IBM Domino Go CSR Creation and Installation

How to generate a CSR in Domino Go Web Server

** Note: MKKF places in the same directory that it is run from unless you choose to specify a different location.

1. Initialize the MKKF utility by entering mkkf at a command prompt. A menu will be displayed.
2. Choose N (make a new key ring.)
3. Enter the new key ring filename.
4. Another menu will display. Choose W (work with keys and certificates)
5. Choose C (create a new key and certificate request)
6. Enter a new password. Make sure to remember the password for later.
7. Choose P (PKCS#10 certificate format)
8. Select M (Modify the certificate request information)
9. Enter your organizational information in the proper fields. It must all be accurate.
10. Choose R. This will generate your key and Certificate Signing Request (CSR).
11. Exit MKKF by selecting X.
12. Make sure to save the changes to your new Key Ring
13. Save a copy of your new Key Ring file to a safe backup location.
14. Please send the CSR file to us for our process.

For each of the three SSL Certificates, follow the steps below:

1. **Preparing your Primary Server Certificate:**
   Open your primary Certificate (your_domain_name.crt) in a text editor and save a copy of this file in .txt format. Name this file "your_domain_name.txt".

2. **Preparing the Root and Intermediate CA Root Certificates:**
   Open the Intermediate Root SSL Certificate (IntermediateCA.crt) into a text editor and save by the same name but as a .txt file. Do the same thing for the Root Certificate (TrustedRoot.crt).

   Make sure sure your text files include the full certificate as in the example below:

   ```
   -----BEGIN CERTIFICATE-----
   text ...
   ------END CERTIFICATE-----
   ```

   Note: If you start the **mkkf utility** from the directory that contains your SSL Certificates the path will not need to included.

   1. Click **R** to Receive an SSL Certificate into a Key Ring file.
   2. You will be prompted for the file name. Enter **TrustedRoot.txt**.
   3. Enter **TrustedRoot** for the label.

    4. Click **Enter** to continue.
    5. Click **W** to work with Keys & Certificates.
    6. Click **L** to Select the Key to work with.
    7. Find the **TrustedRoot** and select **S** to chose that menu.
    8. Click **T** to mark this as a 'Trusted' root.
    9. Click **Y** (Yes) to confirm the request.
    10. Click **Enter** to return to the pervious menu.
    11. Click **X** to Exit the menu.

        Note: Repeated below for the Intermediate Root Certificate. Must be done in the correct order as described in these instructions!

    12. Repeat from **Select R** using the DigiCert Intermediate SSL Certificate.
    13. Change the **TrustedRoot.txt** with **IntermediateCA.txt**.
    14. Change the **TrustedRoot** label with**Root**.

3. **Installing your Primary Server Certificate:**
    0. From the main menu of the **mkkf** utility.
    1. Click **R** to Receive an SSL Certificate into a Key Ring file.
    2. Type the Primary Server Certificate file name: your_domain_name.txt.
    3. Click **W** to Work with Keys & SSL Certificates.
    4. Click **L** to Select the Key to work with.
    5. Click **N** until you find the required file.
    6. Click **S** to Select this SSL Certificate.
    7. Click **F** to mark this Key as the **Default Key**.
    8. Click **X** to Exit this menu.
    9. Click **C** to Create a **stash file** for the Key Ring

        Note: Important Steps (Do Not Overlook)

    10. Click **X** to Exit the menu.
    11. Click **Y** (Yes) to save all changes to the Key and to Confirm/Update.
4. **Enabling SSL on your Domino Go Web Server**
    0. Access your Web Server (using your browser).
    1. Click **Configuration & Administration Forms**.
    2. Locate Security Option.
    3. Click **Security Configuration**.
    4. Make certain that **Allow SSL connections Using Port 443** is selected.
    5. Confirm that the correct **Key-Ring** file is listed.
    6. Apply changes.
5. **Restart your Lotus Domino Web Server**