G-IKEv2

draft-yeung-g-ikev2-02.txt

Aldous Yeung, Sheela Rowles, Paulina Tran

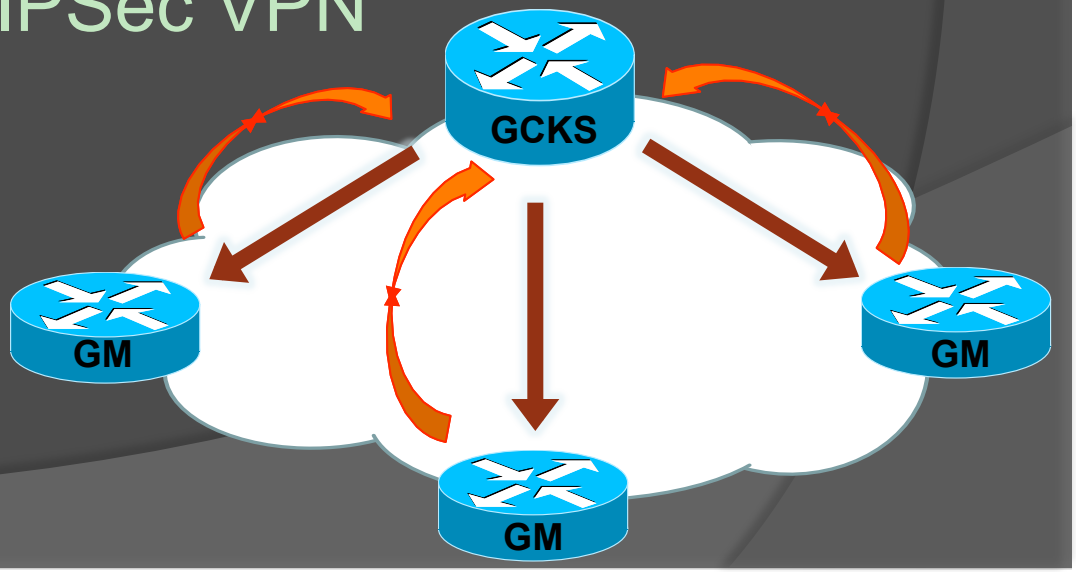
March 23, 2010

Agenda

- What is G-IKEv2?
- Why using IKEv2?
- G-IKEv2 VS GDOI (RFC 3547)
- G-IKEv2 Exchanges
  - Registration Exchanges
  - Rekey Exchange
- New Payloads
- Q & A

What is G-IKEv2?

- Group Key Management using IKEv2 as key exchange and transport protocol
- GCKS – Group Control Key Server, creates and manages the group policies and keys
- GM – Group Member, uses these policies and keys for group IPSec VPN communication



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

G-IKEv2 vs GDOI (RFC 3547)

	G-IKEv2	GDOI
Devices	GCKS GM	GCKS GM
Key management	GCKS	GCKS
Operations	Registration Rekey	Registration (Group-Pull) Rekey (Group-Push)
Transport Protocol	IKEv2	IKEv1
# of Registration Messages	4	9 in Main Mode 6 in Aggressive mode

Registration Exchanges

- Contains *two* exchanges:
  - IKE_SA_INIT

    An *IKEv2 exchange* that negotiates the cryptographic algorithm and exchanges the nonces and Diffie-Hellman values.
  - 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)
  ------------------                ----------------

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

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

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

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

Rekey Exchange (GSA_REKEY)

