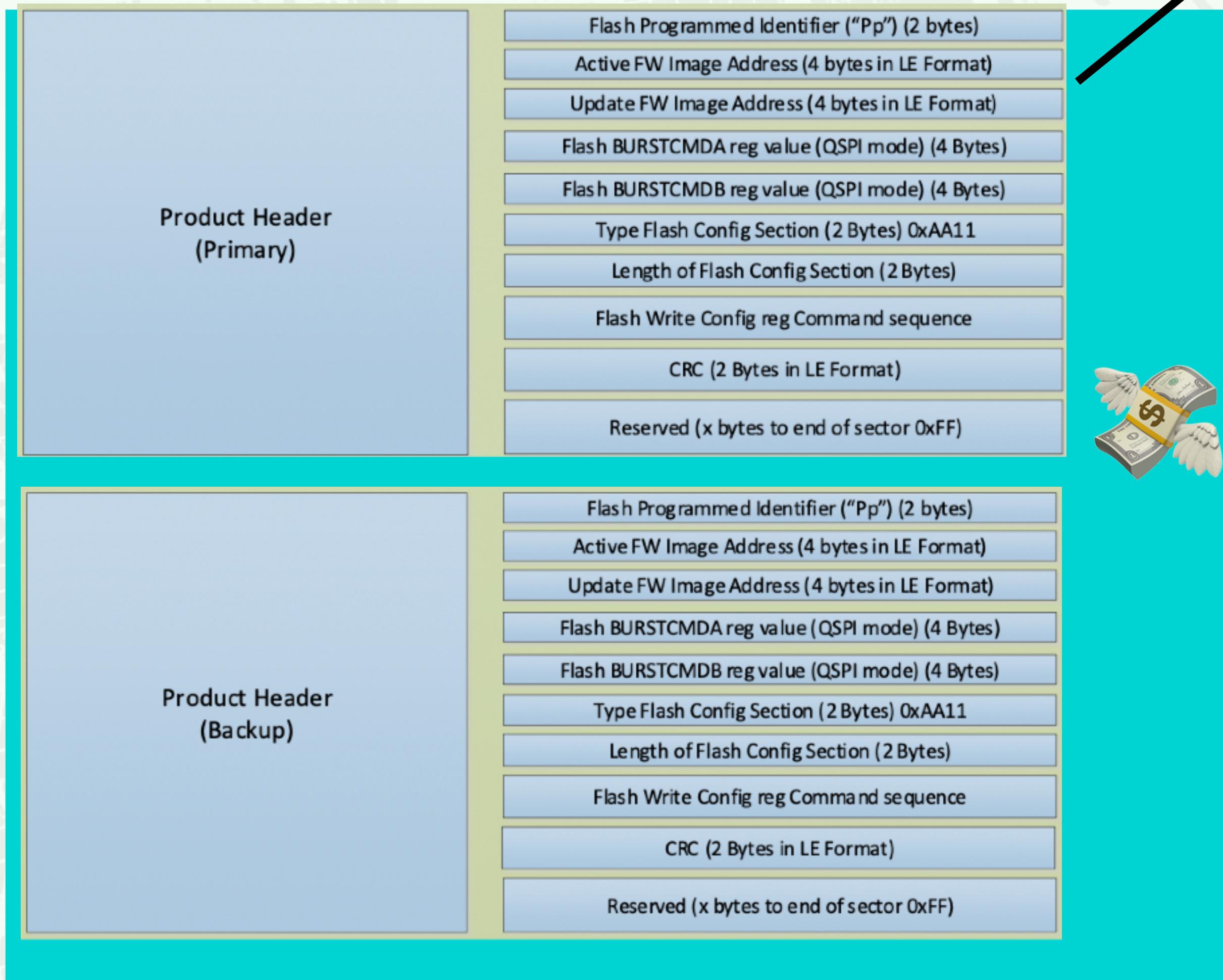


BUGS

Secureboot pain point - writable areas
Flash format defines these



Firmware Image

Image Identifier ("Qq") (2 bytes)
Size (4 Bytes in LE format)
CRC (4 Bytes in LE format)
Version String (16 Bytes)
Timestamp (4 bytes, seconds elapsed since epoch 1/1/1970)
IVT offset rel. to active FW image address (4 bytes LE format)

Security

Type Security Section (2 Bytes) 0xAA22
Length of Security Section (2 Bytes)
Index to ECC Key (1 Byte)
Index to Sym. Key (1 Byte)
NONCE (8 Bytes)
Type Signature Section (2 Bytes) 0xAA33
Length of Signature Section (2 Bytes)
Signature (TLV Format)



SIGNED

Type Device Administration Section (2 Bytes) 0xAA44
Length of Device Administration Section (2 Bytes)
Type Key revocation record (2 bytes) 0xAA55
Length of Key revocation record (2 Bytes)
KeyType (0xA1 = Sign key, 0xA2 = Decr. Key, 0xA3 = User Data Key)
Key Index (1 Byte)
:
KeyType (0xA1 = Sign key, 0xA2 = Decr. Key, 0xA3 = User Data Key)
Key Index (1 Byte)

| IVT |
| Executable |

ENCRYPTED

PRODUCT HEADER VALIDATION

