Negotiation of multiple Child SA with IKEv2

draft-mglt-ipsecme-multiple-child-sa-00

Migault, Klassert

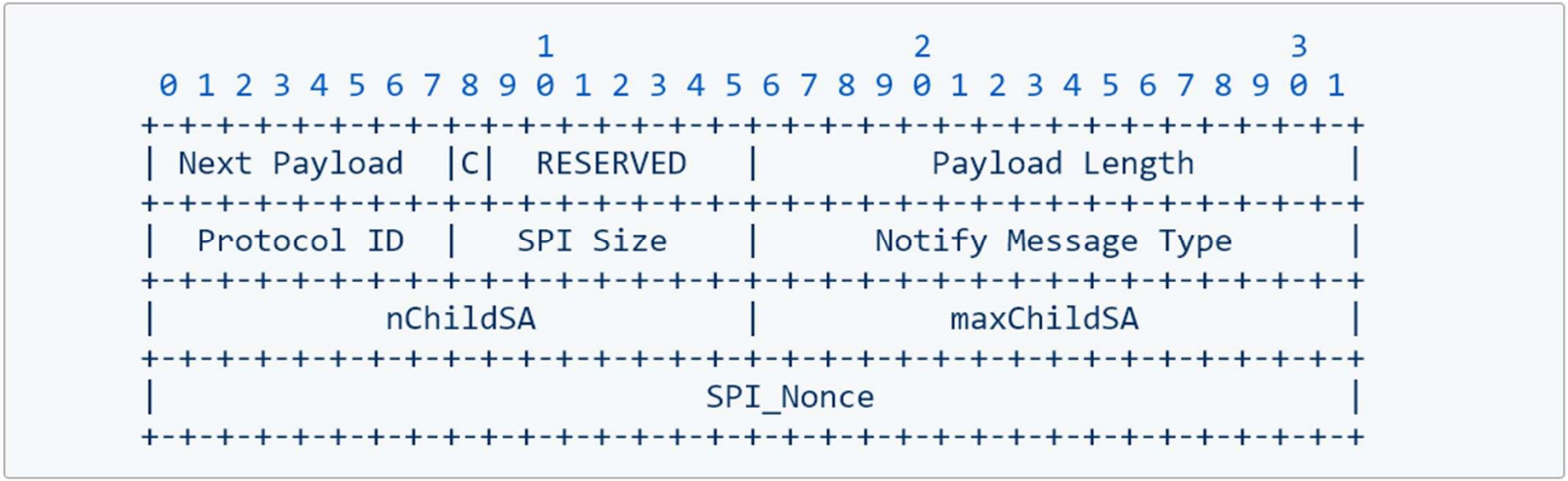
Goal: Create an agreed number n of child SAs

```
initiator                              responder
-------------------------------------------------------------------
HDR, SK {IDi, [CERT,] [CERTREQ,]
    [IDr,] AUTH, SAi2, TSi, TSr,
    N(MULTIPLE_CHILD_SA(nChildSAi, maxChildSA, SPIi_Nonce))}  -->

                <--  HDR, SK {IDr, [CERT,] AUTH,
                           SAr2, TSi, TSr,
                            N(MULTIPLE_CHILD_SA(nChildSA, maxChildSA, SPIr_Nonce))}
```

- nChildSAi: proposed number of additional SAs
- maxChildSA: the maximum allowed number of Child SAs
- nChildSA: agreed number of additional SAs -- in [nChildSAi, maxChildSA]
- SPIi_Nonce, SPIr_Nonce: Nonce to generate SPIs

Derivation of parameters:

```
{KEYMAT_ChildSA, KEYMAT_1..., KEYMAT_nChildSA } = prf+(SK_d, Ni | Nr)

{SPIi_1, ..., SPIi_nChildSA} = prf+(SPIi_Nonce)
{SPIr_1, ..., SPIr_nChildSA} = prf+(SPIr_Nonce)
```


1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Payload
C
RESERVED
Payload Length
Protocol ID
SPI Size
Notify Message Type
nChildSA
maxChildSA
SPI_Nonce

Thanks!