IKEv2 Optional SA&TS Payloads in Child Exchange

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

Sandeep Kampati	Huawei Technologies
Meduri S S Bharath	Huawei Technologies
Wei Pan	Huawei Technologies

IETF 105, Montreal

July 2019

Motivations

- Original Rekeying IKE SAs:

```
Initiator                                          Responder
-----------------------------------------------------------------------
HDR, SK {SA, Ni, KEi} -->
                                          <-- HDR, SK {SA, Nr, KEr}
```

- Original Rekeying Child SAs:

```
Initiator                                          Responder
-----------------------------------------------------------------------
HDR, SK {N(REKEY_SA), SA, Ni, [KEi,]
    TSi, TSr} -->
                                          <-- HDR, SK {SA, Nr, [KEr,]
                                                  TSi, TSr}
```

- If the configurations (the cryptographic suites and ACLs) haven't changed, the negotiation result will remain the same after the SA & TS payloads are processed.
- IKE SAs and Child SAs rekeying happen periodically. For the constrained devices, like IoT devices, processing the SA & TS payloads in such case is a periodic burden that can be omitted.
- More than 100,000 IKE/IPSEC tunnels can be used in 5G networks cRAN/Cloud. The bandwidth that the SA & TS payloads occupied can be huge in such case.

Optimization Solutions

- Sending a new notification payload with the SPI value instead of the SA payloads at rekeying IKE SAs, when there is no change of cryptographic suite configurations.

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

- Sending a new notification payload with the SPI value instead of the SA & TS payloads at rekeying Child SAs, when there is no change of cryptographic suite and ACL configurations.

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

Optimization Support Negotiation

- Send the MINIMAL_REKEY_SUPPORTED notification at the IKE_AUTH message exchange to indicate the support for optimizing the payloads at rekeying IKE SAs and Child SAs.

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

- MINIMAL_REKEY_SUPPORTED Notification Payload Format

```
 0                   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(=0)| SPI Size (=0) |      Notify Message Type      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

o Protocol ID (1 octet) - MUST be 0.

o SPI Size (1 octet) - MUST be 0, meaning no SPI is present.

o Notify Message Type (2 octets) - MUST be <Need to get value from IANA>.

This notification contains no data.

Rekeying IKE SAs Optimization

- 1. No change of cryptographic suites (CS) in Initiator and Responder

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

- 2. Initiator's CS changed, while Responder's CS haven't changed
  - 2.1. Different CS sent by the Initiator (equal to the original way)

```
Initiator                                          Responder
-----------------------------------------------------------------------
HDR, SK {SA, Ni, KEi} -->
                                        <-- HDR, SK {SA, Nr, KEr}
```

  - 2.2. Previously negotiated CS still sent by the Initiator

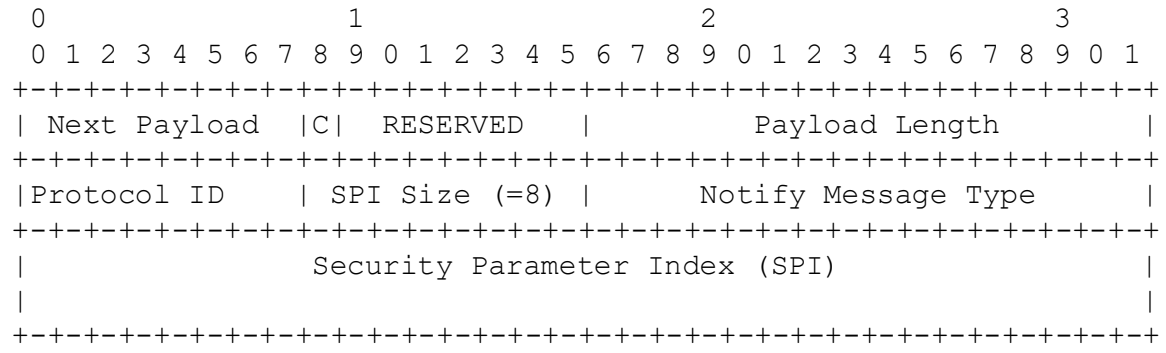
```
Initiator                                          Responder
-----------------------------------------------------------------------
HDR, SK {SA, Ni, KEi} -->
                                        <-- HDR, SK {N(SA_UNCHANGED), Nr, KEr}
```

- 3. Responder's CS Changed, while Initiator's CS haven't changed

