

Ref: *U.S. Department of Commerce IT Security Program Policy and Minimum Implementation Standards*, revised 30 June 2005.

On the Web:

http://ocio.os.doc.gov/ITPolicyandPrograms/Policy___Standards/DEV01_003884#P2653_262381

Background: What is SSL and why are we using it?

Secure Sockets Layer (SSL) technology (and its modern incarnation, the Transport Security Layer [TSL]) is an industry-wide standard which protects Web servers and enables trust in Web site visitors. In short, *SSL/TSL is the way we implement secure communications on the Web*.

One can determine when SSL is in use by the form of Web address. When the Web address begins with ‘https:’, SSL is in use and information is sent and received in an encrypted form. When the Web address begins with ‘http:’, SSL is **not** in use and all information sent between the Web browser and Web server are sent ‘in the clear’; that is, unencrypted.

SSL provides security for Web sessions in three ways:

1. An SSL Certificate enables **encryption** of sensitive information during online transactions.
2. Each SSL Certificate contains unique, **authenticated** information about the certificate owner.
3. A Certificate Authority **verifies** the identity of the certificate owner when it is issued.

Why does the PMN data entry site use SSL?

1. To comply with DOC and NOAA IT security policies.
2. PMN is an *authenticated* site—it requires a username and password combination to log in. Transmission of user credentials *requires* that they be encrypted.

Encryption

Encryption ‘scrambles’ data before it is sent across some medium—in our case, the series of tubes known as the Internet—so that persons who are not authorized to access the data may not intercept it during transmission. Encryption is really a two-part process: the data are scrambled before sending, and unscrambled upon receipt. In order to unscramble the data on the receiving end, the receiver must know how the data were scrambled; that is, the receiver must know the key that was used to perform the encryption. This is where the security certificate comes in.

Authentication

Each security certificate contains two encryption keys, a *public key* and a *private key*. The public key is used to encrypt the information and the private key is used to decipher it. When a Web browser points to a secure server, the SSL ‘handshake’ authenticates both the server (the Web site) and the client (the Web browser), using the certificate provided by the Web server.

The certificate also contains identifying information about the server, which may then be matched against information contained within the HTTPS response packets to ensure that information is indeed coming from the location described in the certificate.

Verification

It is not enough to simply provide a security certificate when hosting a secure Web site. Security certificates can be forged to fool a Web browser into thinking it is accessing a valid secure site.

For instance, consider a bank which provides on-line banking services. A ‘phisher’ could forge a bank’s certificate and redirect Web browser traffic to the phisher’s own Web server and use the impostor site to collect personal information about the bank’s customers and use that information to commit identity theft or other crimes.

To prevent this scenario from occurring a certificate should be issued and hosted by a third-party Certificate Authority, which verifies and validates the contents of a security certificate and provides assurance that the certificate (and, equally importantly, the certificate issuer) are genuine.

Well, two out of three ain’t bad!

Unfortunately, NCDDC (and NOAA generally) provide the certificates and the encryption, but at present there is no third-party certificate authority involved—our certificates are ‘self-signed’, which violates the verification aspect of the certificate. As a result, when a browser is pointed at the PMN data entry site, a warning of some sort may be displayed, depending on the browser.

The next section will discuss certificate warnings and ways to handle them using four specific browsers as examples.

Firefox Version 2

Firefox 2 displays a warning dialog (Figure 1) which gives the user the option to accept a certificate permanently, temporarily or not at all. We recommend accepting the certificate **temporarily**. The reason for this is if the user accepts the certificate permanently, Firefox will store the certificate in its local certificate database. If the

certificate changes at the server end, *Firefox will actively prevent the user from continuing to the site unless the certificate is manually deleted.* Why? Because the certificates don't match, and Firefox will conclude that the new certificate may be forged. The only way to continue is to delete the stored certificate.



Figure 1. Firefox 2 certificate warning.

