G-IKEv2 for Multicast Router Key Management

draft-tran-karp-mrmp-00

Paulina Tran, Brian Weis

November 16, 2011

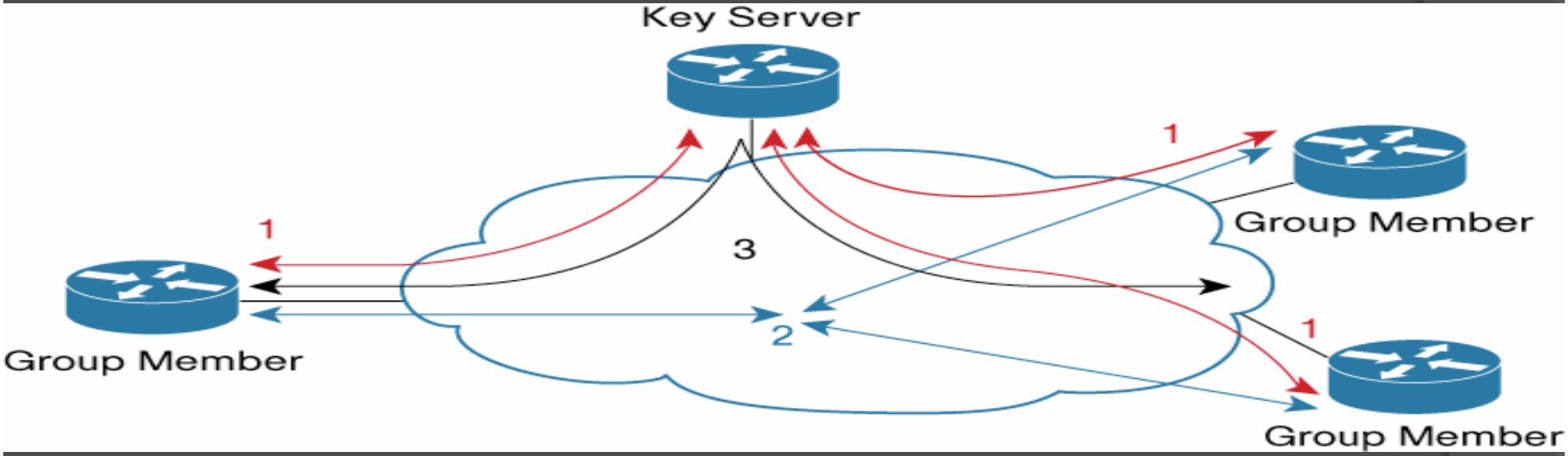
Agenda

- What is Multicast Router Key Management?
- Group key management model
- Group Member (GM) state machine
- Group Controller/Key Server (GCKS) state machine
- New Payloads
- Q & A

What is Multicast Router Key Management?

