# G-IKEv2

draft-yeung-g-ikev2-02.txt

Aldous Yeung, Sheela Rowles, Paulina Tran

*March 29, 2011*

# Agenda

- What is G-IKEv2?
- Why using IKEv2?
- G-IKEv2 Exchanges
  - Registration Exchanges
  - Rekey Exchange
- New Payloads
- MRKMP
- Q & A

# Why using IKEv2?

- Reuse same *framework* for multicast
- Improve in *performance* and *network latency* in registration
- Fix the *cryptographic weakness* in IKEv1
- Industry is *deploying* IKEv2

# Registration Exchanges

- Contains *two* exchanges:
  - GSA_INIT
    1. An *IKEv2 exchange* that negotiates the cryptographic algorithm and exchanges the nonces and Diffie-Hellman values
    2. A *different exchange type* is used so that a device can reject the exchange earlier if it doesn't support G-IKEv2
  - GSA_AUTH
    1. *Authenticates* and *authorizes* the GM to join a particular group
    2. Pushes the *group policies* and *keys* to GM

# Registration Exchanges (con't)

```
  Member (Initiator)                GCKS (Responder)
  ------------------                ----------------

GSA_INIT:
HDR, SAi1, KEi, Ni     -->

                       <--   HDR, SAr1, KEr, Nr, [CERTREQ,]

GSA_AUTH:
HDR, SK { IDi, [CERT,] [CERTREQ,]
[IDr,] AUTH, IDg [, GAP] }    -->

                       <--   HDR, SK { IDr, [CERT,] AUTH,
                             [SEQ,] GSA, KD }
```

# Rekey Exchange (GSA_PUSH)

- A *multicast* rekey which does *NOT* require a *response* from GM

```
   Member (Responder)                GCKS (Initiator)
   ------------------                ----------------

GSA_PUSH:
                                <-- HDR, SK { SEQ, GSA, KD, AUTH }
```

