Copyright © 2019 Diamond Key Security, NFP

Data Transfer with the HSM

The HSM supports transfer of data between it and ‘dks\_setup\_console’. The data transfer capabilities are used for sending updates to the HSM and for performing remote backup and restores to a CrypTech device connected to the computer running ‘dks\_setup\_console’.

All data transfers operations with the HSM must originate from the HSM. Users can request an operation using the console. The HSM will validate the request, perhaps needing the user to reenter the ‘wheel’ password, and then it will send a ‘SEND’ or ‘RECV’ command to ‘dks\_setup\_console’. ‘SEND’ and ‘RECV’ commands are given from the point of view of the HSM. A ‘RECV’ command means that the HSM wants to receive data from ‘dks\_setup\_console’, and a ‘SEND’ command means that the HSM will send data to ‘dks\_setup\_console’.

Command Format

Commands all have the same format “<management code>:<command type>:<parameter list>”. The management code is a 32-bit binary number. The rest of the command is an ASCII string. ‘<command type>’ can be either ‘SEND’ or ‘RECV’. The parameter list is specific to the management code. If the code as only one parameter, the remainder of the command will be the parameter. If the command uses multiple parameters, each parameter will be in curly braces.

Example:

\x11\x12)\x13\x14:RECV:/home/dkey/Downloads/DKEY-HSM-UPDATE-19.04.b2.tar.gz.signed

All commands start with 0x1112. That is the signal to ‘dks\_setup\_console’ that a special command is coming.

RECV Commands

RECV commands are sent by the HSM when it wants to receive data. When the HSM receives data, it can receive text or binary data. The HSM only saves update information to a file where it will immediately verify that it came from Diamond Key by checking the signature. All other data must be JSON data with any binary information encoded as base64. The HSM will never save JSON data to nonvolatile storage to prevent nefarious code from being stored on the HS.

SEND Commands

SEND commands are sent by the HSM when it wants to send data. receive data. The HSM only send JSON data. All binary data will be encoded as base64. SEND commands send the size of the data in bytes as the parameter. ‘dks\_setup\_console’ will then send ‘OK:{<number of bytes to receive>}’ to signal to the HSM that it received the message.