**IBM runmqckm commands for Certificate Management for MQ**

* **Create a key database**
* runmqckm -keydb -create -db clientkey.kdb -pw xxxxx -type cms -stash
* clientkey.kdb is the database name
* xxxxxx is the password you choose. Make sure to have it safely stored. It is a major issue if not know
* cms is the database type. Must be cms for queue managers
* The -stash option stashes the password in a file allowing MQ to access database
* There is an expire option that I have not included. By not specifying this option the password will not expire.
* Once completed, the following files are created:
* clientkey.kdb - the key database file.
* clientkey.sth - the encrypted password stash file
* **Add Root CA certificate to the key data base:**
* runmqckm -cert -add -db clientkey.kdb -label <AliasNameForRootCA> -file <ROOT-CA.cer> -pw xxxxx
* clientkey.kdb - The key database file which we will add the CA certificate to
* < AliasNameForRootCA > - The label (a name that you choose to describe the root ca cert) which will be applied to this CA certificate to distinguish the certificate. It must be unique.
* <ROOT-CA.cer> - The CA certificates file to be added to the .kdb (If it has intermediate certificate then install the root first then the intermediate certificate second)
* xxxxx - The password of the key database that was included in the .kdb creation
* **To generate a certificate request (CSR) for your application.**
* runmqckm -certreq -create -db clientkey.kdb -stached -label <AliasNameForCert> -dn "CN=<GSI-ID.Hostname>" -size 2048 -file certreq.req
* clientkey.kdb - The key database file
* xxxxx - The password of the key database (of your choice).
* <AliasNameForCert> - The label (ibmwebspheremq + <user ID> all in lower case) attached to the personal certificate for this application.
* 2048 - The size of the key.
* certreq.req - The file name of the certificate request.
* Once completed capture the created file and have it signed. (send it to EIS team for signature)
* **Receive the signed Personal Certificate from CA (EIS team)**
* runmqckm -cert -receive -file <signedrequest> -db clientkey.kdb -stached
* <signedrequest> - This is the signed personal certificate you have received back from the CA (EIS team)
* clientkey.kdb - The key database file
* xxxxx - The password of the key database

**Here are additional commands**

* To list all the Certificates in a key database:
* runmqckm -cert -list -db key.kdb -pw xxxxx
* To display detailed information about one certificate:
* runmqckm -cert -details -db key.kdb -pw xxxxx -label cert\_label