# GSA_PULL Exchange

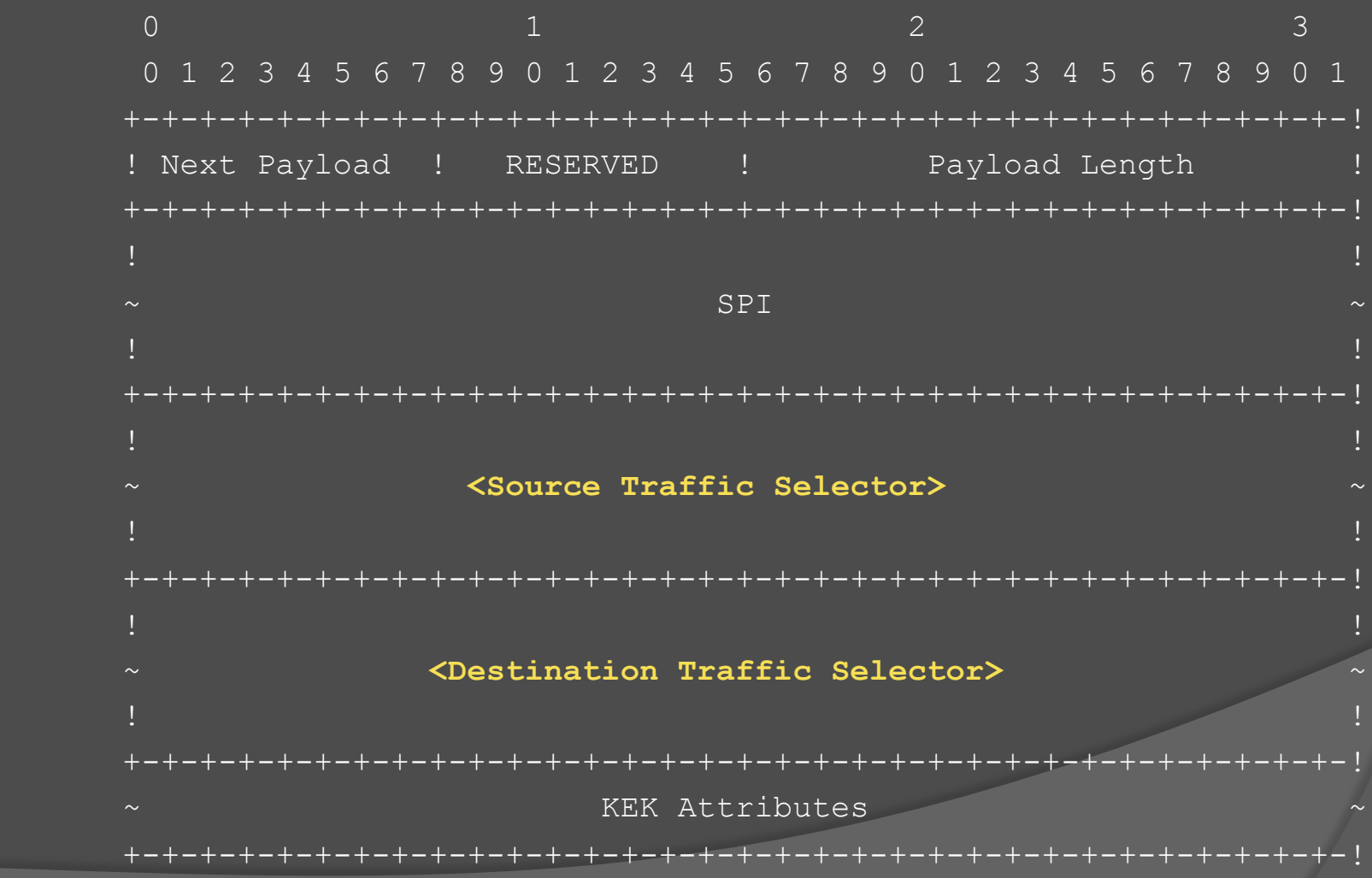
- GM can *reuse* the established secure channel for *another group* registration.

```
   Member (Responder)                GCKS (Initiator)
   ------------------                ----------------

GSA_PULL:
HDR, SK { IDg [, GAP] }     -->

                            <--   HDR, SK { [SEQ,] GSA, KD }
```

