Optimized Rekeys in the IKEv2

draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt

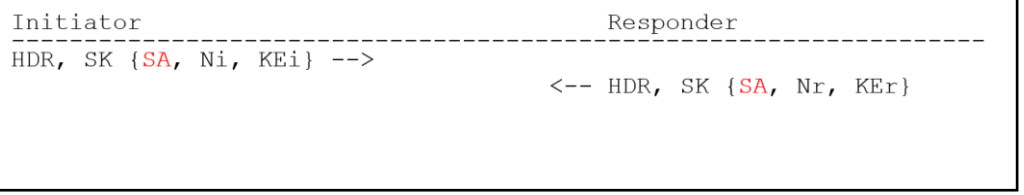
Sandeep Kampati (Microsoft)
Wei Pan (Huawei)
Paul Wouters (Aiven)
Meduri Bharath (Mavenir)
Meiling Chen (CMCC)
Valery Smyslov (ELVIS-PLUS)

IPsec Workshop & IETF 126
July 2026

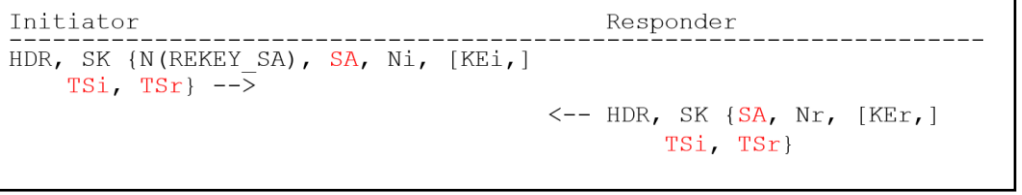
Re-cap: Motivations

- **Current rekeying is:**

Original Rekeying IKE SAs



Original Rekeying Child SAs



- **Parameters for the SAs, which are already known by two peers, are still included in the messages**
  - Even include all the proposals sent in the initial stage
- **In RFC 7296 Section 2.8, it says:**
  - `Note that, when rekeying, the new Child SA` **`SHOULD NOT have different Traffic Selectors and algorithms`** `than the old one`
- **So, omitting the SA&TS payloads during rekey:**
  - doesn't violate RFC 7296,
  - can save the bandwidth in wire and reduce the CPU operations.

Re-cap: Solutions

- **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,]}
```

Re-cap: Interaction with other extensions

- **RFC 9370 Multiple Key Exchanges:**
  - If multiple key exchange methods are used, then **optimized rekey MUST use the same key exchange methods**. CREATE_CHILD_SA will be followed by some IKE_FOLLOWUP_KE exchanges of additional key exchange methods.
- **RFC 5723 Session Resumption:**
  - **Support for optimized rekeys MUST be re-negotiated during the resumption** (in the IKE_AUTH exchange).
  - All IKE SA algorithms, including key exchange methods, are taken from the resumption ticket.
  - Initial Child SA created during the resumption is considered as been created with key exchange methods for the IKE SA. This is despite the fact, that during the resumption no key exchanges (e.g., Diffie-Hellman) take place, the session keys are derived from the keys stored in the resumption ticket.
- **RFC 9867 Mixing Preshared Keys in the CREATE_CHILD_SA Exchanges**
  - If peers support [RFC9867] and a PPK was used for the SA being rekeyed, then they **MUST NOT silently re-use this PPK** in case of optimized rekey and **MUST re-negotiate the use of PPKs in the CREATE_CHILD_SA exchange**.

Re-cap: Optimized Rekey of Initial Child SA

- **Problem recap:**
  - PFS policy & KE method(s) for Child SAs are not negotiated during the creation of the initial Child SA
  - Problem 1: Mismatched configuration causes the rekey fails
  - Problem 2: What KE method(s) to use is not known when rekey for the first time
- **If draft-ietf-ipsecme-child-pfs-info is used:**
  - PFS policy and KE method(s) for the initial Child SA is known during its creation.
  - When rekeying the initial Child SA for the first time, the optimized way SHOULD be used.
- **If draft-ietf-ipsecme-child-pfs-info is not supported or used:**
  - A regular rekey MUST be used for the first time to negotiate these parameters. Then, the next rekey can use the optimized way.

Status

- **Being stable since v05 in July 2025**
  - Interaction with other extensions and optimized rekeying of the initial Child SA have been addressed.
  - No other technical issues raised.
- **v06 and v07 in January 2026, and v08 in March 2026**
  - Editorial changes
  - Update the references

What’s the next?

- **Is the WG still interested in this document?**
- **How to proceed? WGLC?**
- **Wait for draft-ietf-ipsecme-child-pfs-info?**