```
Initiator                                          Responder
-----------------------------------------------------------------------
HDR, SK {N(SA_UNCHANGED), Ni, KEi} -->
                                        <-- HDR, SK {N(NO_PROPOSAL_CHOSEN), Nr, KEr}
HDR, SK {SA, Ni, KEi} -->
                                        <-- HDR, SK {SA, Ni, KEi}
```

Rekeying IKE SAs Optimization

- SA_UNCHANGED Notification Payload Format



- Protocol ID (1 octet) - MUST be 1.
- SPI Size (1 octet) - MUST be 8.
- Notify Message Type (2 octets) - MUST be <Need to get value from IANA>.
- SPI (8 octets) - Security Parameter Index.

Rekeying Child SAs Optimization

- 1. No change of CS and ACL in Initiator and Responder

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

- 2. Initiator's CS or ACL changed, while Responder's CS and ACL haven't changed
  - 2.1. Different CS or Traffic Selectors sent by the Initiator (equal to the original way)

```
Initiator                                        Responder
-----------------------------------------------------------------------------
HDR, SK {N(REKEY_SA), SA, Ni, [KEi,]
    TSi, TSr} -->
                                        <-- HDR, SK {SA, Nr, [KEr,]
                                            TSi, TSr}
```

  - 2.2. Previously negotiated CS and Traffic Selectors still sent by the Initiator

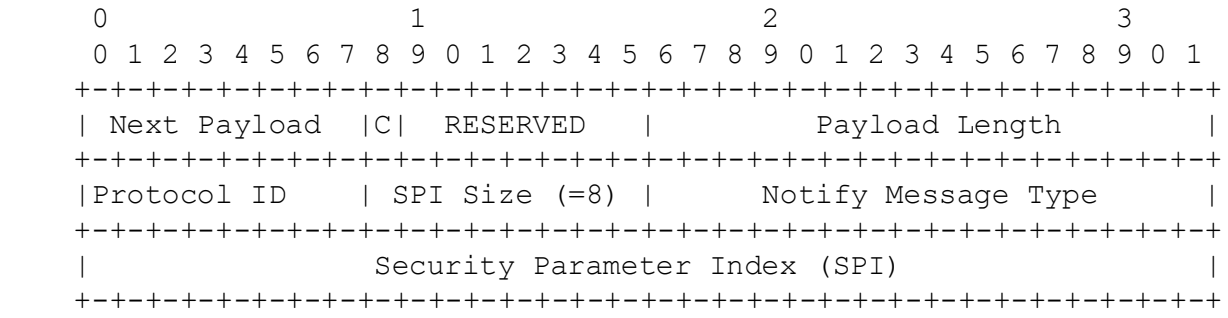
```
Initiator                                        Responder
-----------------------------------------------------------------------------
HDR, SK {N(REKEY_SA), SA, Ni, [KEi,]
    TSi, TSr} -->
                                        <-- HDR, SK {N(SA_TS_UNCHANGED), Nr, [KEr]}
```

- 3. Responder's CS or ACL Changed, while Initiator's CS and ACL haven't changed

```
Initiator                                        Responder
-----------------------------------------------------------------------------
HDR, SK {N(REKEY_SA), N(SA_TS_UNCHANGED),
    Ni, [KEi]} -->
                                        <-- HDR, SK {N(NO_PROPOSAL_CHOSEN),
                                            Nr, KEr}
HDR, SK {N(REKEY_SA), SA, Ni, [KEi,]
    TSi, TSr} -->
                                        <-- HDR, SK {SA, Nr, [KEr,]
                                            TSi, TSr}
```

Rekeying Child SAs Optimization

- SA_TS_UNCHANGED Notification Payload Format



- Protocol ID (1 octet) - MUST be either (2) to indicate AH or (3) to indicate ESP.
- SPI Size (1 octet) - MUST be 4.
- Notify Message Type (2 octets) - MUST be <Need to get value from IANA>.
- SPI (4 octets) - Security Parameter Index.

Rekeying IKE SAs Packet Format Comparison

IKE rekey Exchange format with single cryptographic Suites

HDR, SK {**SA**, Ni, KEi}