# Payloads changed from GDOI

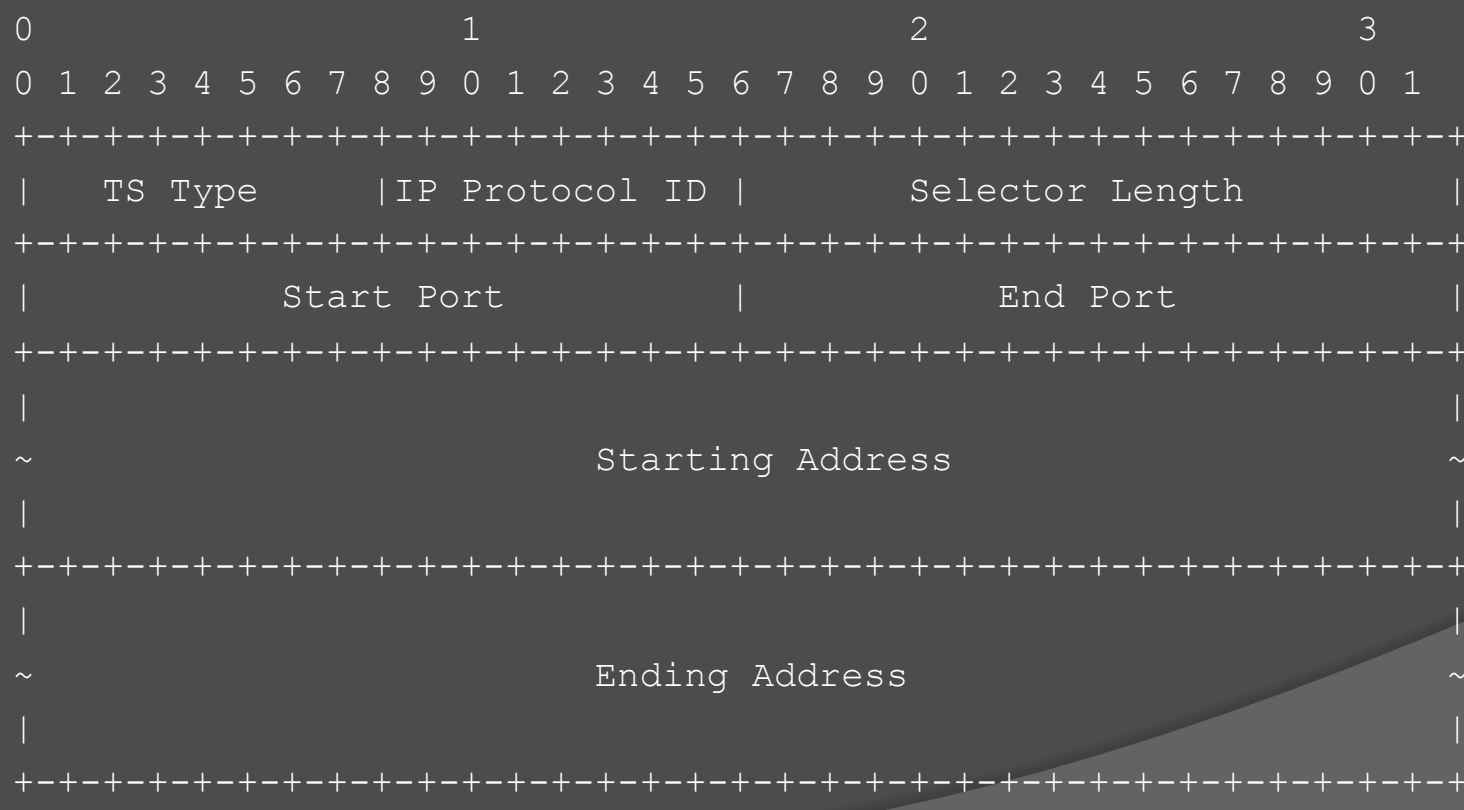
- Leverages the IKEv2 payload format, such as Traffic Selector
- RFC 2407, 2408, 2409 are *obsoleted*
- Payloads that are *changed* from GDOI:
  - Key Encryption Key (KEK)
  - Traffic Encryption Key (TEK)

