

ENCRYPTION

Key Indexes

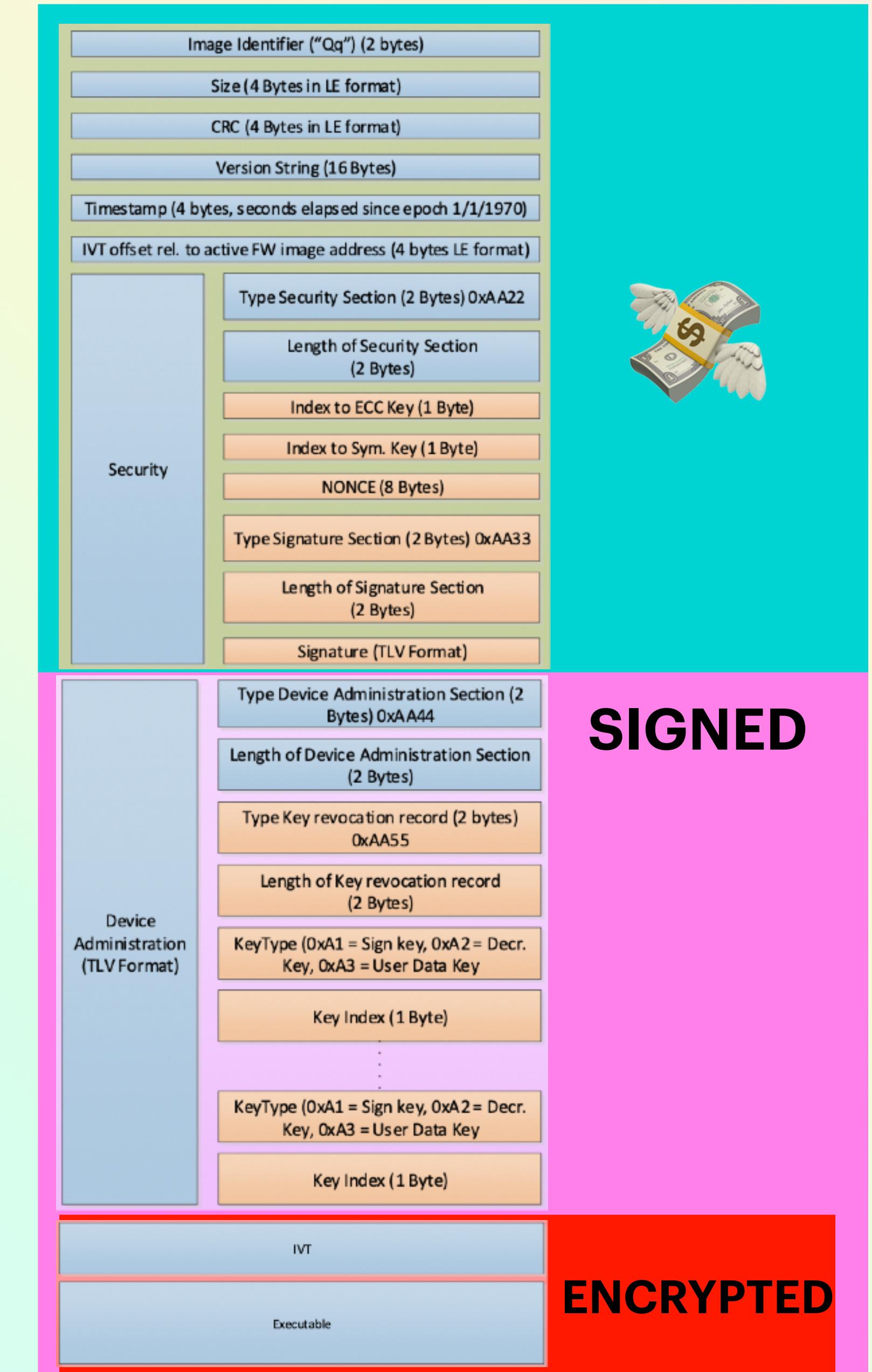
- Index into OTP for encryption engine

Nonce

- User defined Nonce
- Avoid IV reuse

AES-CTR mode enables fast/arbitrary block decryption

AES-CTR provides no auth (malleable)



**“A CORRUPTED NONCE COULD
NOT BE USED TO EXECUTE
ARBITRARY CODE, RIGHT?”**

ME, PROBABLY