To manually delete a certificate in Firefox 2:

1. Select 'Tools -> Options -> Advanced -> Encryption' (Figure 2).

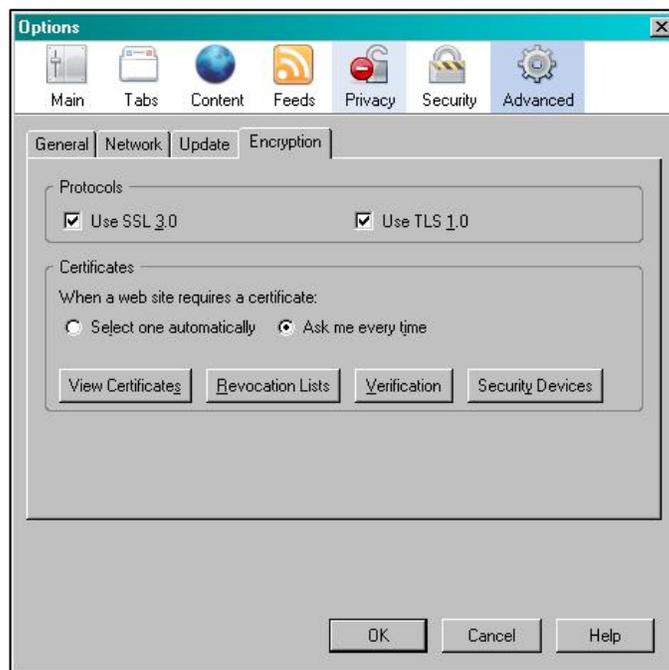


Figure 2. Firefox 2 Options dialog.

2. Select the 'View Certificates' button.
3. In the Certificates Manager dialog, select the 'Web Sites' tab.
4. Scroll down until you see the 'NOAA' group. If there is a plus sign ('+') next to the NOAA group, expand the group by clicking on the plus sign. The view should be similar to that shown in Figure 3.

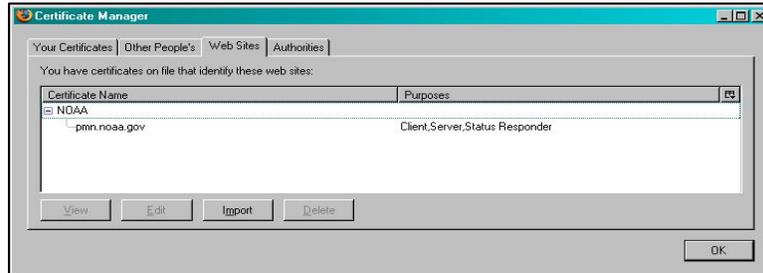


Figure 3. Firefox 2 Certificate Manager.

5. Select the 'pmn.noaa.gov' certificate.
6. Select the 'Delete' button. You will be prompted to confirm the certificate deletion; select the 'OK' button to do so.

Firefox Version 3

Firefox version 3 is a bit more aggressive in its handling of a self-signed certificate. Below is the certificate warning displayed by Firefox 3.



Figure 4. Firefox 3 certificate warning.

There's lots of scary text here saying that the certificate is not trusted and someone could be trying to impersonate the server. *Generally these are valid concerns and this warning should always be taken seriously.* For our purposes, though, the warnings may be disregarded.

At the bottom of this certificate warning is a hyperlink that says 'Or you can add an exception...' Click on this link and the warning box will change to add a couple of pushbuttons (Figure 5).



Figure 5. Firefox 3 certificate warning after selecting the ‘Or you can add an exception...’ hyperlink.

Select the ‘Add Exception...’ pushbutton. Firefox 3 will then display the ‘Add Security Exception’ dialog, as shown below.

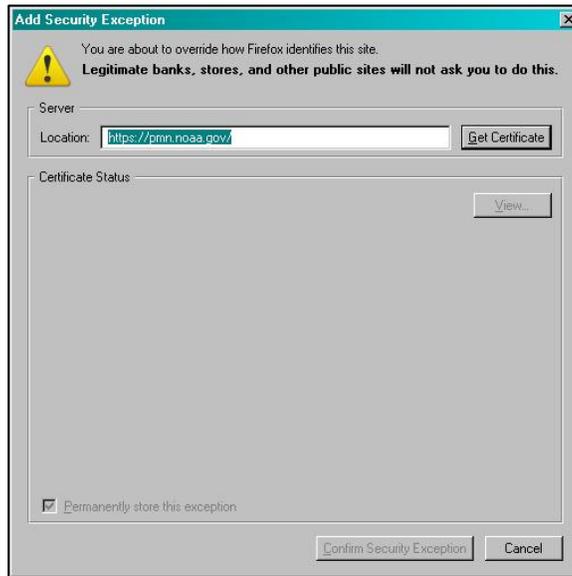


Figure 6. Firefox 3 ‘Add Security Exception’ dialog.