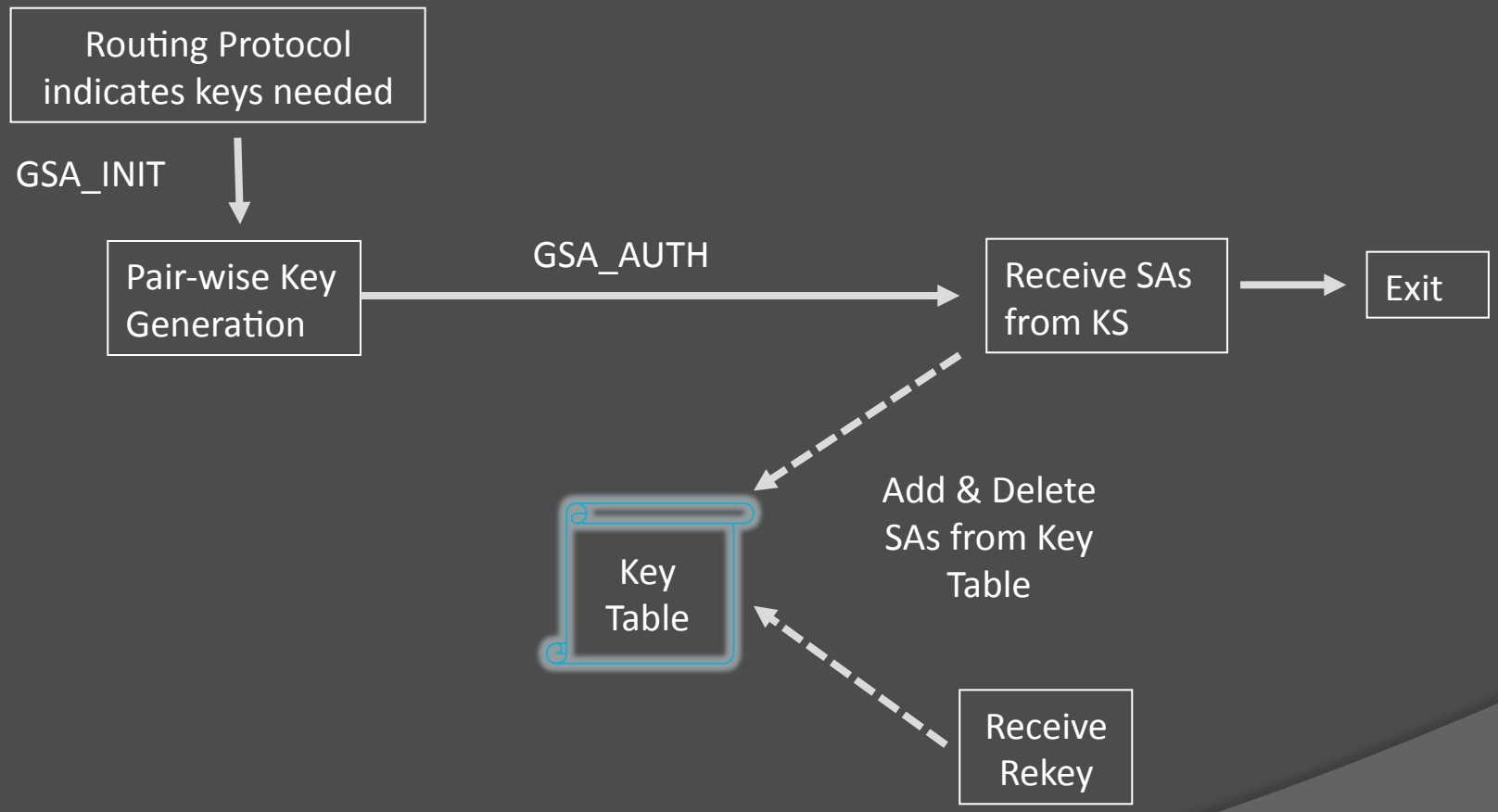
- Key management for routing protocols using multicast addresses (such as OSPFv2, OSPFv3 and PIM)
- Uses G-IKEv2 protocol defined in draft-yeung-g-ikev2-03 (to be progressed as an AD sponsored draft). This protocol re-uses IKEv2 protocol definitions and leverages GDOI [RFC6407]

