This is PREF-FAQ notes I made while researching heads. These notes might become Questions which could then be added to the FAQ.

- X What commands are available in the recovery shell?
    - The shell is based on busybox?
    - In addition to some standard unix commands these are the heads commands available
        - kexec
        - kexec-boot
        - kexec-insert-key
        - kexec-iso-init
        - kexec-parse-bls
        - kexec-save-default
        - kexec-save-key
        - kexec-seal-key
        - kexec-unseal-key
        - kexec-select-boot
        - kexec-sign-config
- X How do I find more information on commands in the recovery shell?
    - Some of the commands have the standard --help switch. Other than that we have to use source code as a reference. These commands do not have --help and could use documentation first: (* => no help switch but dumps help on error)
        - kexec-insert-key
        - kexec-iso-init*
        - kexec-parse-bls
        - kexec-parse-boot
        - kexec-save-default
        - kexec-save-key
        - kexec-seal-key
        - kexec-select-boot
        - kexec-sign-config
        - kexec-unseal-key
        - kexec-boot

Help

mount-boot

2 parameters: device = /dev/sda , offset = 256

Device = boot device or partition

Offset = ? NOT USED?

Questions

- Is this for mounting a signed boot partition?
- What should be the next step if there is no trustedkeys.gpg file?
- What secret(s) is/are stored in nvram? What are they used for?
- What is stored in the MBR section of disk or partitions?

kexec-save-key

Generate a TPM key used to unlock LUKS disks. Saves key

-p <partition>

-l ?

kexec

Used to boot OS from inside heads environment.

Not a binary in source? Is this built as the main component of heads booting? Binary ends up in initrd?

kexec-insert-key

Unseal a disk key from TPM and add to a new initramfs

kexec-iso-init

Boot from signed ISO

kexec-parse-bls

?

kexec-save-default

Save options to be the persistent default [boot?]

kexec-seal-key

This will generate a disk encryption key and seal / ecncrypt with the current PCRs and then store it in the TPM NVRAM. It will then need to be bundled into initrd that is booted.

kexec-unseal-key

This will unseal and unecncrypt the drive encryption key from the TPM. The TOTP secret will be shown to the user on each encryption attempt. It will then need to be bundled into initrd that is booted.

kexec-select-boot

Generic configurable boot script via kexec

kexec-sign-config

Sign a valid directory of kexec params

kexec-parse-boot

?