Confirm that the server location says ‘https://pnn.noaa.gov/’ and select the ‘Get Certificate’ pushbutton.

Firefox 3 will retrieve the certificate and display *yet another* warning that the certificate is untrusted because it cannot be verified by a recognized authority (Figure 7).



Figure 7. Firefox 3 ‘Confirm Security Exception’ dialog.

Note there is a checkbox that says ‘Permanently store this exception’ which is enabled by default. Leave this as it is because this process is a hassle to go through every time.

Select the ‘Confirm Security Exception’ pushbutton to complete the process and proceed to the PMN data entry site. Whew!

Deleting a certificate in Firefox 3 is very much like the procedure for Firefox 2, but the appearance of the dialogs is slightly different.

To delete a certificate in Firefox 3:

1. Select ‘Tools -> Options -> Advanced -> Encryption’ (Figure 8).

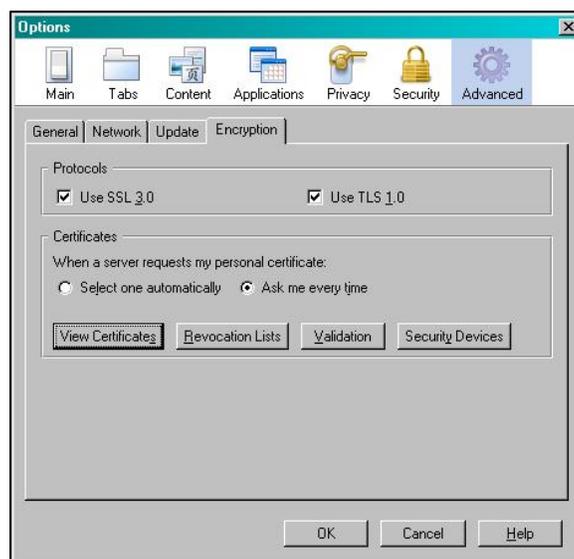


Figure 8. Firefox 3 ‘Options’ dialog.

2. Select the 'View Certificates' button.
3. In the Certificates Manager dialog, select the 'Servers' tab.
4. Scroll down until you see the '(Unknown)' group. If there is a plus sign ('+') next to the '(Unknown)' group, expand the group by clicking on the plus sign. The view should be similar to that shown in Figure 9.

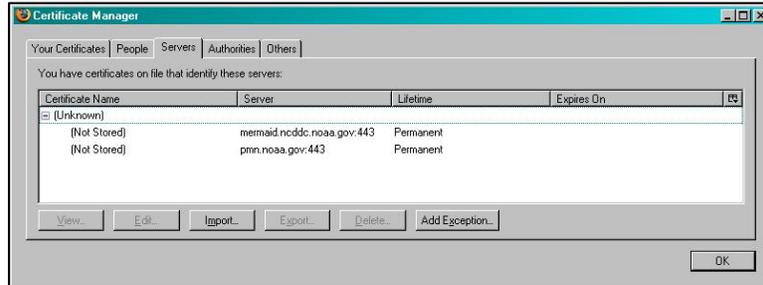


Figure 9. Firefox 3 Certificate Manager.

5. Select the 'pmn.noaa.gov' certificate.
6. Select the 'Delete' button. You will be prompted to confirm the certificate deletion; select the 'OK' button to do so.

Internet Explorer Version 7

Internet Explorer displays a warning page (Figure 10) which gives the user the option of continuing to the website or not. It is okay to continue to the PMN data entry site when presented with this warning. If you are prevented from doing so, however, it may be necessary to delete the certificate.

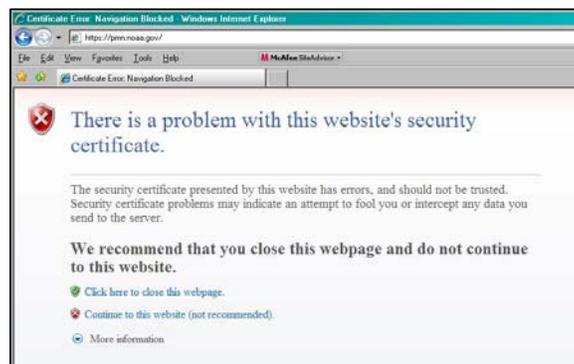


Figure 10. Internet Explorer certificate warning.

