Restore Secure Boot Keys, Bootloader, LUKS TPM Key after Firmware update

After a firmware upgrade the firmware settings might get reset to their default values, including bootloater entries and custom secure boot keys.

Restore secure boot keys

First, you should restore any custom secure boot keys that might have been lost.

If you already had secure boot keys before the update you should be able to simply restore them by pushing them into the firmware again like you did on initial setup. Keep in mind that you still need to put the secure boot state into **setup mode** (e.g. by deleting all keys from storage) or else the keys will not be writable and restore will fail.

Boot the Arch Linux install media, mount your drives (especially the EFI system partition) and `arch-chroot` into it.

If you only boot Arch Linux:

```
sbctl enroll-keys
```

If you dual-boot Windows:

```
sbctl enroll-keys --microsoft
```

Restore boot loader

Depending on which boot loader you use you can probably restore it by just installing it again.

See the Boot Loader section for install instructions.

After restoring the boot loader, make sure to sign it with your keys and regenerate and re-sign the initrd as well!

```
sbctl sign-all
```

Regenerate TPM-based LUKS key

Since the firmware code changed the PIN you set up for a TPM-based LUKS key will probably stop validating (e.g. if you sealed against PCR 0).

You will need to re-enroll the TPM-based key into a free LUKS key slot in order to restore TPM-based PIN unlocking.

First, clear any TPM-based key from the LUKS device:

```
systemd-cryptenroll --wipe-slot=tpm2
```

Then, enroll a new key as described on Trusted Platform Module.

Revision #3
Created 7 April 2023 17:40:47 by Sebin
Updated 7 April 2023 19:08:15 by Sebin