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

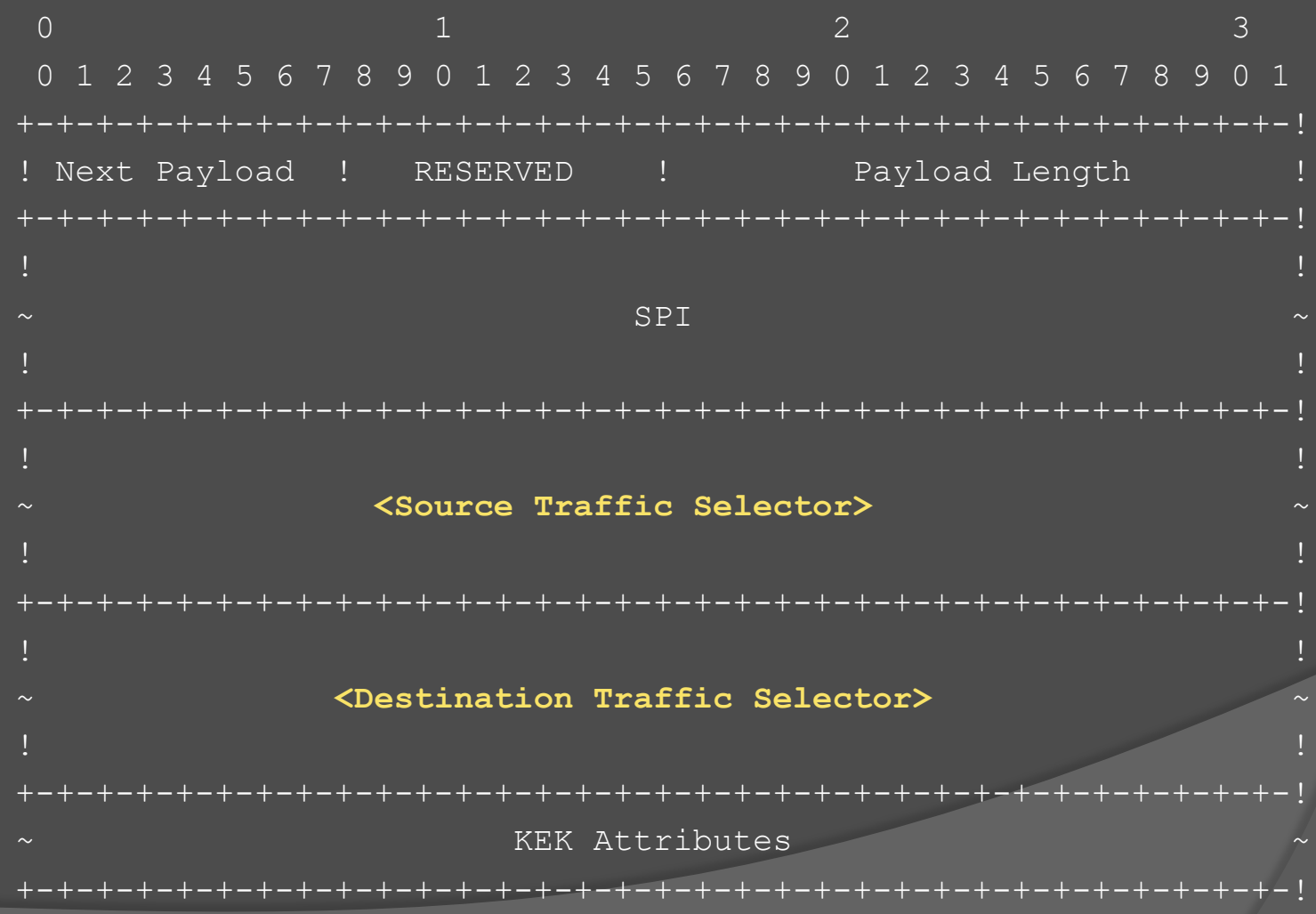
```
   Member (Responder)                GCKS (Initiator)
   ------------------                ----------------

GSA_REKEY:
                                <--   HDR, SK { SEQ, GSA, KD, SIG }
```