To manually delete a certificate in Internet Explorer:

1. Select 'Tools -> Internet Options -> Content' (Figure 11).

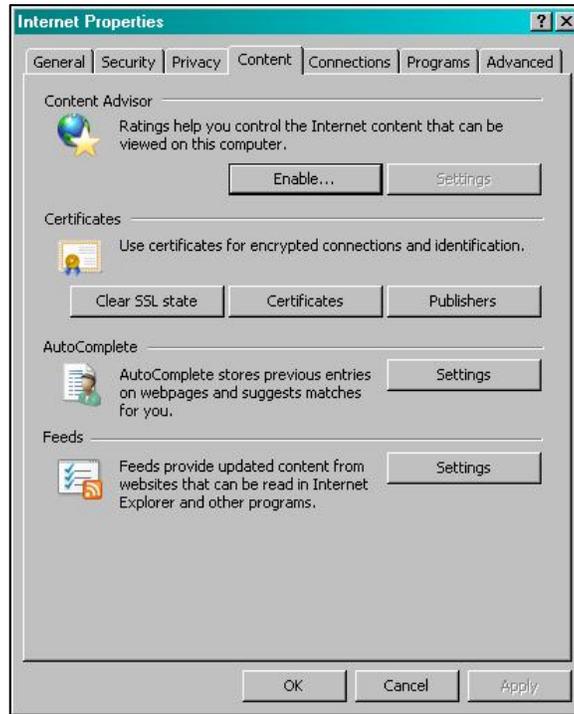


Figure 11. Internet Explorer 'Internet Properties' dialog.

2. Select the 'Certificates' button. There will be several tabs across the top of the Certificates dialog, such as 'Personal', 'Other People', etc (Figure 12). Browse through all of these tabs and see if there is one for 'pmn.noaa.gov'. If you find one delete it and see if you can then access the site.

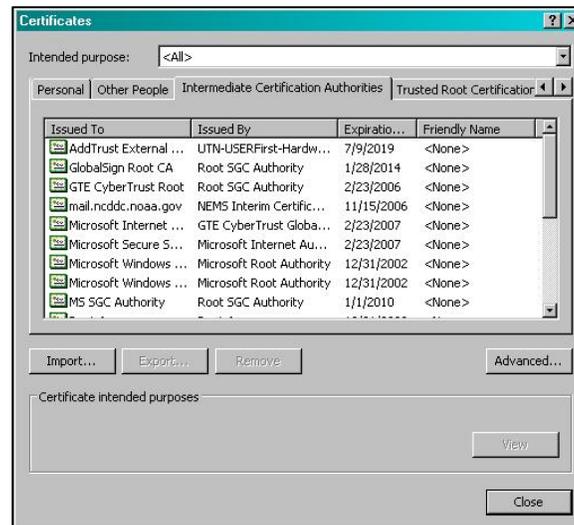


Figure 12. Internet Explorer Certificate

NOTE: there are more tabs than are displayed by the dialog; you will see left/right arrows at the end of the tab display which will scroll the additional tabs across the dialog. Be sure to look in all of them because we're not sure where the PMN certificate might be stored, and there might be more than one.

Also select the 'Publishers' button in the 'Content' dialog and look through those too.

Safari Version 3

Safari displays a warning dialog (Figure 13) which gives the user the option of continuing to the website. It is okay to continue to the PMN data entry site when presented with this warning.

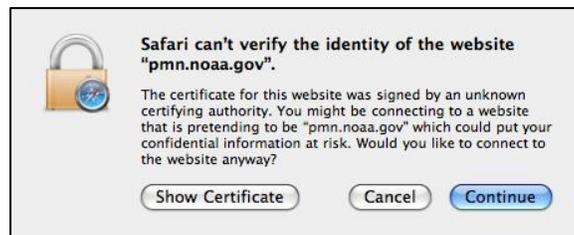


Figure 13. Safari certificate warning.

Safari does not itself provide an interface for managing certificates; rather it stores the certificates 'natively' in Windows Explorer's certificate database, accessible via the XP Control Panel.

To view and manage certificates in Windows XP:

1. Select Start -> Control Panel -> Internet Options.
2. In Internet Options click the 'Content' tab.
3. Refer to Step 2 in the Internet Explorer 7 section above.