**Entrust.Net**

# Technical Information –
# CRL Checking

Client Confidential

_____

## TABLE OF CONTENTS

_____

# CRL CHECKING

## 1.1  HOW TO LOCATE THE SERIAL NUMBER OF A DIGITAL CERTIFICATE AND VERIFY VALIDITY WITH MICROSOFT INTERNET EXPLORER 5.X

This procedure describes how to locate the serial number of a digital certificate, and how to verify the status of that certificate.

**Locate and obtain the Serial Number**

1.  Go to the secure Web site where you want to confirm the status of the certificate.

2.  Double-click the closed lock icon on the status bar at the bottom of the browser window.  The Certificate dialog box appears.

2.  Click the Details tab. The Details tab contains two windows.

3.  Select Serial Number from the list in the top window of the Details tab.  The certificate serial number is displayed in the bottom window of the Details tab.

4.  Select the contents of the lower window.

5.  Press the CTRL key and the C key on your keyboard at the same time to copy the serial number to your computer memory.

**Verify the Validity of the Certificate**

1.  Open a new browser.

2.  Go to the Entrust.net Web site (http://www.entrust.net).

3.  Click the Customer Service button.  The browser goes to the Customer Service page.

4.  Click the CRL Checking link, located under Customer Options on the left of the screen. The browser goes to the CRL Checking page.

5.  Paste the serial number in the Serial Number: field.

6.  Remove any special characters from the Serial Number: field, if any are present. The serial number you submit should be eight characters long, consisting of letters and numbers only. For example, 374AD2B0
    Some examples of special characters are: ! @ # $ % ^ & * ( ) [ ] { } - + = . , \ | / ? : ;
    Please note that blank spaces are also considered special characters.

7.  Click the Submit button.
    The browser sends the serial number to Entrust.net to verify its validity.
    The browser goes to the validity confirmation page and informs you if the certificate with the serial number that you submitted is valid or invalid.

_____

_____


# CRL CHECKING


## 1.2  HOW TO LOCATE THE SERIAL NUMBER OF A DIGITAL CERTIFICATE AND VERIFY VALIDITY WITH NETSCAPE 4.X

This procedure describes how to locate the serial number of a digital certificate, and how to verify the status of that certificate.

Locate and obtain the Serial Number

1.  Go to the secure Web site where you want to confirm the status of the certificate.

2.  Click the closed lock icon on the status bar at the bottom of the browser window.
    The Security Info window appears.

3.  Click the View Certificate button.
    The "View A Certificate" window appears.

4.  Select and highlight the Serial Number.

5.  Press the CTRL key and the C key on your keyboard at the same time to copy the serial number to your computer memory.


Verify the Validity of the Certificate


1.  Open a new browser.

2.  Go to the Entrust.net Web site (http://www.entrust.net).

3.  Click the Customer Service button.
    The browser goes to the Customer Service page.

4.  Click the CRL Checking link, located under Customer Options on the left of the screen.
    The browser goes to the CRL Checking page.

5.  Paste the serial number in the Serial Number field.

6.  Remove any special characters from the Serial Number: field, if any are present. The serial number you submit should be eight characters long, consisting of letters and numbers only.
    For example, 374AD2B0
    Some examples of special characters are: ! @ # $ % ^ & * ( ) [ ] { } - + = . , \ | / ? : ;
    Please note that blank spaces are also considered special characters.

7.  Click the Submit button.
    The browser sends the serial number to Entrust.net to verify its validity.
    The browser goes to the validity confirmation page and informs you if the certificate with the serial number that you submitted is valid or invalid.

_____

# CRL CHECKING

## 1.3  CHECKING THE ENTRUST.NET CERTIFICATE FINGERPRINT

The Entrust.net chain certificate you are importing tells your Web browser what sites it can trust on the Web. Before you can trust the chain certificate, however, you must be sure that you are importing the right one. To do this, compare the certificate fingerprint on the certificate you are importing to the one below. If the two fingerprints match you can be sure you are importing the correct certificate. If they do not match, please contact Entrust support immediately and do not import the chain certificate.

The fingerprint for the Entrust.net chain certificate is:

0D:8D:DE:C8:66:59:5E:C9:F1:FE:48:6F:A5:E3:AF:65