IBM z16 Increased Certificate Key Length for HMC & OSA-ICC

August 7, 2024

—

SHARE in Kansas City

Brian Valentine
HMC/SE Development
File Updated: 08-05-24

IBM z16 Increased Certificate Key Length for HMC & OSA-ICC

z16 -- Increased Certificate Key Length for HMC & OSA-ICC

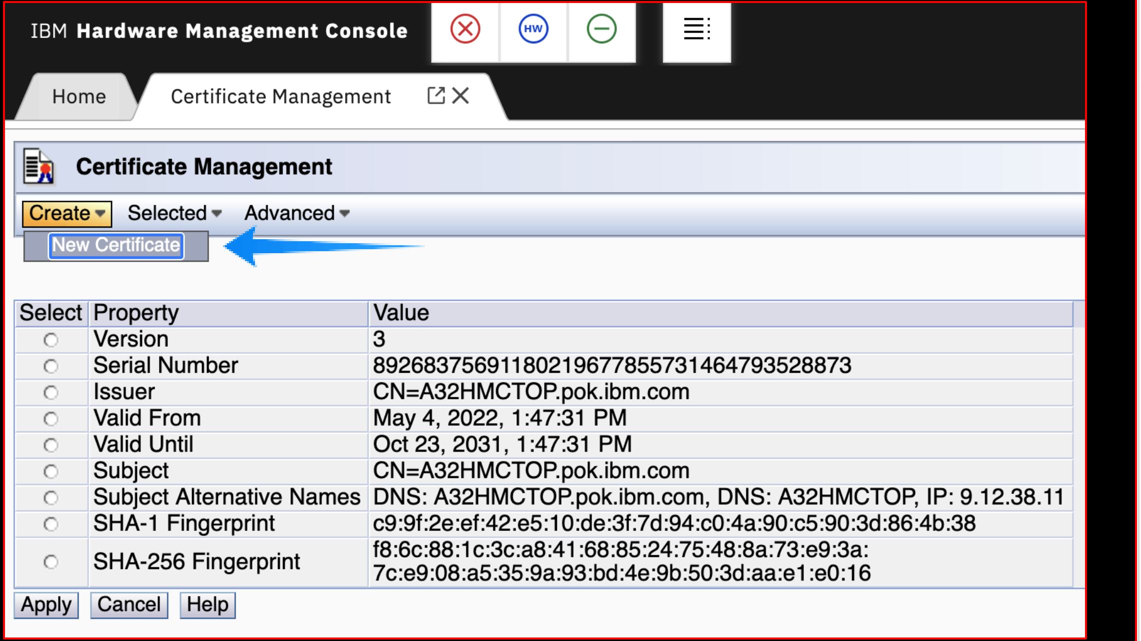
- HMC & OSA-ICC Current key length: 2048 bit

- Increase key length, but give selection options of 2048, 3072, 4096 for new certificates
  - New Default: 3072

- 3072-bit keys required to conform to EMEA Standards
  - e.g. *https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf*

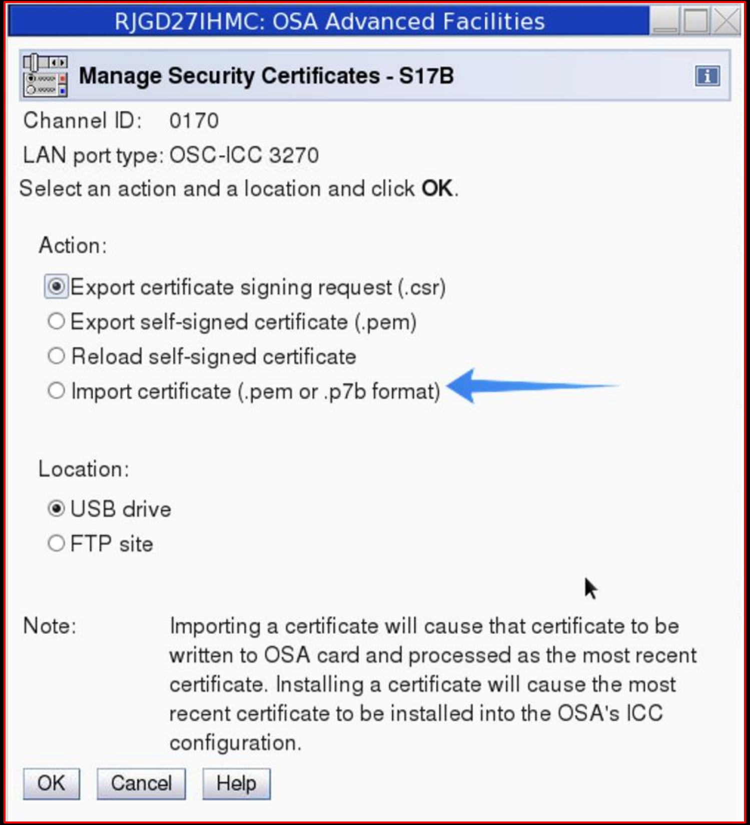
- Enhancement provided in HMC & SE MCL Bundles H26/S34
  - Bundle H26 available
  - Bundle S34 available
    - If H26 fix is active & S34 is not on z16 (or z15 or earlier system is targeted),
      - HMC Certificate will support for longer key length options including SOO (Single Object Operations) to SE/CPC
      - OSA-ICC Certificate will only provide the 2048 key length option, but z16 CPCs (with S34) will get the 2K, 3K, & 4K options.