```
                    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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       IKE SA Initiator SPI                    |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       IKE SA Responder SPI                    |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Payload | MjVer | MnVer | Exchange Type |     Flags     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Message ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Length                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Last Substruc |   RESERVED    |         Proposal Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Proposal Num  |  Protocol ID  |    SPI Size   |Num  Transforms|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                        SPI (variable)                         ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Last Substruc |   RESERVED    |        Transform Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Transform Type |   RESERVED    |  Transform ID = ENCR_AES_CBC    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|A|       Attribute Type        |    AF=0  Attribute Length       |
|F|                             |    AF=1  Attribute Value        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Last Substruc |   RESERVED    |        Transform Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Transform Type |   RESERVED    |   Transform ID=PRF_HMAC_SHA1    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Last Substruc |   RESERVED    |        Transform Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Transform Type |   RESERVED    | Transform ID = AUTH_HMAC_SAH1   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Last Substruc |   RESERVED    |        Transform Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Transform Type |   RESERVED    | Transform ID = DH768-bit        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                         Nonce Data                            ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Diffie-Hellman Group Num    |           RESERVED              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                      Key Exchange Data                        ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IKE Header

Transform ENCR

Transform PRF

Transform AUTH

Transform DH

Proposal

SA

Nonce

KE

Packet format of IKE Rekey

HDR, SK {**N(SA_UNCHANGED)**, Ni, KEi}

```
                    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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       IKE SA Initiator SPI                    |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       IKE SA Responder SPI                    |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Payload | MjVer | MnVer | Exchange Type |     Flags     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Message ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Length                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Protocol ID  | SPI Size=8    |Notify Message Type              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~            Security Parameter Index (SPI)                     ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                         Nonce Data                            ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Diffie-Hellman Group Num    |           RESERVED              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                      Key Exchange Data                        ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IKE Header

SA_UNCHANGED Notify

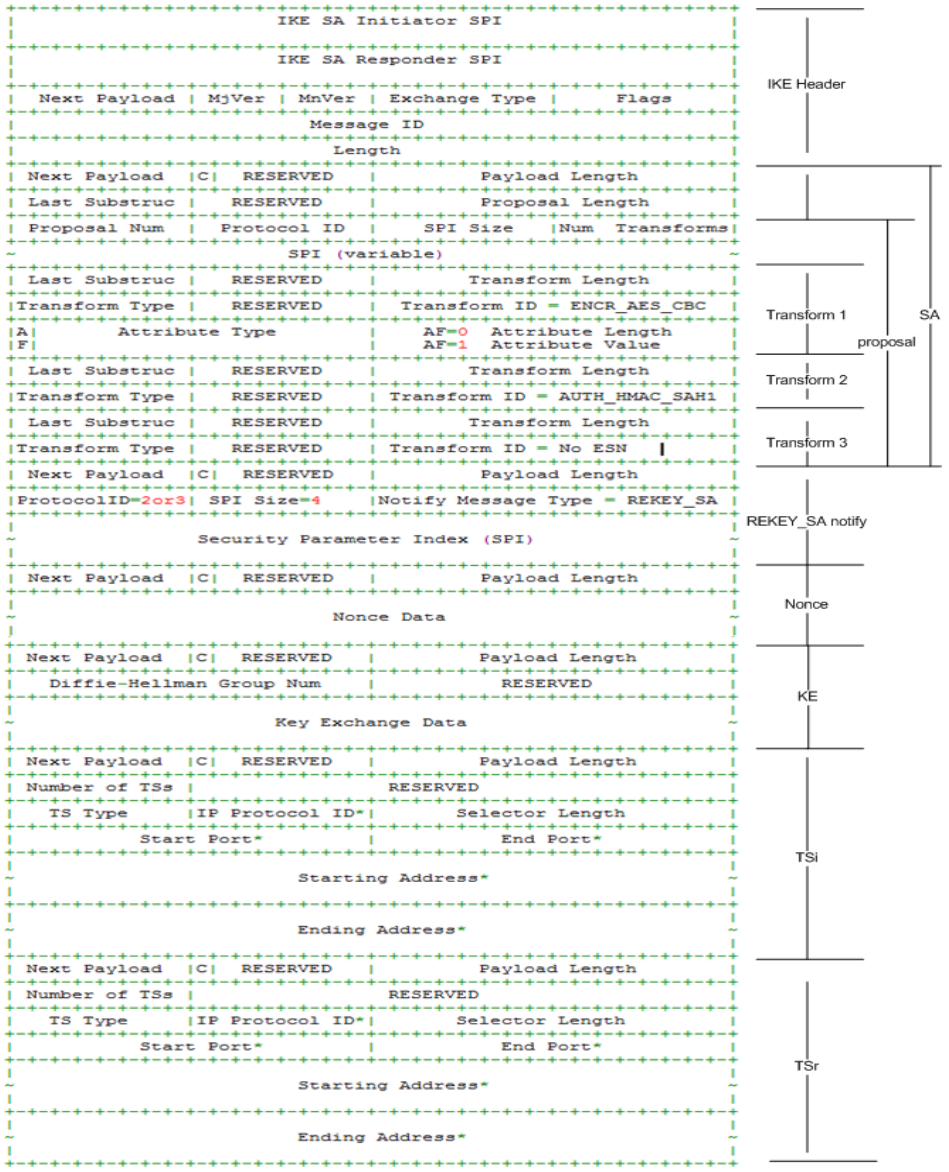
Nonce

KE

Rekeying IPSec SAs Packet Format Comparison

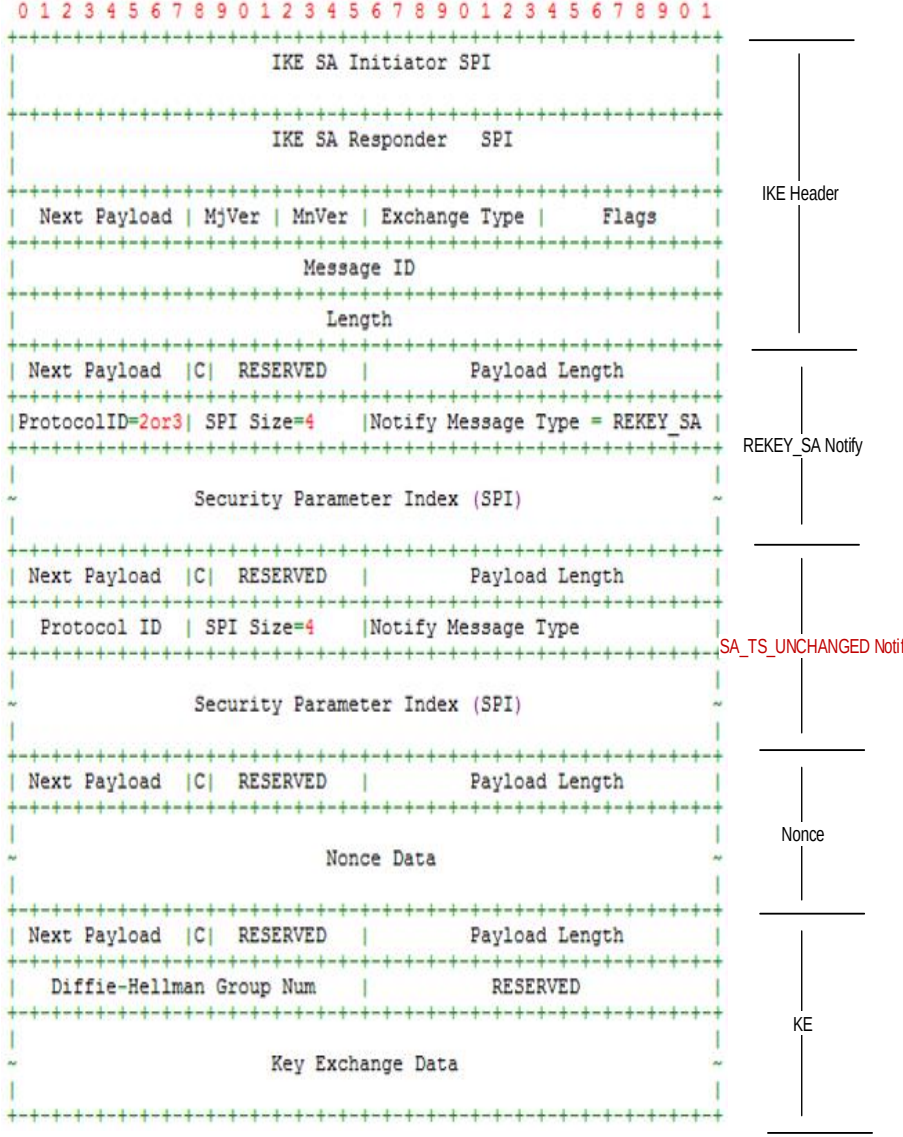
IPSEC rekey Exchange format with single cryptographic Suites

HDR, SK {N(REKEY_SA), **SA**, Ni, [KEi],**TSi**, **TSr**}



Packet format of IPSEC Rekey

HDR, SK {N(REKEY_SA), **N(SA_TS_UNCHANGED)**, Ni, [KEi]}



Optimization Effect

Rekeying Type	Minimum payloads length before optimization	Payloads length after optimization	Reduced bytes / percentage
IKE	112 bytes	76 bytes	36 bytes / 32%
AH (IPv4)	112 bytes	44 bytes	68 bytes / 61%
AH (IPv6)	160 bytes	44 bytes	116 bytes / 73%
ESP (IPv4)	112 bytes	44 bytes	68 bytes / 61%
ESP (IPv6)	160 bytes	44 bytes	116 bytes / 73%

- If more than one cryptographic suites are contained in the SA payload, then the reduced bytes / percentage will increase linearly.

Future Plan

- More comments and reviews
- WG Adoption

Appendix: Bytes Calculation

- Minimum SA payload length calculation:

