IKEv2 Count Based SA Extension

Migault, Liu, Zhang

Problem Statement

Hardware accelerated IPsec:

- Are designed for a fix number of SAs
- SAs that cannot be created result in traffic being rejected.

Simultaneous IKEv2 rekeys result in the creation of redundant SAs

- underutilisation of the hardware component

SAs life time can be expressed using a time or a byte count limit.

Time limit:

- makes limit predictable (over time)
  - it is easy to anticipate the expiration time
- Uniformly randomizing time limit distributes the IKEv2 rekey uniformly
  - and works pretty well

byte count limit:

- are hard to predict - as it depends on the traffic.
  - our implementation checks every 2s which SAs needs to be rekeys
- the randomization does not compensate the traffic bursts

As a result, count bases SA results in multiple redundant rekey

Why we want to use byte count limit ?

- a direct expression of the lifetime of the cryptographic key
- binding the SA life time to traffic is appropriated for device that can be in long sleeping mode.

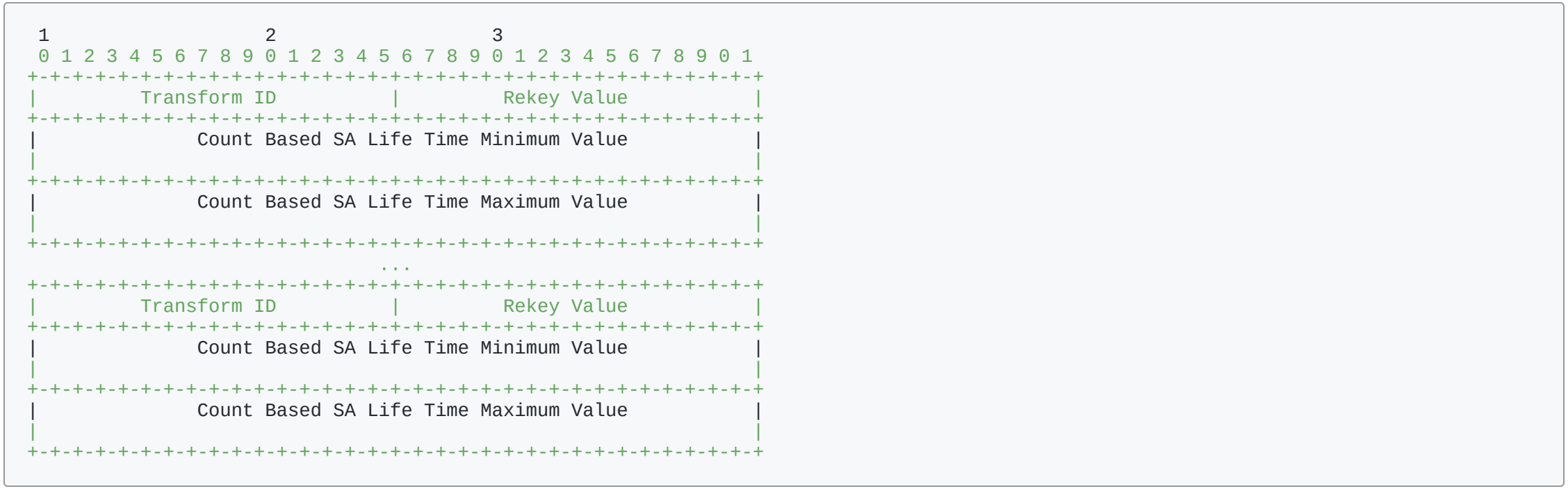
The document describes an IKEv2 extension the prevents redundant rekey:

- no magic: peers agree who is expected to start the rekey

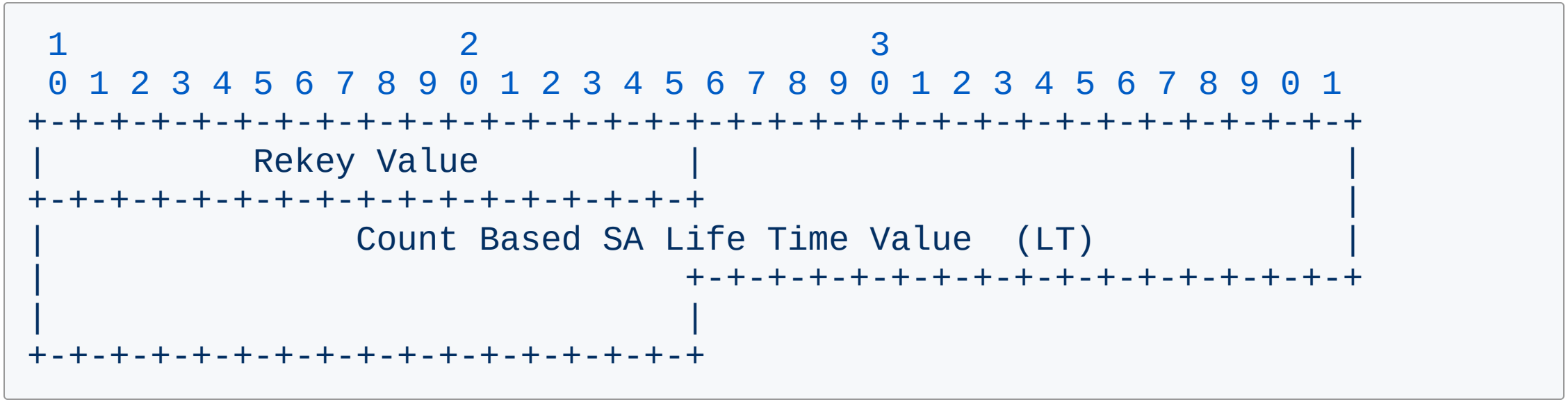
```
Initiator                                Responder
-----------------------------------------------
HDR, SAi1, KEi, Ni  -->
                          <--  HDR, SAr1, KEr, Nr, [CERTREQ]
HDR, SK {IDi, [CERT,] [CERTREQ,]
    [IDr,] AUTH, SAi2,
    TSi, TSr, N(COUNT_BASED_SA_PROPOSED)}  -->
                          <--  HDR, SK {IDr, [CERT,] AUTH,
                             SAr2, TSi, TSr, N(COUNT_BASED_SA_SELECTED)}
```

COUNT_BASED_SA_PROPOSED Notification Data contains for each Transform ID:

- Acceptable count base life time
- Rekey Value (random)



COUNT_BASED_SA_SELECTED Notification Data



1. Selection of the initiator for the next rekey:

- The peer with the greatest Rekey Value is designated to initiate the next rekey.
- In case of equality, the current initiator remains the initiator.

2. setting the Hard (H) and Soft (S) count base SA lifetime:

- initiator:
  - S = X_i * LT + rand(0, 5% LT) with X_i <= 80%
  - H = LT
- responder :
  - S = X_r LT + rand(0, 5% LT) with X_r >= 95%
  - H = LT

Thanks!