Keystore

You must be logged-in or su'ed to root to do this on a unix/linux system.

Go to the 'bin' directory under your JRE distribution. For example, on a linux system:

```
cd /usr/java/latest/jre/bin
```

List the existing Certificate-Authorities like this:

```
./keytool -list -keystore ../lib/security/cacerts
```

When it asks you for the password, type "changeit".

Now suppose you saved the DER certificate in the /tmp directory on that machine. The command to add this to Java's keystore is:

```
./keytool -import -keystore ../lib/security/cacerts -file /tmp/VeriSignClass3SecureServerCA-G3.der
```

Likewise, when it asks for the keystore password, type "changeit".

When it asks if you want to trust this certificate, type "yes".

Now, as user "lrgs" stop and the re-start the LRGS server. Watch the log file to ensure that the pdt download was successful. This will happen shortly after the restart.