# KEK Payload

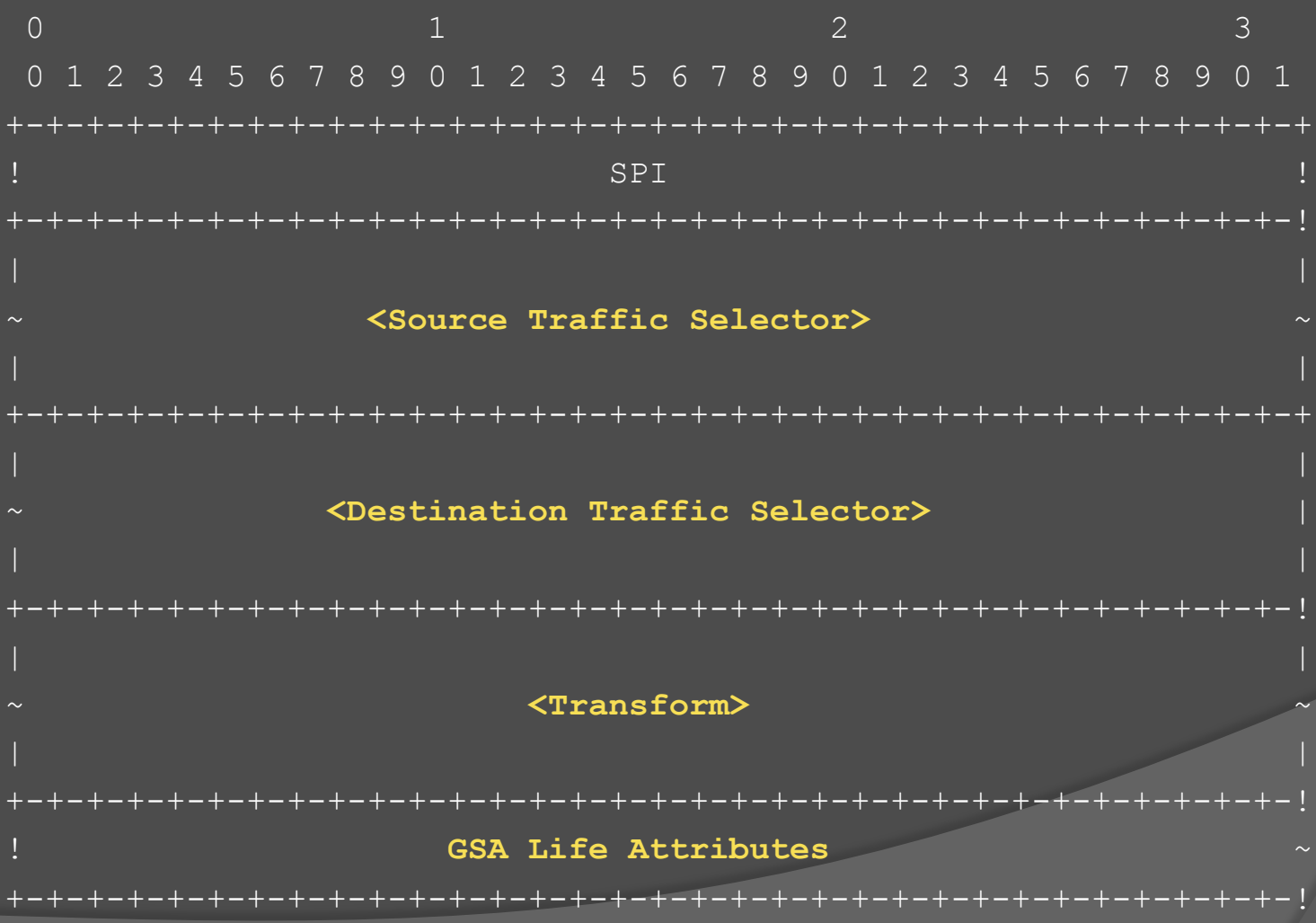

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Payload
RESERVED
Payload Length
SPI
<Source Traffic Selector>
<Destination Traffic Selector>
KEK Attributes

# Src/Dst Traffic Selector

- IKEv2 (RFC 5996), section 3.13.1



# ESP & AH TEK Payload



# GSA Life Attributes

- Redefining SA *Life Type* and *Duration* as they are obsoleted from RFC 2497

| class | value | type |
|---|---|---|
| GSA Life Type | 1 | B |
| GSA Life Duration | 2 | V |

