G-IKEv2 - Group Key Management using IKEv2

Valery Smyslov

IPsec Workshop, Madrid, July 2025

IP Multicast Security in IETF

- The Multicast Security (MSEC) WG was active in 2001-2011, which looked at the needs of securing IP multicast traffic
  - RFC 3740: The Multicast Group Security Architecture
  - RFC 4046: MSEC Group Key Management Architecture
  - RFC 5374: Multicast Extensions to the Security Architecture for the Internet Protocol
  - RFC 6407: The Group Domain of Interpretation (based on IKEv1)
- Platforms supporting IP multicast security take advantage of IKEv2 benefits by replacing GDOI with G-IKEv2

G-IKEv2 Document History

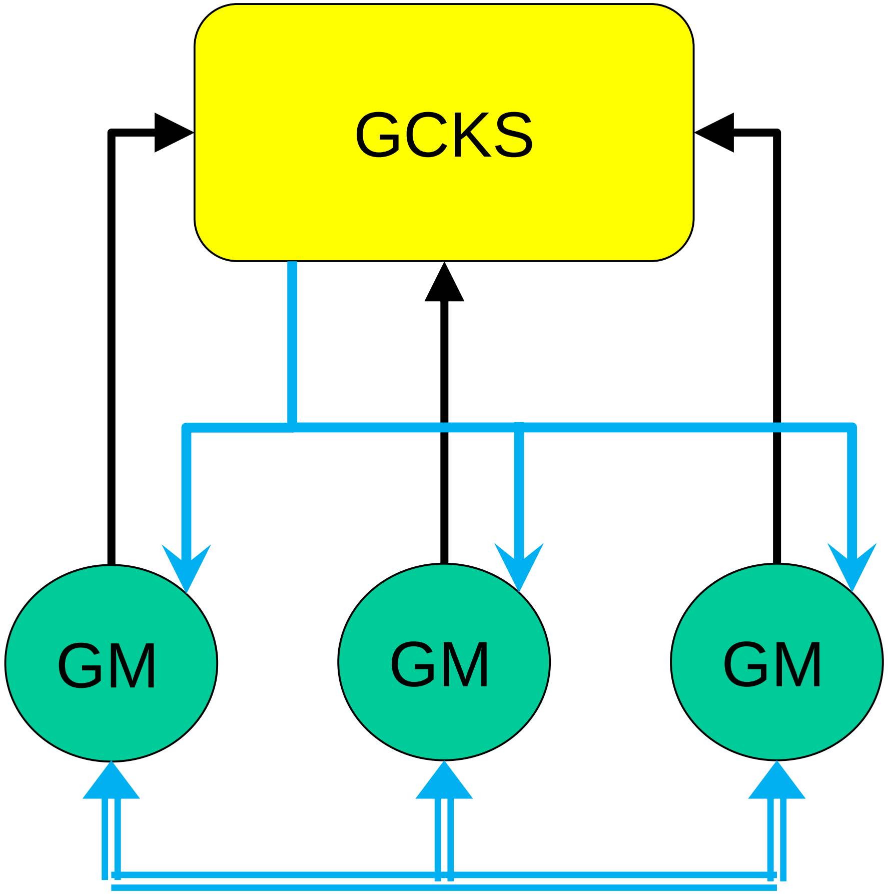
Has been in development for more than15 years:

- First published as individual draft in March 2010
  - few implementations of early draft versions exist
- Adopted by IPSECME WG in 2019
- WGLC from August 2021 to March 2023
- Waited for write-up from March 2023 to November 2024
- Publication requested in November 2024
- In RFC Editor queue since February 2025
- Expected to be published as RFC soon

Securing IP Multicast

- IP multicast applications
  - Contain at least 1 sender, and N receivers
  - Take advantage of the network to route and replicate IP packets, such that the same packet reaches all N receivers
- This requires senders and receivers to share setup an IPsec SA using the same keys
  - The IPsec policy and keys are not individually negotiated, but instead of distributed by a Group Controller / Key Server (GCKS) to Group Members (GMs)
  - A GM invokes a unicast Registration protocol to authenticate to the GCKS. The GCKS then authorizes the GM, and distributes IPsec policy and keys to the GM.
  - A Rekey protocol enforces a time-based key rollover strategy