Payloads changed from GDOI

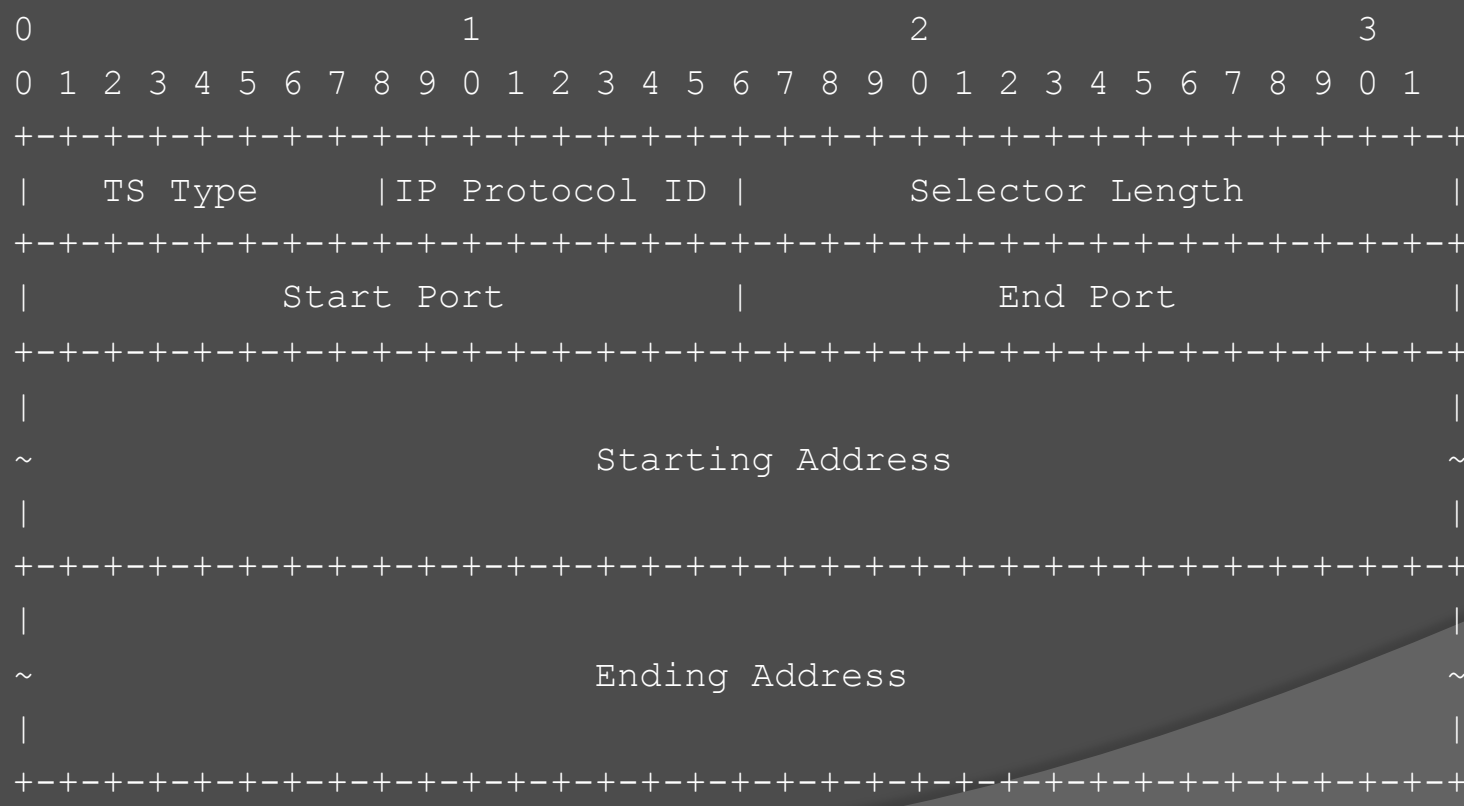
- Leverages the IKEv2 payload format, such as Traffic Selector
- RFC 2407, 2408, 2409 are *obsoleted*
- Payloads that are *changed* from GDOI:
  - Key Encryption Key (KEK)
  - Traffic Encryption Key (TEK)
  - Signature (SIG)

