

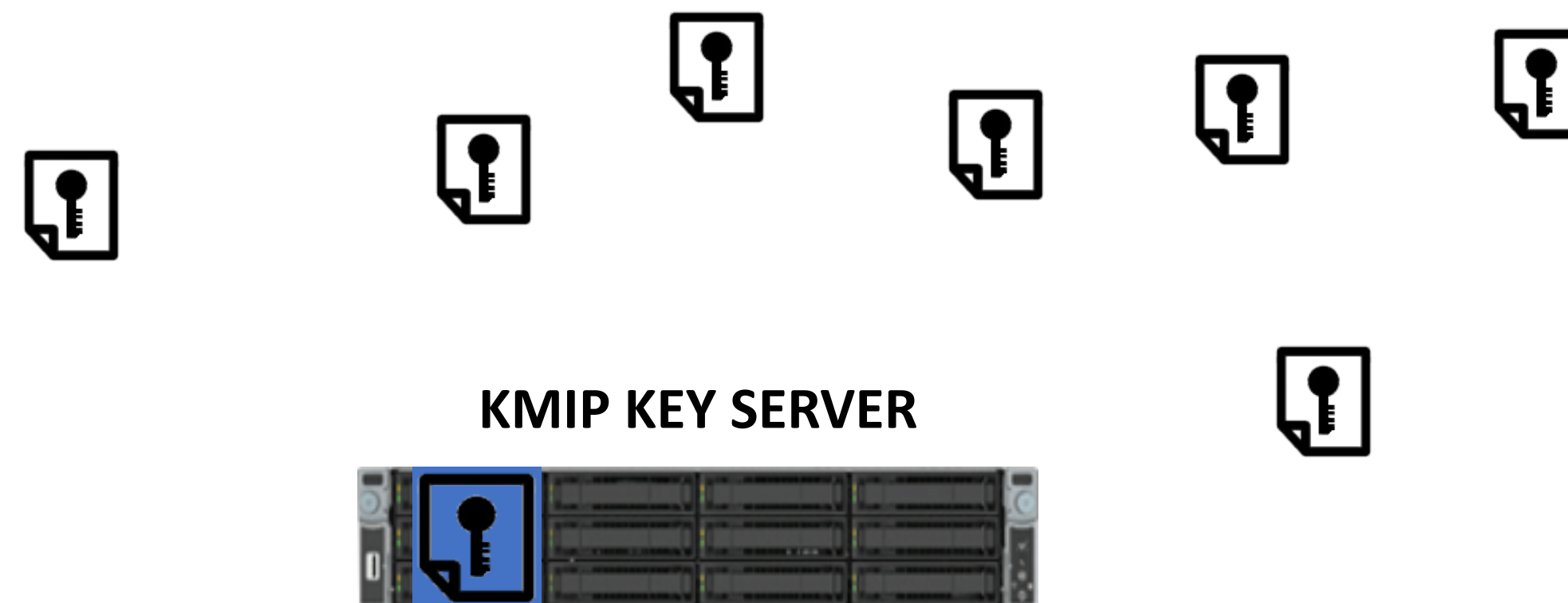


QuantaStor 5.11 KMIP & SED Security Features Overview



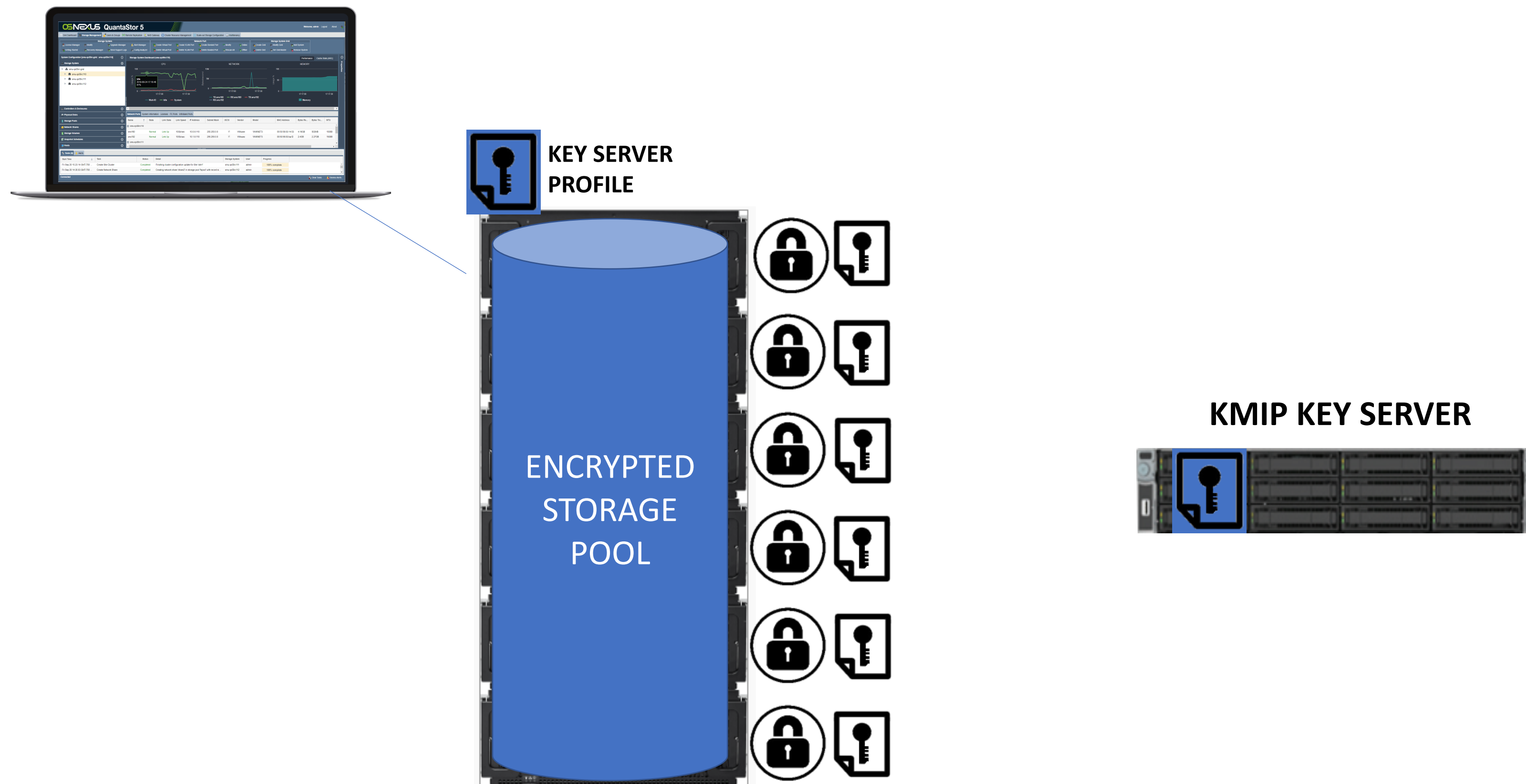
WHAT IS KMIP?

