Diamond-HSM™ Prototype Release Notes version 18.12.b1

Welcome to the Diamond Key HSM Beta. The Diamond-HSM prototype delivered under this agreement is a "Beta" or pre-release product. Although it has been designed and constructed in a manner that is similar to a future product release, it is not intended for commercial, in-network, operation.

Before you power up the device, we recommend that you read these notes, and take care about operational issues that we have recorded here. This is very much a Beta release. Some functionality is more mature and better tested than other functionality. We are documenting issues we have found in our testing so far and we look forward to hearing from you about issues you find in your testing.

We expect to have an update to fix a number of these issues in January. We may have some intermediate updates before then and there will continue to be updates after that. For many of these issues we can perform them remotely if you are willing to make access to the device available over the Internet. We will be happy to do that at a scheduled time.

For issues you discover, please send them to ….

Physical Known Issues:

1) USB interface – we have provided a USB interface on the front of the box. This interface is not connected internally at this point in time. We are working on functionality to make use of this interface.

2) Enclosure – this is the first iteration of the physical enclosure and we discovered some issues during assembly of the Beta. Some have been addressed but other remain that will be addressed in a future hardware revision.

3) Enclosure "Gap" – One example of an enclosure issue to be addressed in the future is a possible gap where the front panel meets the top cover of the case/enclosure. Future case releases will have this corrected.

Operational Known Issues:

Please note: when you power on the HSM, if you follow the steps specified in the manual, some of the issues described below will be minimized.

Please note: If the 'wheel' user password is ever forgotten, the HSM will no longer be configurable as there is no way to change the 'wheel' password without knowing the current 'wheel' password.

1) It takes the CrypTech devices about 45 seconds to perform console key store operations such as erasing the key store, and settings PINs. The Diamond-HSM currently doesn't enforce this delay so ***please wait 45-60 seconds*** when erasing the key store or restoring the HSM, and ***15-30 seconds*** after setting the 'wheel', 'so', or 'user' PINs. Future updates will enforce the delay.

2) The current version does not support mirroring the two internal CrypTech devices; Our key backup strategy has a couple of steps. First, is the ability to mirror the contents of the two CrypTech devices inside our HSM. We expect to have an update soon that will enable this functionality. After that, we will provide a full backup strategy based upon what CrypTech has already implemented that will allow users to export keys for a backup and to export them to a different HSM. ***Please note, to be able to support mirroring the CrypTech devices in the future, the 'ENABLE_EXPORTABLE_PRIVATE_KEYS' option must be set in the console or private keys will be permanently restricted to the CrypTech device that generated it. ***

3) The hardware is present in the HSM to detect a range of tamper events. At this point, the HSM will only detect a case open tamper event. When it does, it will clear the master key, but the tamper light in the front of the HSM has not yet been programmed so the light will not turn red. We expect an update soon that will utilize the sensors inside the HSM to detect a range of tamper events in addition to case open and at that time the tamper detected light will be made operational.

4) Tamper detection can be reset by correctly attaching the case and cycling power. Otherwise the tamper detect withholds access to the MKM until a clear signal is sent or the HSM is power cycled

5) A battery has not been installed so a loss of power will clear the master key. We plan to add one when we do an update in the near future.

6) The 'findHSM' utility that uses zeroconf to find the HSM on a DHCP network sometimes can't detect HSMs plugged in after it was initially run. Currently, the only fix is to restart the host computer.

7) When updating the HSM, if the update file can't be found, 'dks_setup_console' will need to be restarted.

Preserving the HSM and Troubleshooting

1) When possible, shutdown the HSM using the console command before pulling power.

2) Wait **45-60** seconds after key store operations to prevent key store corruption.

3) If the HSM has problems detecting a CrypTech device on startup, wait 90 seconds, then power off the HSM using the power switch. Wait 60 seconds and then restart the HSM. Wait 60 seconds after all the lights turn green before accessing the HSM.

4) The latest versions of the CrypTech firmware and FPGA bit stream have already been loaded. DO NOT upgrade the CrypTech, firmware, bootloader, or bit stream without first contacting Diamond Key Security. Diamond Key will inform users when CrypTech device upgrades are needed. Updating the FPGA bit stream can cause permanent key store corruption if not successful.