KEK Payload

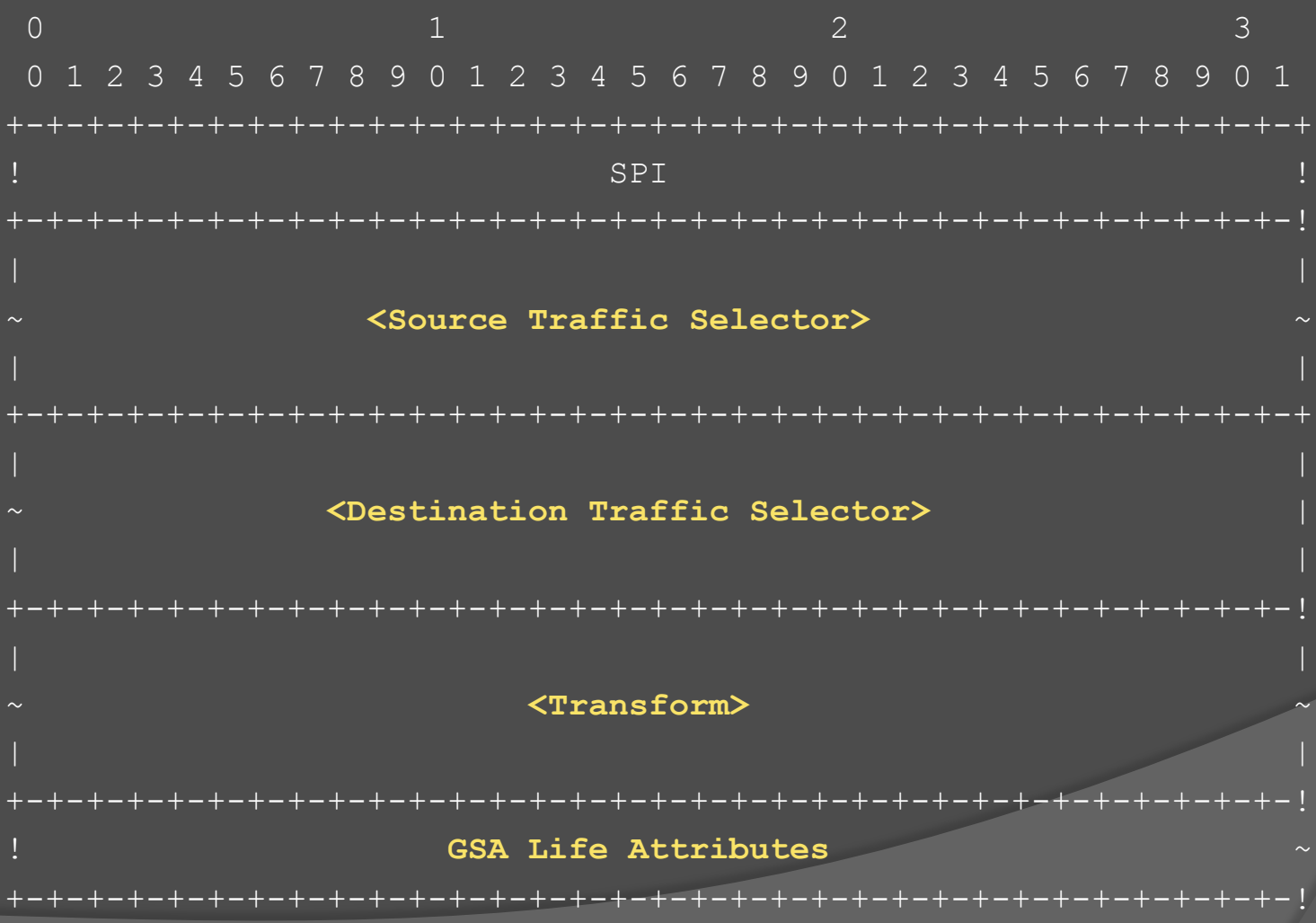

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Payload
RESERVED
Payload Length
SPI
<Source Traffic Selector>
<Destination Traffic Selector>
KEK Attributes

Src/Dst Traffic Selector

- IKEv2 (RFC 4306), section 3.13.1



TEK 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
SPI
<Source Traffic Selector>
<Destination Traffic Selector>
<Transform>
GSA Life Attributes

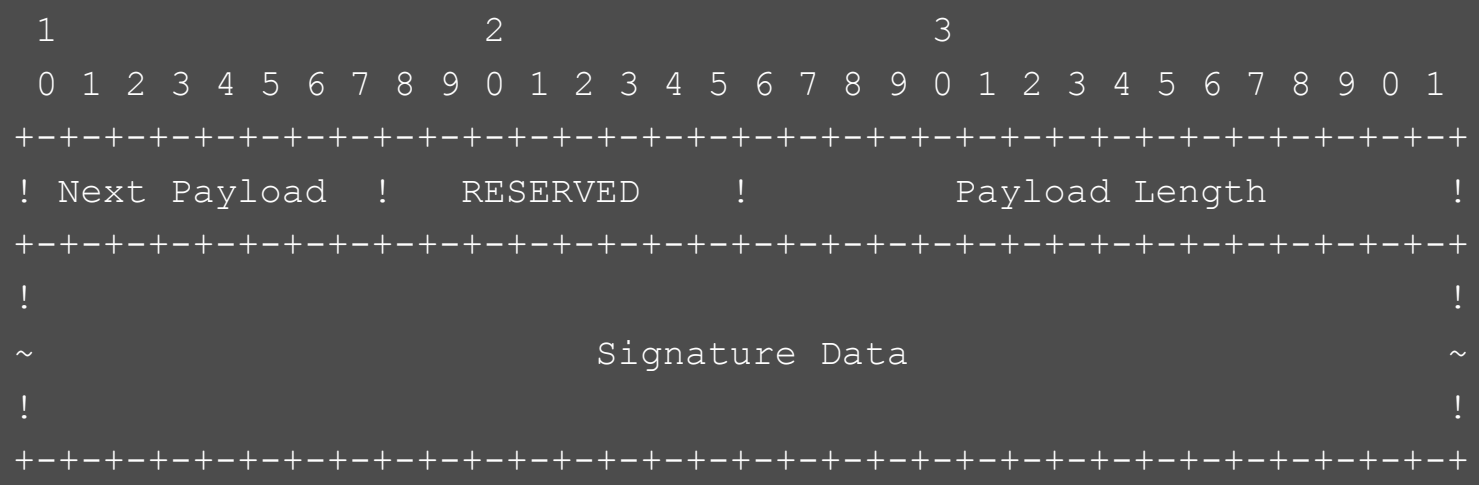
GSA Life Attributes

- 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

SIG Payload

- Redefining since it is obsoleted from RFC 2408



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
Signature Payload (SIG)	TBD

We Need You!

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

Q & A