Minor IPsec updates

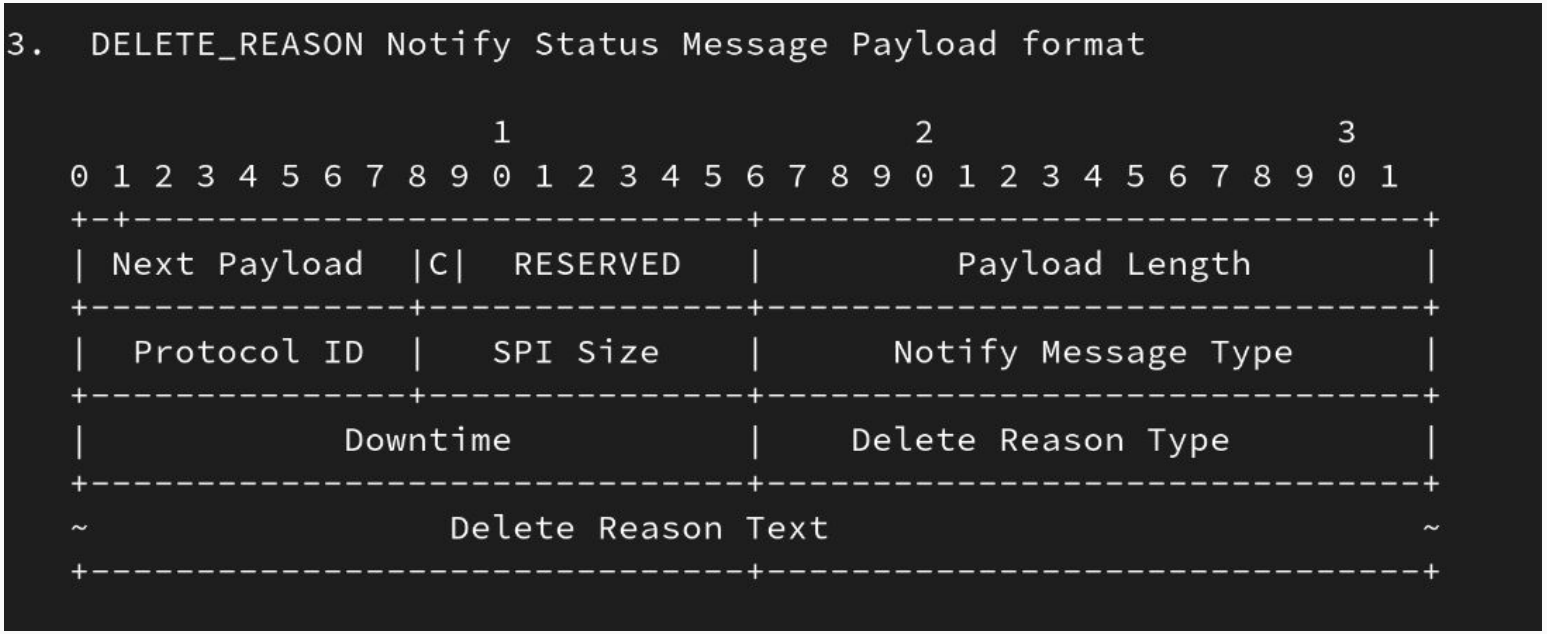
draft-pwouters-ipsecme-delete-info
draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt
draft-pan-ipsecme-anti-replay-notification
draft-pwouters-ipsecme-child-pfs-info

Paul Wouters
IETF 120 Vancouver
23 July 2024

draft-pwouters-ipsecme-delete-info-02

- **Enum list or free text? people wanted both.**
  - enum plus optional text field
  - Example section changed to initial IANA Registry