Group Key Management model

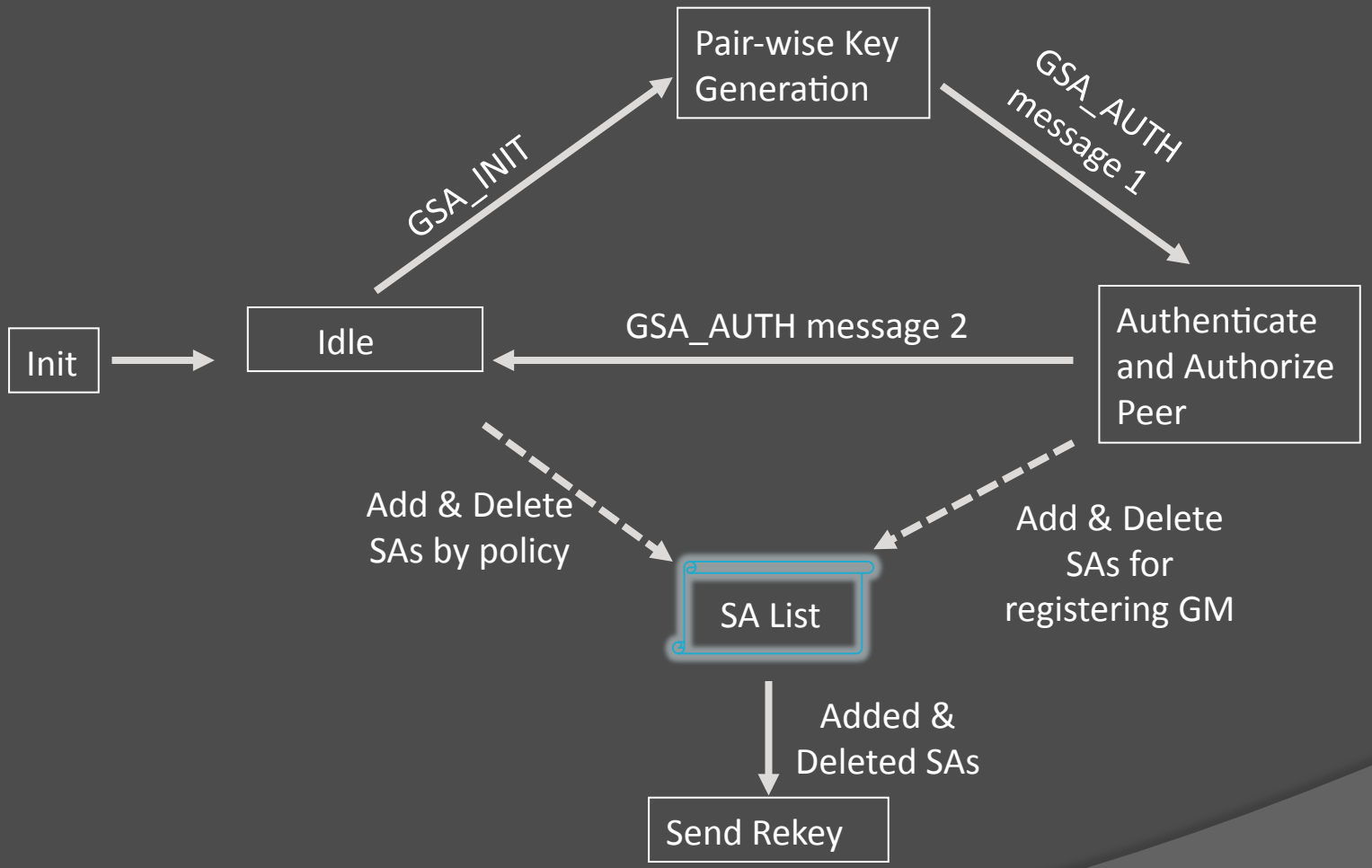


1. Group members register with the GCKS. The GCKS authenticates and authorizes the group members, and downloads the group policy and keys to the group members. (Registration SA)
2. Group members use policy and keys to secure communication between group members (ex. IPSEC SA)
3. The GCKS distributes new group keys to group member as needed using multicast. (REKEY SA)

GM State Machine



GCKS State Machine

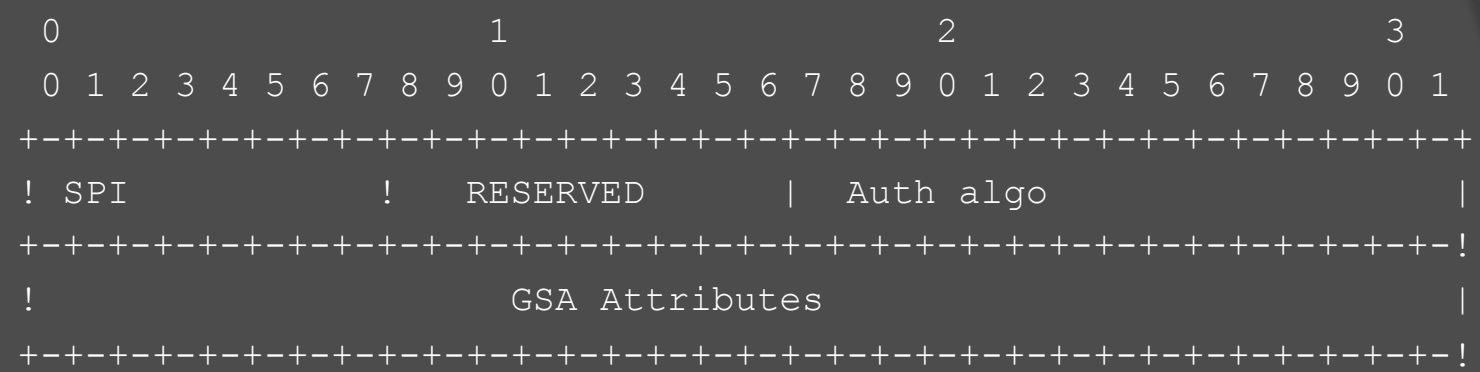


TEK protocol-ID

- Define TEK protocol type

Protocol ID	Value
RESERVED	0
GSA_PROTO_IPSEC_ESP	1
GSA_PROTO_IPSEC_AH	2
GSA_PROTO_OSPFv2	TBD (new)
GSA_PROTO_OSPFv3	TBD (new)
GSA_PROTO_PIM	TBD (new)