G-IKEv2 for Large Groups

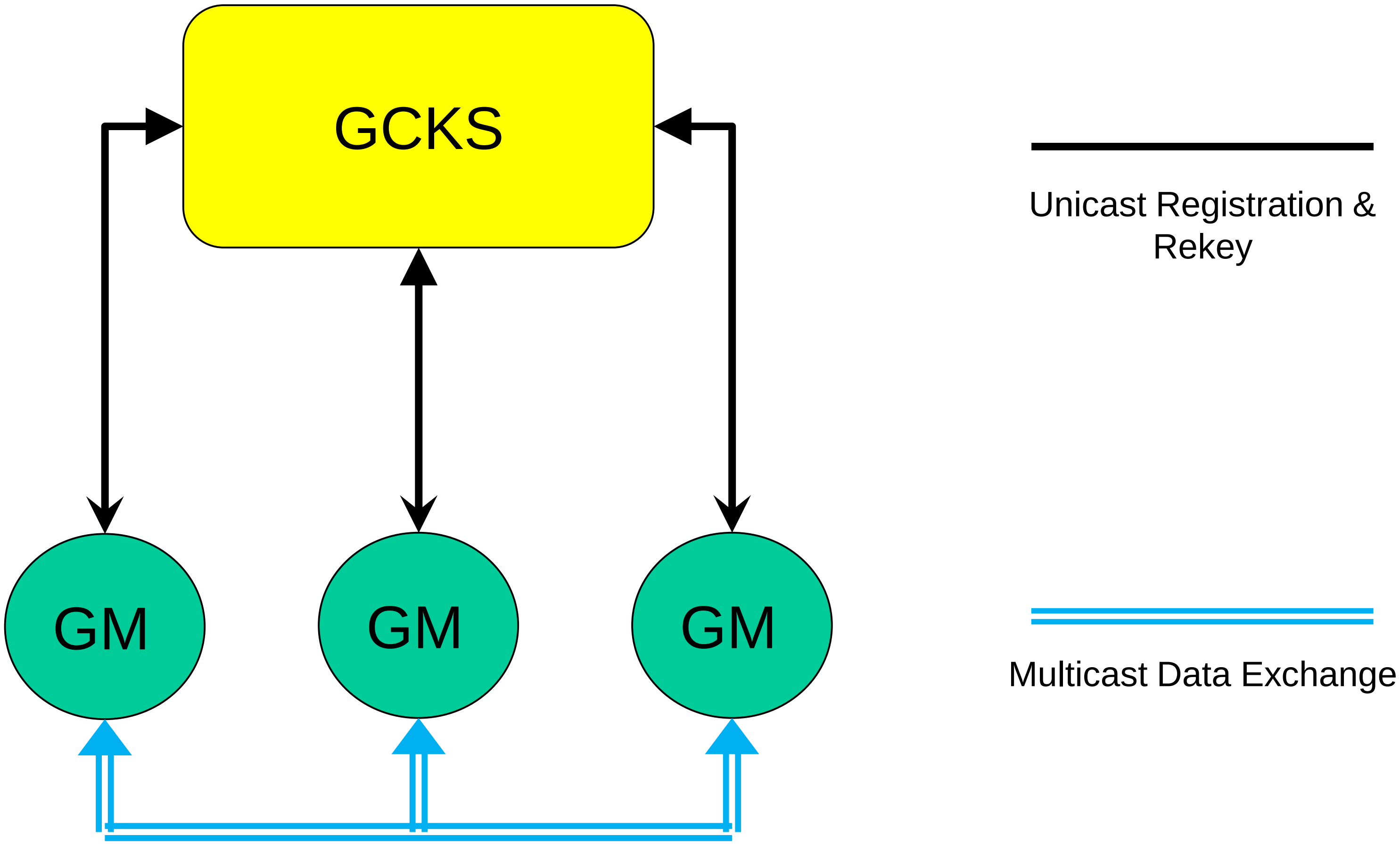


━ Unicast Registration

━ Multicast Rekey

═ Multicast Data Exchange

G-IKEv2 for Small Groups



GCKS

GM

GM

GM

Unicast Registration & Rekey

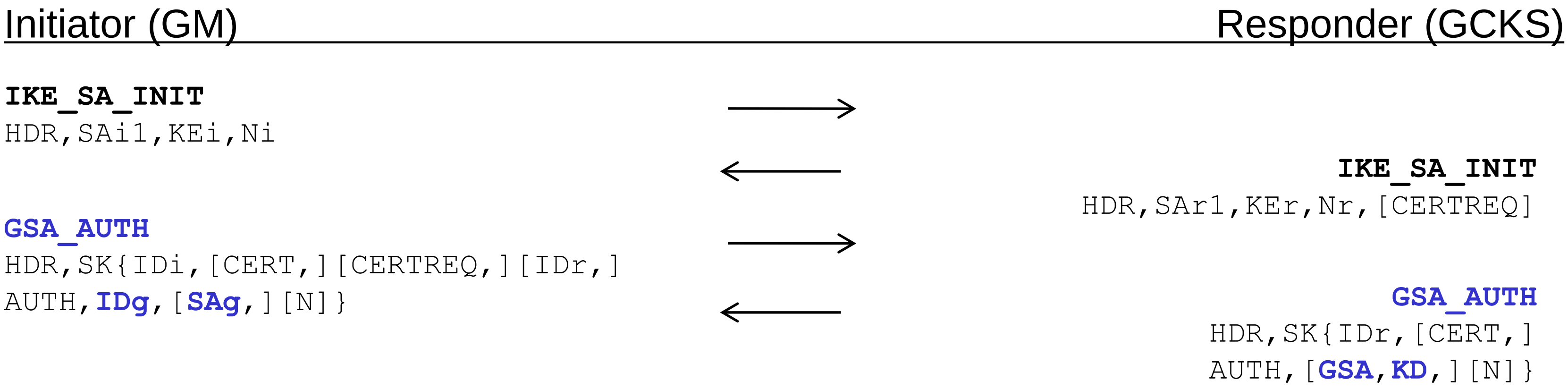
Multicast Data Exchange

Transport & Encapsulation

- G-IKEv2 registration operations
  - for compatibility with GDOI the draft allows using port 848. Standard IKEv2 ports 500/4500 are also allowed, as well as using TCP
- G-IKEv2 rekey operations
