IKEv2 Optional SA&TS Payloads in Child Exchange

https://datatracker.ietf.org/doc/draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt/

Sandeep Kampati (Huawei)

Wei Pan (Huawei)

Paul Wouters (Aiven)

Meduri Bharath (Mavenir)

Meiling Chen (CMCC)

Michael Richardson (SSW)

IETF 113

March 2022

Solution Recap:

- Negotiation of Support for OPTIMIZED REKEY

```
Initiator                           Responder
-----------------------------------------------------------------------
HDR, SK {IDi, [CERT,] [CERTREQ,]
    [IDr,] AUTH, SAi2, TSi, TSr,
    N(OPTIMIZED_REKEY_SUPPORTED)} -->
                                    <-- HDR, SK {IDr, [CERT,] AUTH,
                                        SAr2, TSi, TSr,
                                        N(OPTIMIZED_REKEY_SUPPORTED)}
```

- Optimized Rekey of the IKE SA

```
Initiator                           Responder
-----------------------------------------------------------------------
HDR, SK {N(OPTIMIZED_REKEY,newSPIi),
    Ni, KEi} -->
                                    <-- HDR, SK {N(OPTIMIZED_REKEY,newSPIr),
                                        Nr, KEr}
```

Note: The current SPI is from the IKE header.

- Optimized Rekey of Child SAs

```
Initiator                           Responder
-----------------------------------------------------------------------
HDR, SK {N(REKEY_SA,currentSPI), N(OPTIMIZED_REKEY,newSPIi),
    Ni, [KEi,]} -->
                                    <-- HDR, SK {N(OPTIMIZED_REKEY,newSPIr),
                                        Nr, [KEr,]}
```

Updates from -07 to -08

- Most are editorial changes
- Clearly show how new and old SPIs are included in the Child Exchange
  - At rekeying IKE SA:
    - The current SPI is included in the IKE header.
    - The newSPIs are respectively included in the initiator and responder's OPTIMIZED_REKEY payloads.
  - At Rekeying Child SA:
    - The current SPI is included in the initiator’s REKEY_SA payload.
    - The newSPIs are respectively included in the initiator and responder's OPTIMIZED_REKEY payloads.

Next Step

- Ask for WG adoption
  - The authors believe current version is clear and mature.