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)

IETF 123
July 2025

Changes v04 – v05

- **Interaction with draft-ietf-ipsecme-ikev2-qr-alt**
  - Add section 7.3
  - The use of PPKs must also be re-negotiated in the optimized rekeys
- **Optimized Rekey of the Initial Child SA**
  - Move to a dedicated section 5.1
  - Rely on draft-pwouters-ipsecme-child-pfs-info
    - If it is used, the first rekey should be the optimized way
    - If not used, the first rekey must be the regular way
- **Editorial changes**

Interaction with draft-ietf-ipsecme-ikev2-qr-alt

- **Section 5 “Optimized Rekey of Child SAs”**
  - Except for the key and identification information such as the SPI and CPI, all other properties of the Child SA being rekeyed MUST be inherited to the one newly created by the optimized rekey. Notify payloads that can affect these properties, such as USE_TRANSPORT_MODE, ESP_TFC_PADDING_NOT_SUPPORTED, ROHC_SUPPORTED [RFC5857] or USE_AGGFRAG [RFC9347] MUST NOT be sent.
    In contrast, the Post-quantum Preshared Keys (PPKs) defined in [I-D.ietf-ipsecme-ikev2-qr-alt] can be considered as part of the key information since they are used in the session keys calculations, therefore, the PPKs negotiation MUST be included in the optimized Child SA rekey if [I-D.ietf-ipsecme-ikev2-qr-alt] are used.

- **Section 7.3 “Mixing Preshared Keys in the CREATE_CHILD_SA Exchanges”**
  - **[I-D.ietf-ipsecme-ikev2-qr-alt] defines how PPKs can be mixed into the session keys calculations. In particular, this document allows PPKs to be used in the CREATE_CHILD_SA exchanges when SAs are being rekeyed. If peers support [I-D.ietf-ipsecme-ikev2-qr-alt] 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.**

Optimized Rekey of the 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
- **Several solution options provided at last meeting, and simple solution is preferred**
  - Directly try optimized rekey and go back to regular rekey if failed
    - not feasible in multiple KEs situation
  - Or, use regular rekey for the first time and optimized rekey for the next times
    - A little bit sad 😔 because our goal is to avoid regular rekey as much as possible
- **No perfect solution, but what if the PFS policy & KE method(s) can be negotiated when creating the initial Child SA?**

Negotiate KE methods for the Initial Child SA

- **Valery suggested one possible solution for draft-pwouters-ipsecme-child-pfs-info**
  - Lift the prohibition for KE transforms to appear in the SA payloads in IKE_AUTH
  - Negotiate KE method(s) in the IKE_AUTH, but don't use them for computing session keys for initial Child SA

```
Initiator                          Responder
-----------------------------------------------------------------
HDR, SAi1, KEi, Ni
   N(EARLY_CHILD_PFS_INFO)  -->
                           <--  HDR, SAr1, KEr, Nr, [CERTREQ],
                                   N(EARLY_CHILD_PFS_INFO)
```

IKE_INIT_SA Exchange

```
Initiator                          Responder
-----------------------------------------------------------------
HDR, SK {IDi, [CERT,] [CERTREQ,]
   [IDr,] AUTH, SAi2_with_KE,
   TSi, TSr}  -->
                                <--  HDR, SK {IDr, [CERT,] AUTH,
                                        SAr2_with_KE, TSi, TSr}
```

IKE_AUTH Exchange

- Allow **full-fledged negotiation of KE methods identical to what CREATE_CHILD_SA allows** with no restrictions on the policy (or these restrictions are the same as for CREATE_CHILD_SA)
- **Easy to implement** - already have code for handling SA payloads in CREATE_CHILD_SA, which does all the work
- **If this is used, the problem of using optimized rekey for the initial Child SA rekey will gone**

Optimized Rekey of the Initial Child SA

- **Section 5.1 “Optimized Rekey of the Initial Child SA”**
  - **For the initial Child SA that was negotiated as part of an initial IKE exchange (e.g., IKE_AUTH), at the time of its creation the parameters of PFS and KE method(s) for Child SAs are not negotiated. However, [I-D.pwouters-ipsecme-child-pfs-info] provides a mechanism to negotiate these parameters during the creation of the initial Child SA.**
  - **If both peers support and use [I-D.pwouters-ipsecme-child-pfs-info], the PFS policy and KE method(s) for the initial Child SA is known during its creation. Therefore, in this situation, when rekeying the initial Child SA for the first time, the optimized way SHOULD be used. If [I-D.pwouters-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.**
- **Dependencies**
  - Normatively relies on the solution on the previous page.
  - Will draft-pwouters-ipsecme-child-pfs-info adopt the solution?
  - Will the WG adopt draft-pwouters-ipsecme-child-pfs-info?

Further Considerations

- Any thoughts about rekeying the initial Child SA?
- Implementation and interop test are needed