Key Management Interoperability Protocol ([KMIP](#)) is an extensible communication protocol for managing security keys that has been developed and standardized by the [OASIS standards body](#).



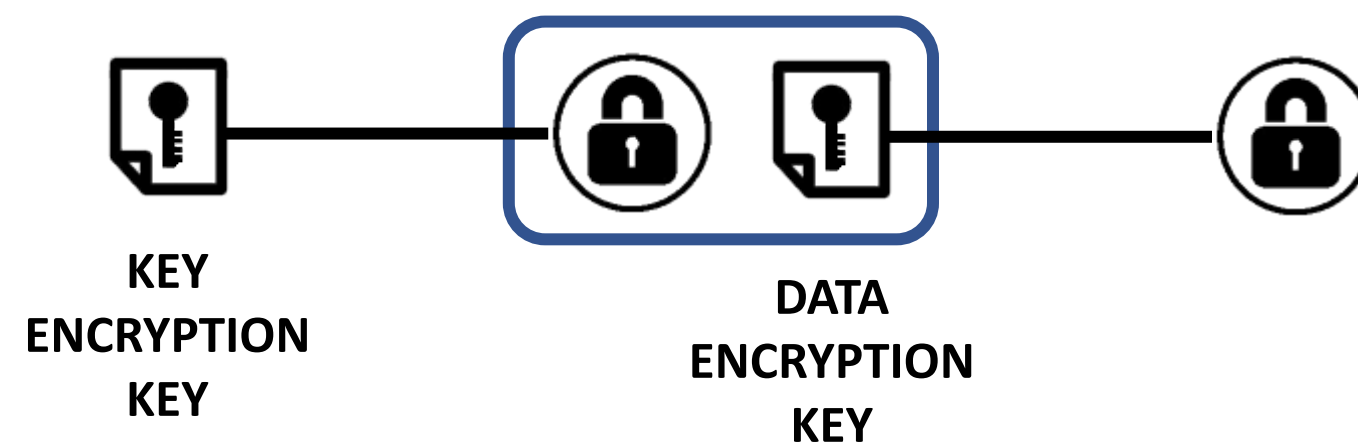
HOW DOES QUANTASTOR INTEGRATE WITH KMIP?

- QuantaStor integrates with KMIP via a new feature called Key Server Profiles
- Key Server Profiles contain the IP, certificates, and credentials for communicating with a KMIP Server
- When an encrypted Storage Pool is created one can optionally select a Key Server Profile to use for key management
- Whenever a system is rebooted or a Storage Pool is started, keys are gathered automatically from the KMIP Server to unlock the media.
- QuantaStor supports both SED hardware and software encryption with integration with KMIP



WHAT IS A SELF-ENCRYPTING DRIVE (SED)?

- Most new SSDs now have built-in data encryption capabilities
- HDDs with built-in data encryption capabilities are usually special models of enterprise HDDs.
- Devices with this capability are referred to as Self Encrypting Drive (SED) media
- Opal and Ruby are the names of the SED standards developed by the Trusted Computing Group (TCG)



- Key Encryption Key (KEK) can be changed at any time and the data on the device doesn't need to be re-encrypted.
- Data Encryption Key (DEK) is an internal tamper-proof key that is used to encrypt and decrypt the data written to the media.
- Data Encryption Key (DEK) is only changed to erase the media. Instant Secure Erase (ISE) is a feature of SED media that regenerates a new Data Encryption Key in order to securely erase the device.