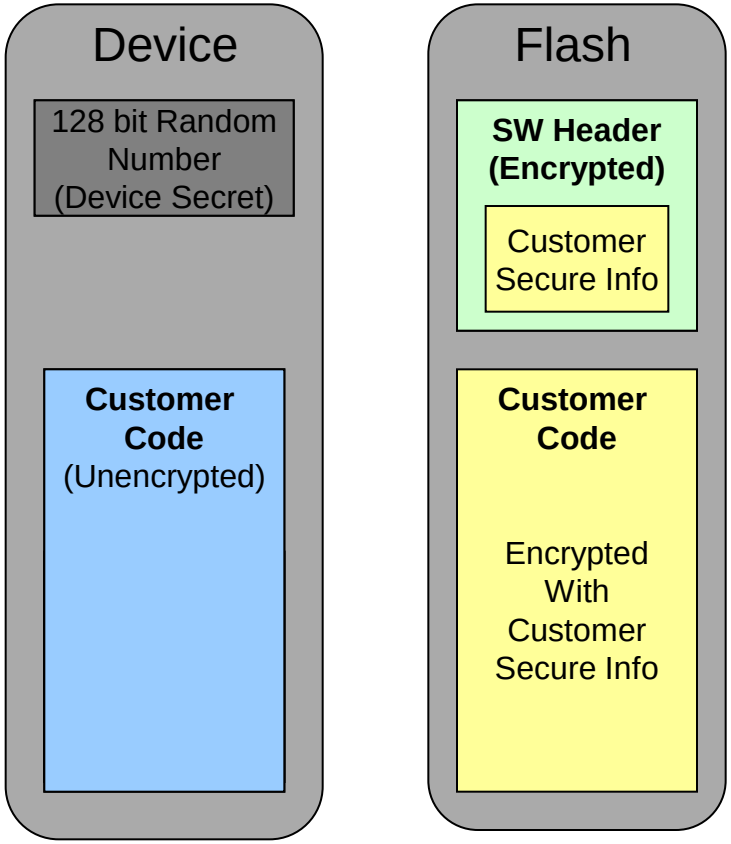
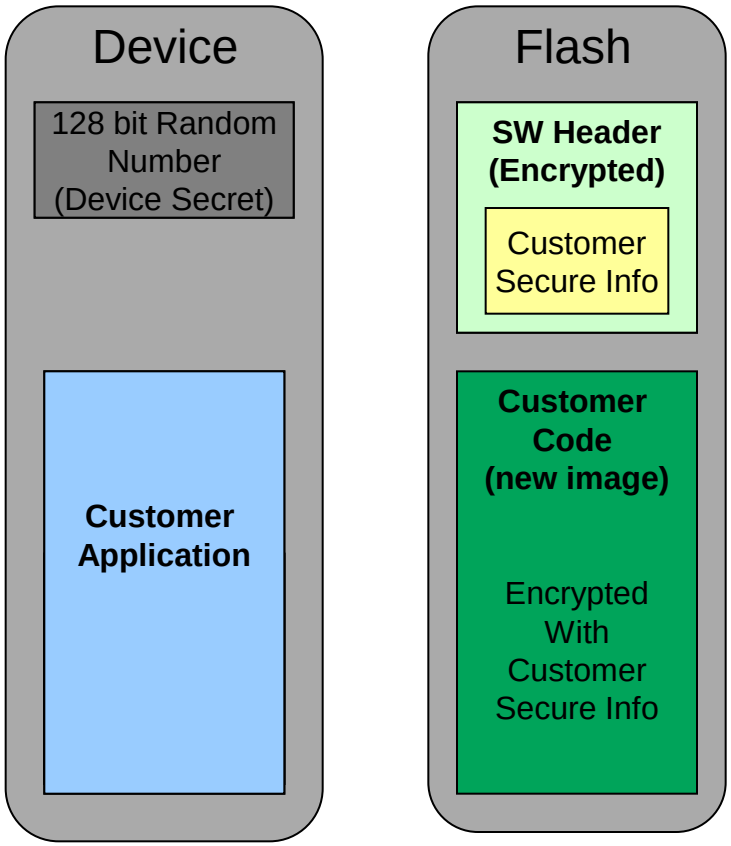
Basic Secure Boot Flow: Summary



- Initially SW Header is unencrypted
- Boot Sequence
  - On first boot:
    - Device reads SW Header
    - Device encrypts SW Header w/ Device Secret using AES
    - Device returns SW Header
  - On subsequent boots:
    - Device decrypts SW Header
    - Device uses customer key to decrypt customer code
    - Device destroys customer key
    - Device hides random number until next power-up
    - Device begins running customer code
- Advantages
  - Provides SW IP protection w/ no additional Si overhead
  - Easy field upgradability
- Disadvantages
  - SW Header initially in the clear
    - Must trust manufacturing process
  - No device takeover protection (SW can be replaced)

Easy field upgradability



- Customer encrypted code/firmware can be easily upgraded in the field
- Handled by the customer application
- Possible steps for firmware upgrade:
  1. Customer creates a new encrypted image using the customer key in a secure facility
  2. Customer application running on this device in the field acquires this new image through the available connectivity options (e.g. Ethernet)
  3. Customer application overwrites the existing customer code with the new image on the flash
- From the next boot cycle the new image will be successfully unencrypted and used