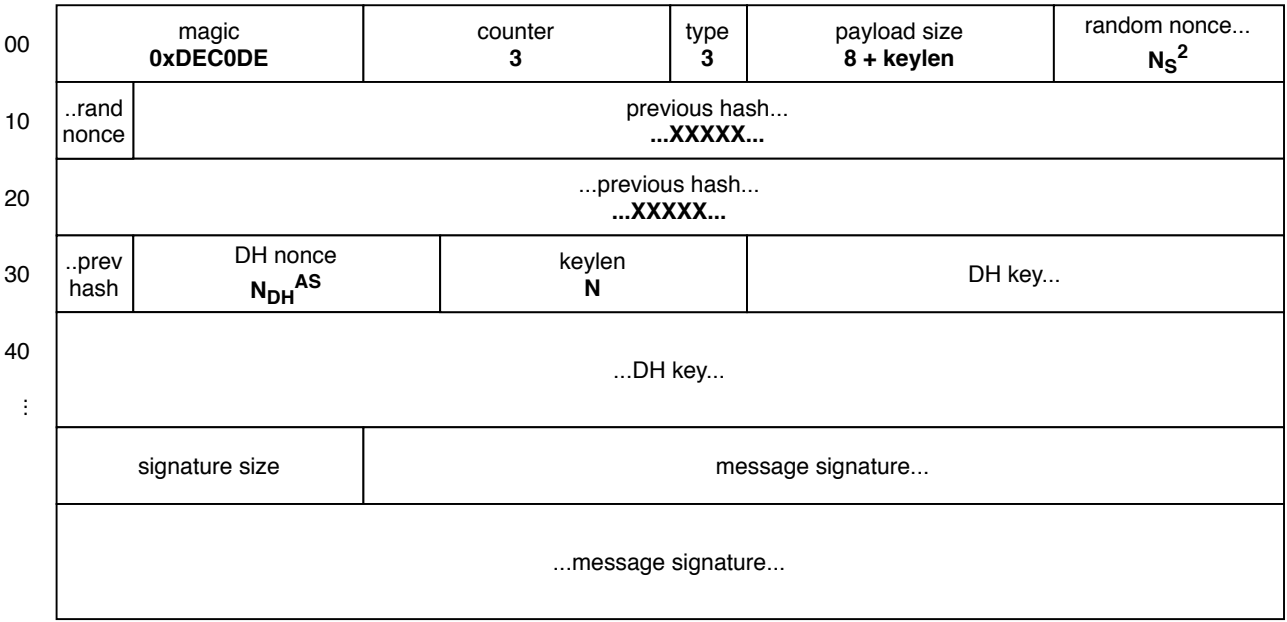
0 1 2 3 4 5 6 7 8 9 A B C D E F
00
magic
0xDEC0DE
counter
3
type
3
payload size
8 + keylen
random nonce...
N_S^2
10
..rand nonce
previous hash...
...XXXXX...
20
...previous hash...
...XXXXX...
30
..prev hash
DH nonce
N_{DH}^{AS}
keylen
N
DH key...
40
...DH key...
signature size
message signature...
...message signature...