

eFuses - 1Kb

BLK0 - 256-bit - system purposes

BLK1 - 256-bit - Flash Encryption key

BLK2 - 256-bit - Secure Boot key

BLK3 - 256-bit - Custom MAC address

FLASH - 4MB

DIGEST - 0x0

Bootloader + verejný kľúč - 0x1000
(Second-Stage)

Partition table - 0x10000

NVS - 0x11000

OTA_DATA - 0x15000

PHY_INIT - 0x17000

Factory_APP - Firmware 0 + podpis- 0x20000

OTA_1 - Firmware 1 + podpis - 0x120000

OTA_2 - Firmware 2 + podpis - 0x220000

Nepoužitá flash - 0x320000 - 0x3FFFFFF

Vstup - AES kľúč
z eFuse BLK2

SBDA
(Secure Boot Digest Algorithm) -
Výstup: Digest 192B
(128B IV + 64B SHA512)

ROM

Hardware Bootloader
(First-Stage)

SBDA == DIGEST?
(je zhoda?)

nie

Reštart v
nekonečnej
slučke

áno

Na základe príznaku
z OTA_DATA
partície sa bootuje
firmvér z danej
partície
(overenie dig.
podpisu)

Výber dostupnej
aplikačnej partície podľa
príznaku
FACTORY_APP /
OTA_1 / OTA_2