TEK OSPFv2 Protocol-Specific Payload

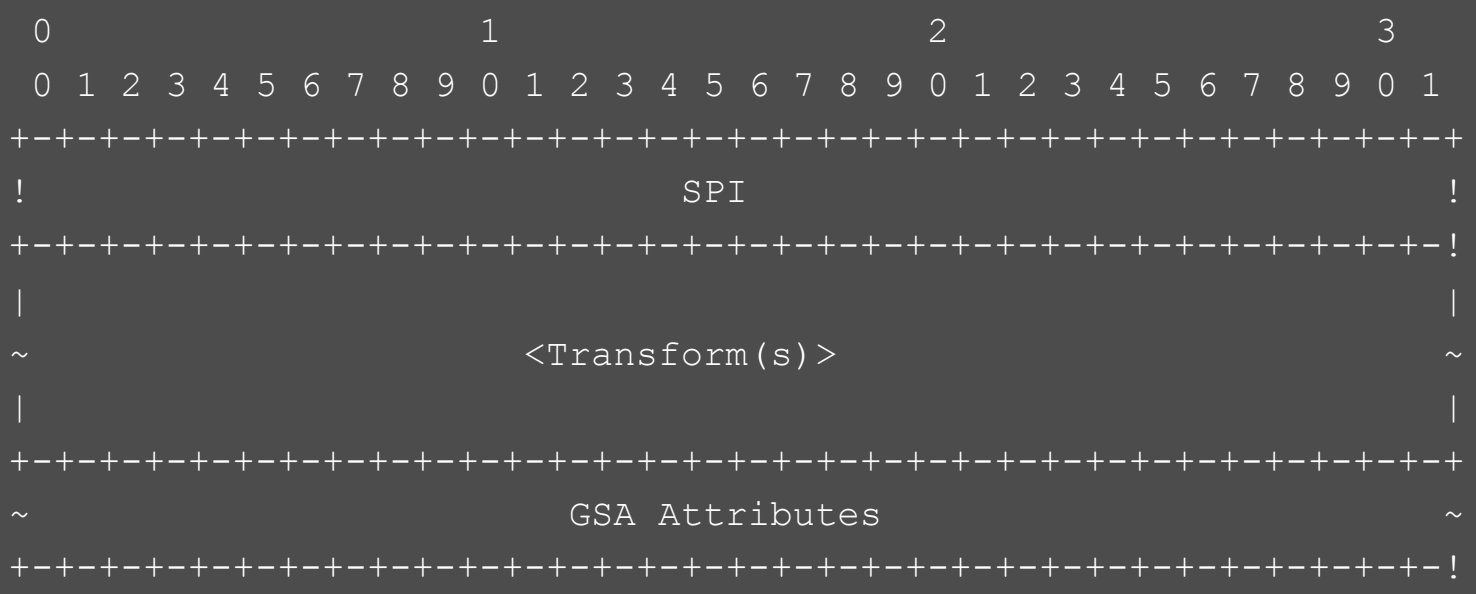


SPI - (1 octet) Secure Parameter Index will be used in OSPFv2 header as Key ID (RFC 2328, Appendix D)

Auth algo - (2 octets) Authentication Algorithm

Keyed-MD5	(defined in RFC 2328, Appendix D)
HMAC-SHA-1	(defined in RFC 5709, Section 3)
HMAC-SHA-256	(defined in RFC 5709, Section 3)
HMAC-SHA-384	(defined in RFC 5709, Section 3)
HMAC-SHA-512	(defined in RFC 5709, Section 3)

TEK OSPFv3 and PIM IPsec Protocol-Specific Payload



Summary

- MRKM can be used to manage keys for OSPFv2, OSPFv3 and PIM
  - No changes required to the existing routing protocol definitions
- MRKM is not a complete solution though
  - GCKS is fixed, not elected
  - Key management & routing protocol interaction not defined

Next Steps

- G-IKEv2 draft to be reviewed and published
- Feedback requested as to whether MRKM meets the routing protocol requirements

Q & A

Group Member to Key server registration

```
  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 }

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