# At-A-Glance

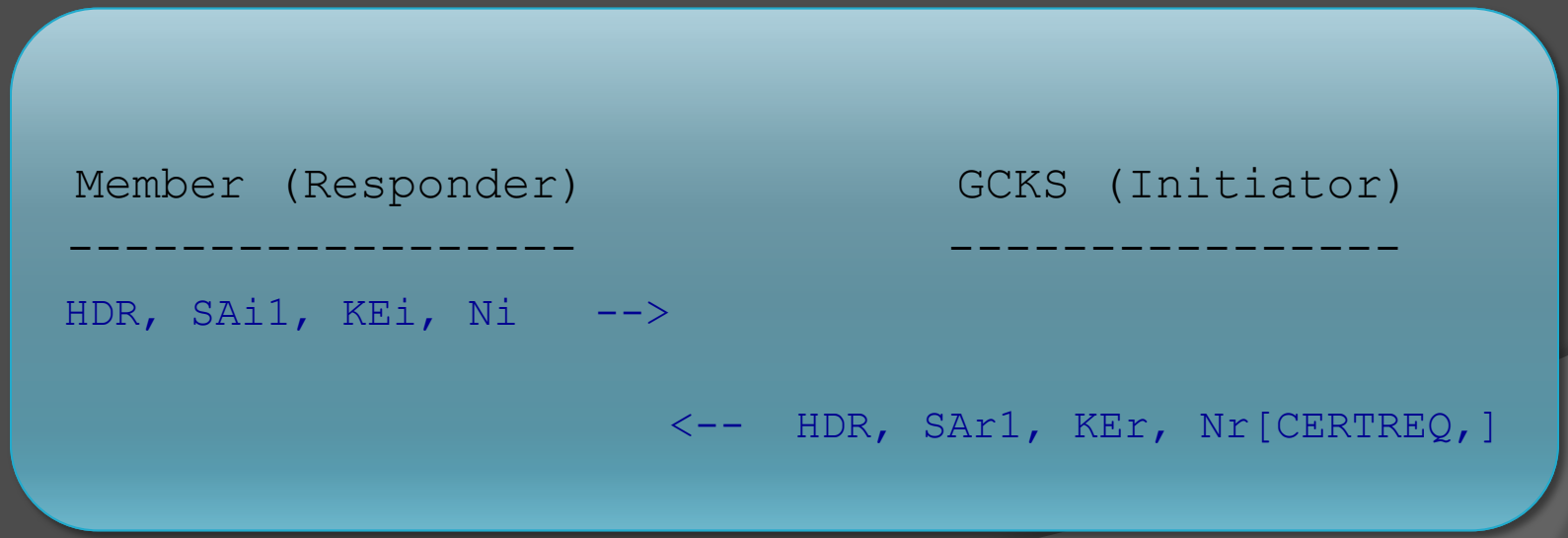
| Next Payload Type | Value |
|---|---|
| Group Identification (IDg) | TBD |
| Group Security Association (GSA) | TBD |
| GSA KEK Payload (GSAK) | TBD |
| GSA GAP Payload (GGAP) | TBD |
| GSA TEK Payload (GSAT) | TBD |
| Key Download (KD) | TBD |
| Sequence Number Payload (SEQ) | TBD |

# Relationship to MRKMP

- MRKMP was presented in the MSEC meeting duringIETF 79
  - draft-hartman-karp-mrkmp-01.txt
- G-IKEv2 defines much of the same protocols and payloads
  - Can reuse most G-IKEv2 exchanges
  - G-IKEv2 would also need a new TEK type (e.g., draft-weis-gdoi-mac-tek-02)
- GCKS selection differs (an election is used in MRKMP)

# MRKMP/G-IKEv2

- MRKMP Initial Exchange – can use GSA_INIT as described in G-IKEv2 draft (section 3.1.1), including the use of pre-shared keys as described in MRKMP.



# MRKMP/G-IKEv2

- MRKMP Group Join Exchange – can use GSA_AUTH as described in G-IKEv2 draft (section 3.1.2)

```
  Member (Responder)                    GCKS (Initiator)
  ------------------                    ----------------
   HDR, SK { IDi, [CERT,] [CERTREQ,]
[IDr,] AUTH, IDg [, GAP] }    -->

                        <--   HDR, SK { IDr, [CERT,] AUTH,
                              [SEQ,] GSA, KD }
```

- MRKMP new requirements:
  - New ID type may need to be added to describe particular application (e.g. OSPF

# MRKMP/G-IKEv2

- MRKMP Rekey – can use GSA_PUSH described in G-IKEv2 draft (section 3.3.1)

```
Member (Responder)                GCKS (Initiator)
------------------                ----------------

                    <-- HDR, SK { SEQ, GSA, KD [,AUTH] }
```

- MRKMP new requirements:
  - Optional AUTH payload - allow KS to send KEK to trusted GMs
  - Periodically send GSA_PUSH of current policy without new info

# MRKMP/G-IKEv2

- MRKMP get update master key – can use GSA_PULL described in G-IKEv2 draft (section 3.1.3)

```
   Member (Responder)                GCKS (Initiator)
   ------------------                ----------------


GSA_PULL:
HDR, SK { IDg [, GAP] }    -->

                          <--   HDR, SK { [SEQ,] GSA, KD }
```

- MRKMP new requirements:
  - New SA TEK payload to request for update master key

# We Need You!

Please review and consider taking this on as a working group item

# Q & A