Atmega does not have a nonvaltile memory where secrets can be written without the fear that they might be deleted after reset? A solution that comes to mind is to update the new secrets using the bootloader part of the chip and just write it again in the program. How to evade this? When microcontroller restarts, it declares it ATSHA. Hence both of them restart from their original key and then update their keys every time they do authentication. Hence, the parent secret always remain there. To ensure that the parent secret is not divulged, right after start ATSHA and micro both update the parent key randomly. Hence, the key is never seen on either side.

**HMAC is not important, hence neglect it! See the end of datasheet.**

Use bootloader to encode data in flash with a key stored in ATSHA. Very ingenious idea!