  - multicast rekey can only use UDP, port is provided by the GCKS (and can have any value)
- Data-security (ESP) SA
  - run directly over IP
  - UDP encapsulation is not supported (as not needed for unidirectional traffic)
  - transport mode and tunnel mode are supported, although in tunnel mode inner and outer IP address are the same (as per RFC 5374)

G-IKEv2 Registration

- Initial registration (no IKE SA between GM and GCKS)



Initiator (GM) Responder (GCKS)

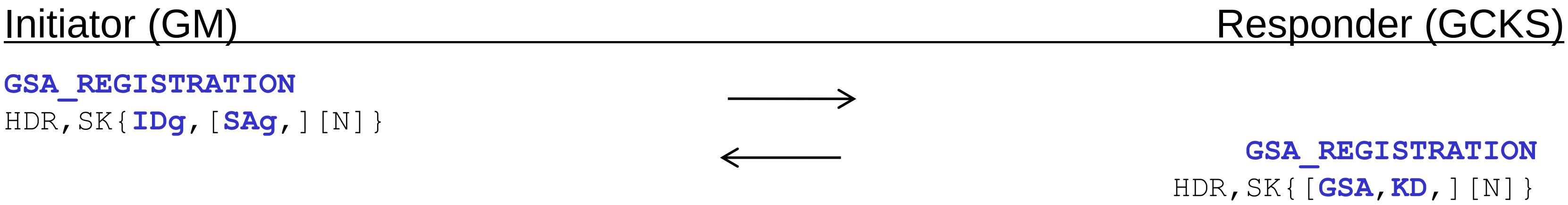
IKE_SA_INIT →
HDR,SAi1,KEi,Ni

← **IKE_SA_INIT**
HDR,SAr1,KEr,Nr,[CERTREQ]