3. DELETE_REASON Notify Status Message Payload format



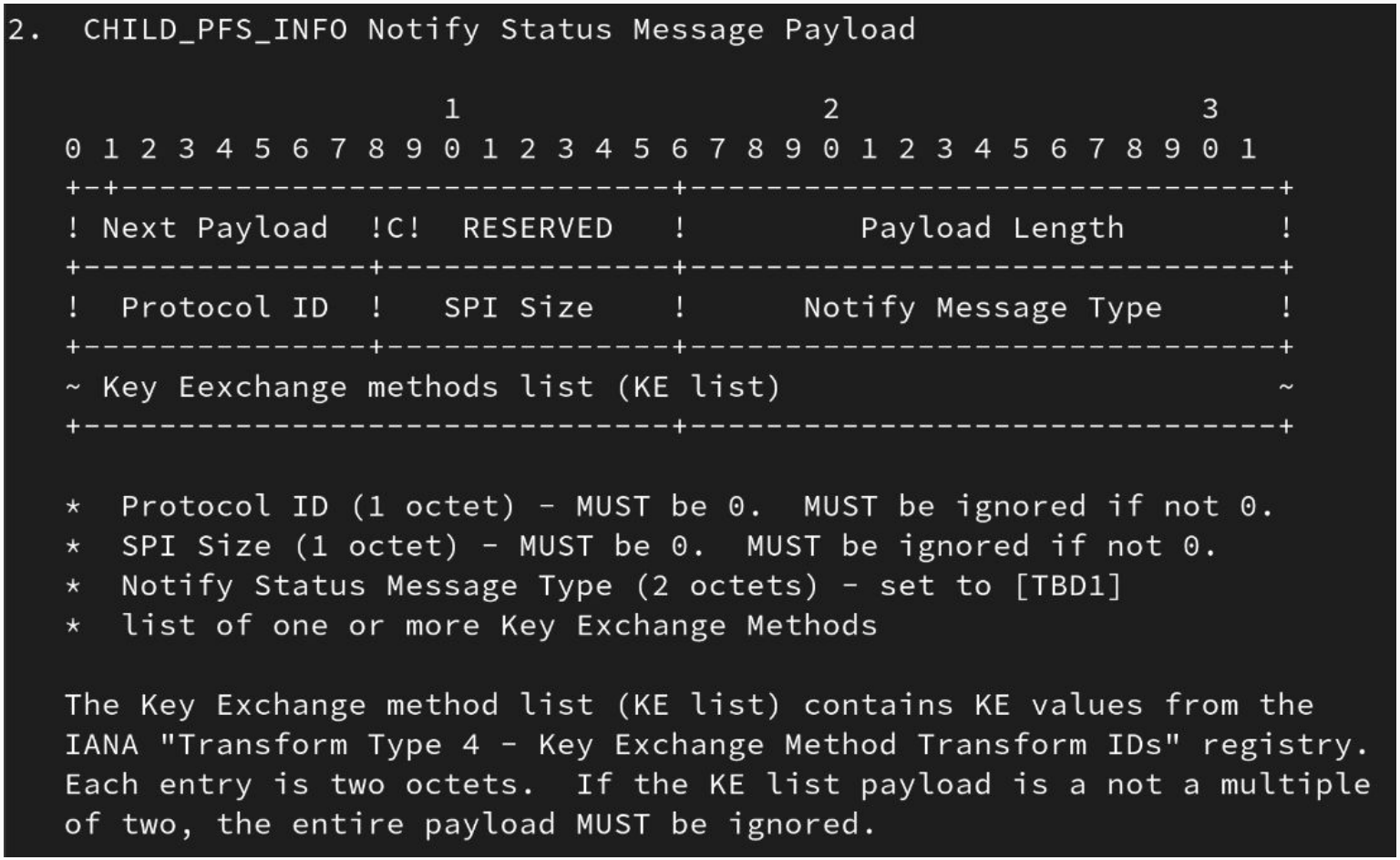
draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt-03

- **Fixed Protocol ID and SPI Size to be 0**
  - As it is a regular NOTIFY payload
- **Renamed SPI to “new SPI” to avoid confusion**
- **Very minor textual fixups**
- **Would like interop tests, then WGLC**
  - Please implement so we can interop test :)

draft-pwouters-ipsecme-child-pfs-info-00

- **Convey PFS/KE for Initial IPsec SA**

2. CHILD_PFS_INFO Notify Status Message Payload



* Protocol ID (1 octet) - MUST be 0. MUST be ignored if not 0.
* SPI Size (1 octet) - MUST be 0. MUST be ignored if not 0.
* Notify Status Message Type (2 octets) - set to [TBD1]
* list of one or more Key Exchange Methods

The Key Exchange method list (KE list) contains KE values from the IANA "Transform Type 4 - Key Exchange Method Transform IDs" registry. Each entry is two octets. If the KE list payload is a not a multiple of two, the entire payload MUST be ignored.

IETF

draft-pwouters-ipsecme-child-pfs-info-00

- **Currently only coves basic case**
- **Cannot convey info on INTERMEDIATE params**
- **Cannot convey info on multiple KE**

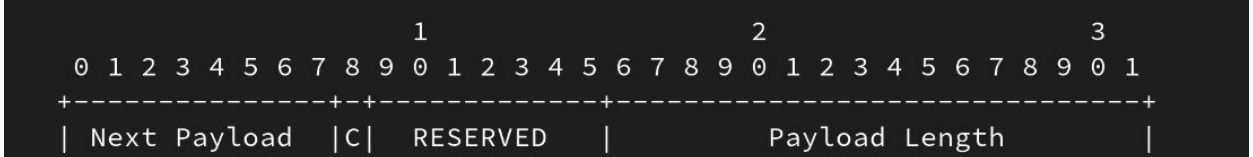
- **Leave for only simply case or make complicated?**

draft-pan-ipsecme-anti-replay-notification-00

- **Missing method to convey “no replay support”**
- **Should we add value for “ESN separate from anti-reply”**

4. ANTI_REPLAY_STATUS Notify Payload Format

The ANTI_REPLAY_STATUS Notify Message type notification is used by the initiator and responder to indicate their own anti-replay status to each other when creating the Child SAs.



* Protocol ID (1 octet) - this field MUST contain either (2) to indicate AH or (3) to indicate ESP.
* SPI Size (1 octet) - MUST be 0.
* Notify Message Type (2 octets) - MUST be set to the value TBD1.
* Status (4 octets) - this field MUST be 0 to indicate the anti-replay is enabled or 1 to indicate the anti-replay is disabled.