z16 -- Increased Certificate Key Length for HMC & OSA-ICC



Certificate Management

Select	Property	Value
○	Version	3
○	Serial Number	89268375691180219677855731464793528873
○	Issuer	CN=A32HMCTOP.pok.ibm.com
○	Valid From	May 4, 2022, 1:47:31 PM
○	Valid Until	Oct 23, 2031, 1:47:31 PM
○	Subject	CN=A32HMCTOP.pok.ibm.com
○	Subject Alternative Names	DNS: A32HMCTOP.pok.ibm.com, DNS: A32HMCTOP, IP: 9.12.38.11
○	SHA-1 Fingerprint	c9:9f:2e:ef:42:e5:10:de:3f:7d:94:c0:4a:90:c5:90:3d:86:4b:38
○	SHA-256 Fingerprint	f8:6c:88:1c:3c:a8:41:68:85:24:75:48:8a:73:e9:3a: 7c:e9:08:a5:35:9a:93:bd:4e:9b:50:3d:aa:e1:e0:16



Manage Security Certificates - S17B

Channel ID: 0170

LAN port type: OSC-ICC 3270

Select an action and a location and click **OK**.

Action:

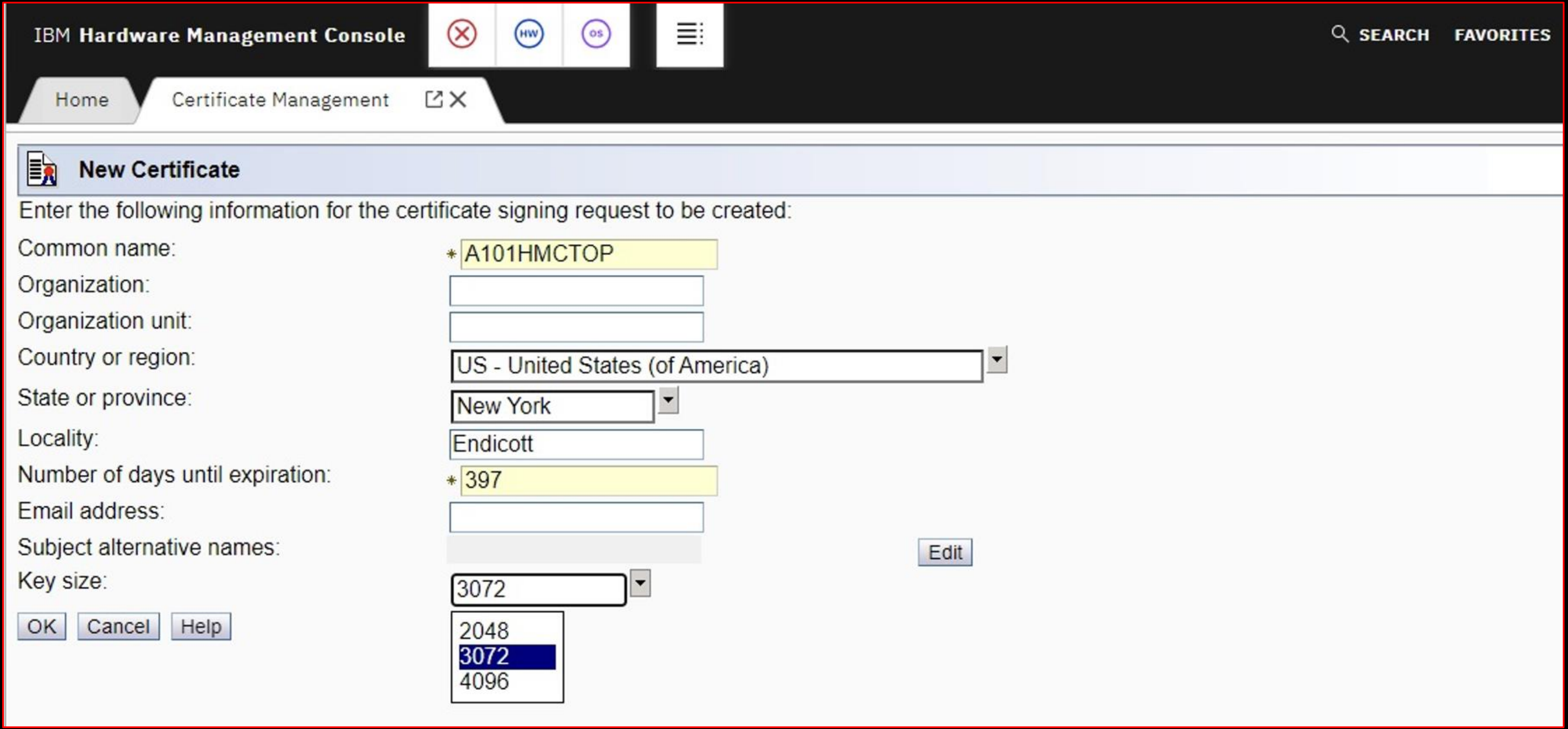
- ● Export certificate signing request (.csr)
- ○ Export self-signed certificate (.pem)
- ○ Reload self-signed certificate
- ○ Import certificate (.pem or .p7b format)

Location:

- ● USB drive
- ○ FTP site

Note: Importing a certificate will cause that certificate to be written to OSA card and processed as the most recent certificate. Installing a certificate will cause the most recent certificate to be installed into the OSA's ICC configuration.

z16 -- Increased Certificate Key Length for HMC & OSA-ICC



New Certificate

Enter the following information for the certificate signing request to be created:

Common name:	* A101HMCTOP
Organization:	
Organization unit:	
Country or region:	US - United States (of America)
State or province:	New York
Locality:	Endicott
Number of days until expiration:	* 397
Email address:	
Subject alternative names:	Edit
Key size:	3072

Thank you for your time and consideration….

Brian Valentine
HMC/SE Team
X (Twitter): @bdvalent125

Contact for questions or additional feedback:
Brian Valentine, bdvalent@us.ibm.com