



IKEV2 OPTIMIZED REKEY SUPPORT

DRAFT-IETF-IKEV2-SA-TS-PAYLOADS-OPT

IPsec, IETF 117
July 2023

Paul Wouters

Remaining Issues: IPCOMP

- Further clarify if IPcomp used, rekey MUST contain an IPCOMP_SUPPORTED payload with CPI and same compression algorithm.
- RFC 7296 states:
 - This Notify message may be included only in a message containing an SA payload negotiating a Child SA
 - but we have no SA payload in an Optimized Rekey.
- Do these issues require an Updates: 7296 addition ?

Remaining Issues: Initial Child SA

- Initial Child SA protected under the IKE SA Key Exchange Method.
- Peers do not know if other end wants to use PFS for Child SA rekeys.
- And for some (unwise) implementations, allow a different Key Exchange type/strength for a rekeying child SA than the initial IKE SA Key Exchange

Remaining Issues: Initial Child SA

- If peers have PFS mismatch, OPTIMIZED_REKEY will fail.
- Should it sent INVALID_KEY ?
- Should it then retry OPTIMIZED_REKEY or go back to “classic” ?
- Solution 1: Require same KE type for IKE and Child SAs when using Optimized Rekeys
- Solution 2: Send Notify in Initial Exchange for child KE type
- Solution 3: Always do 1 “classic” rekey, remember the KE type, then subsequently use optimized rekeys

Remaining Issues: Critical Bit

- Draft states Critical Bit should be set for the new Notify payload – this is wrong
- Solution 1: Just remove it. Nothing else needed.
- Solution 2: Change OPTIMIZED_REKEY from a Notify payload to its own type of payload, then set critical bit on it.

Next steps ?

- Confirm consensus of previous slides answers on the list
- Push out new draft
- Start WGLC next week?

(please don't let this take another 4 months)