Diamond-HSM Remote Backup Procedure

Copyright © 2019 Diamond Key Security, NFP

The following is the plan for performing a remote backup of a Diamond-HSM on the network to a CrypTech alpha.

1. A screenshot of a cell phone

   Description automatically generated User initiates a remote backup using dks\_setup\_console
2. The Diamond-HSM will respond with a code requesting dks\_setup\_console to generate a KEKEK on the CrypTech device
3. dks\_setup\_console will then send the public KEKEK to the Diamond-HSM
4. The Diamond-HSM will load the KEKEK encryption key onto its internal CrypTech device.
5. The Diamond-HSM will use the KEKEK to wrap the private keys stored in the Diamond-HSM’s internal CrypTech device and return the PKCS#8 key and KEK.
6. Public keys on the HSM’s internal CrypTech devices will be sent as plain text because they are public keys.
7. The Diamond-HSM will send the key information using the JSON format.
8. dks\_setup\_console will retrieve the key information as a JSON file. (private keys have been wrapped)
9. dks\_setup\_console will then use pkey\_import to load save the keys to the CrypTech device.