

# 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)

IETF 111, Online

July 2021

# Updates from -02 to -07

- Whole solution is much simpler, text is more readable
  - 3 steps of optimization:
    - Negotiation of support for rekey optimization
    - Initiator and responder omit the SA payloads at rekeying IKE SAs
    - Initiator and responder omit the SA and TS payloads at rekeying Child SAs
  - No more consideration for the situation of configuration change
  - 2 new Notify Message type notifications are needed (Previous was 3)

<b>3. Protocol Details</b>
3.1. Negotiation of Support for Optimizing Optional Payload at Rekeying IKE SAs and Child SAs
3.2. Payload Optimization at Rekeying IKE SAs
3.2.1. Rekeying IKE SAs When No Change of Initiator and Responder's Cryptographic Suites
3.2.2. Rekeying IKE SAs When Responder's Cryptographic Suites Changed
3.3. Payload Optimization at Rekeying Child SAs
3.3.1. Rekeying Child SAs When No Change of Initiator and Responder's Cryptographic Suites and ACL Configuration
3.3.2. Rekeying Child SAs When Responder's Cryptographic Suites or ACL Configuration Changed
<b>4. Payload Formats</b>
4.1. MINIMAL_REKEY_SUPPORTED Notification
4.2. SA_UNCHANGED Notification
4.3. SA_TS_UNCHANGED Notification

**Previous**

<b>3. Negotiation of Support for OPTIMIZED REKEY</b>
<b>4. Optimized Rekey of the IKE SA</b>
<b>5. Optimized Rekey of Child SAs</b>
<b>6. Payload Formats</b>
6.1. OPTIMIZED_REKEY_SUPPORTED Notify
6.2. OPTIMIZED_REKEY Notify

**Current**

- Two co-authors added: Paul Wouters (Aiven), Meiling Chen (CMCC)

# 3 Steps of Optimizations

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

- Optimized Rekey of Child SAs

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

# Open questions

- 1) Should the SUPPORTED notify mean that peers MAY/SHOULD/MUST use this method?
- 2) Alternatively, the SUPPORTED notify could have a payload that signifies whether the old method is supported or not.
- 3) When a Child SA was negotiated with PFS, what should an optimized rekey do when there is no KE payload? Send INVALID\_KE\_PAYLOAD?

# Next Steps

- Ask for WG adoption
- Discuss and close the open questions
- Looking for implementations to do interop testing