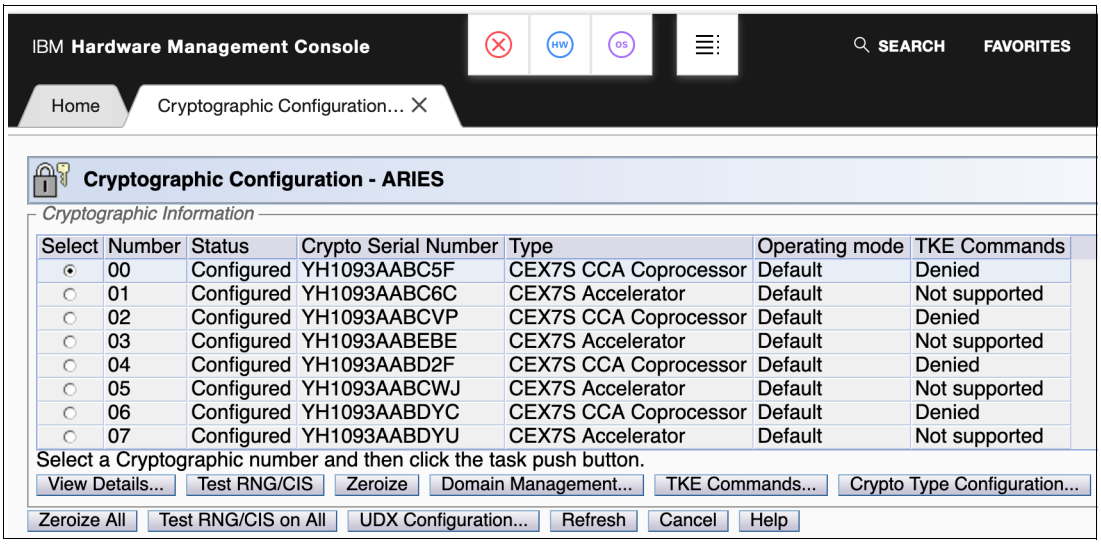

Figure 10-28 Cryptographic Configuration window

The Usage Domain Zeroize task is provided to clear the appropriate partition crypto keys for a usage domain when you remove a crypto card from a partition. Crypto Express7/6/5S in EP11 mode is configured to the standby state after the zeroize process.

For more information, see *IBM z15 (8561) Configuration Setup*, SG24-8860.

Digitally signed firmware

Security and data integrity are critical issues with firmware upgrades. Procedures are in place to use a process to digitally sign the firmware update files that are sent to the HMC, SE, and TKE. By using a hash algorithm, a message digest is generated that is then encrypted with a private key to produce a digital signature.

This operation ensures that any changes that are made to the data are detected during the upgrade process by verifying the digital signature. It helps ensure that no malware can be installed on IBM Z products during firmware updates. It also enables the z15 Central Processor Assist for Cryptographic Function (CPACF) functions to comply with Federal Information Processing Standard (FIPS) 140-2 Level 1 for Cryptographic LIC changes. The enhancement follows the IBM Z focus of security for the HMC and the SE.

The Crypto Express7S (CEX7S) is compliant with CCA PCI HSM. TKE workstation is optional when used to manage a Crypto Express7S feature that is defined as a CCA coprocessor in normal mode. However, it is mandatory when it is used to manage a Crypto Express7S feature that is defined as a CCA coprocessor in PCI-HSM mode or is defined as an EP11 coprocessor (CCA in PCI-HSM mode and EP11 also require a smart card reader plus smart cards with FIPS certification).

10.5.14 Installation support for z/VM that uses the HMC

Starting with z/VM V5R4 and z10, Linux on Z can be installed in a z/VM virtual machine from HMC workstation media. This Linux on Z installation can use the communication path between the HMC and the SE. No external network or extra network setup is necessary for the installation.