```
Protocol    Mandatory Transform Types    Optional Transform Types
-------------------------------------------------------------------
IKE         ENCR, PRF, INTEG*, D-H
ESP         ENCR, ESN                    INTEG, D-H
AH          INTEG, ESN                   D-H
SA(IKE) = 4(header) + 8(proposal) + 8(SPI) + 4 * 8(per transform) = 52 bytes
SA(AH)  = 4(header) + 8(proposal) + 4(SPI) + 2 * 8(per transform) = 32 bytes
SA(ESP) = 4(header) + 8(proposal) + 4(SPI) + 2 * 8(per transform) = 32 bytes
```

- Other payloads length calculation:

```
Nx  = 4(header) + 16(the least nonce value) = 20 bytes
KEx = 8(header) + 32(256-bit ECDSA) = 40 bytes
N(REKEY_SA) = 8(header) + 4(SPI) = 12 bytes
TS(IPv4) = 8(header) + 8(TS header) + 4(starting address) + 4(ending address) = 24 bytes
TS(IPv6) = 8(header) + 8(TS header) + 16(starting address) + 16(ending address) = 48 bytes
```

- New payloads length calculation:

```
N(SA_UNCHANGED) = 8(header) + 8(SPI) = 16 bytes
N(SA_TS_UNCHANGED) = 8(header) + 4(SPI) = 12 bytes
```

- Total payloads length calculation:

```
IKE = SA(IKE) + Nx + KEx = 112 bytes
AH(IPv4) = N(REKEY_SA) + SA(AH) + Nx + 2 * TS(IPv4) = 112 bytes
AH(IPv6) = N(REKEY_SA) + SA(AH) + Nx + 2 * TS(IPv6) = 160 bytes
ESP(IPv4) = N(REKEY_SA) + SA(ESP) + Nx + 2 * TS(IPv4) = 112 bytes
ESP(IPv6) = N(REKEY_SA) + SA(ESP) + Nx + 2 * TS(IPv6) = 160 bytes

IKE(Optimized) = N(SA_UNCHANGED) + Nx + KEx = 76 bytes
AH(Optimized)  = N(REKEY_SA) + N(SA_TS_UNCHANGED) + Nx = 44 bytes
ESP(Optimized) = N(REKEY_SA) + N(SA_TS_UNCHANGED) + Nx = 44 bytes
```