GSA_AUTH →
HDR,SK{IDi,[CERT,][CERTREQ,][IDr,]
AUTH,**IDg**,[**SAg**,][N]}

← **GSA_AUTH**
HDR,SK{IDr,[CERT,]
AUTH,[**GSA**,**KD**,][N]}

- Subsequent registration (IKE SA has already been created)



Initiator (GM) Responder (GCKS)

GSA_REGISTRATION →
HDR,SK{**IDg**,[**SAg**,][N]}

← **GSA_REGISTRATION**
HDR,SK{[**GSA**,**KD**,][N]}

G-IKEv2 Rekey

- Multicast rekey: intended for large groups, protected by policy previously distributed by the GCKS

Responder (GM) Initiator (GCKS)

←

GSA_REKEY
HDR,SK{[**GSA**,**KD**,][N,][AUTH]}

- Unicast rekey: intended for small groups, used registration IKE SAs with each GM

Responder (GM) Initiator (GCKS)

←

GSA_INBAND_REKEY
HDR,SK{[**GSA**,**KD**,][N,]}

GSA_INBAND_REKEY
HDR,SK{}

→

Group SA Payload (GSA)

Contains policy necessary to participating in the group:

- Traffic Protection policies
  - AH/ESP SPI
  - traffic selectors
  - single set of AH/ESP SA related transforms
  - additional parameters
- Multicast Rekey policy
  - Rekey SA SPI
  - traffic selectors
  - single set of Rekey SA related transforms, including new transforms:
    - Key Wrap Algorithm (KWA)
    - Group Controller Authentication Method (GCAUTH)
  - additional parameters
- Group-Wide Policy
  - Group-wide parameters

Group Security Association Policy Substructure

```
                     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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Protocol   |   SPI Size    |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                              SPI                              ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                  Source Traffic Selector                      ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                Destination Traffic Selector                   ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                       <GSA Transforms>                        ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                       <GSA Attributes>                        ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Group-wide Policy Substructure

```
                     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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Protocol    |   RESERVED    |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                     <GW Policy Attributes>                    ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Key Download Payload (KD)

Contains a set of Key Bags

- Group Key Bags
  - AH/ESP/GIKE_UPDATE SPI
  - wrapped group key (KEYMAT)
- Member Key Bag
  - GM-specific attributes
    - Sender-ID
  - wrapped keys or key tree

Group Key Bag Substructure

```
                     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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Protocol   |   SPI Size    |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                              SPI                              ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                   <Group Key Bag Attributes>                  ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Member Key Bag Substructure

```
                     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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Protocol   |   SPI Size    |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                  <Member Key Bag Attributes>                  ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Key Wrapping

Keys are always protected (wrapped) with other keys (Key Wrap Keys, KWKs):

- default KWK: GSK_w
  - for unicast SA: GSK_w = prf+(SK_d, "Key Wrap for G-IKEv2")
  - for multicast rekey SA: GSK_e | GSK_a | GSK_w = KEYMAT
- other KWKs can be part of key tree construction(e.g., Logical Key Hierarchy, LKH) that would allow exclude GMs from the group using multicast rekey operations
- Key Wrapping algorithms are registered by IANA
  - RFC 5649 (AES)
  - ARX-KW (Chacha20)

Wrapped Key

```
                     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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              Key ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              KWK ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                          Encrypted Key                        ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Authentication of Multicast Rekey

- Implicit authentication
  - no additional authentication data in the rekey message (no AUTH payload)
  - relies on the fact, that GM can decrypt rekey message and verify MAC
  - does not really authenticate the GCKS, any GM can impersonate it
- Digital Signature
  - every rekey message is digitally signed by GCKS
  - the signature is in the AUTH payload

IDg Payload

Contains identity of the group a GM wants to join

- has the same format as IKEv2 ID payload
- only some ID types are expected to be used
  - ID_KEY_ID **MUST** be supported
  - ID_IPV4_ADDR, ID_IPV6_ADDR, ID_FQDN, ID_RFC822_ADDR **SHOULD** be supported

Reuse of IKEv2 payloads

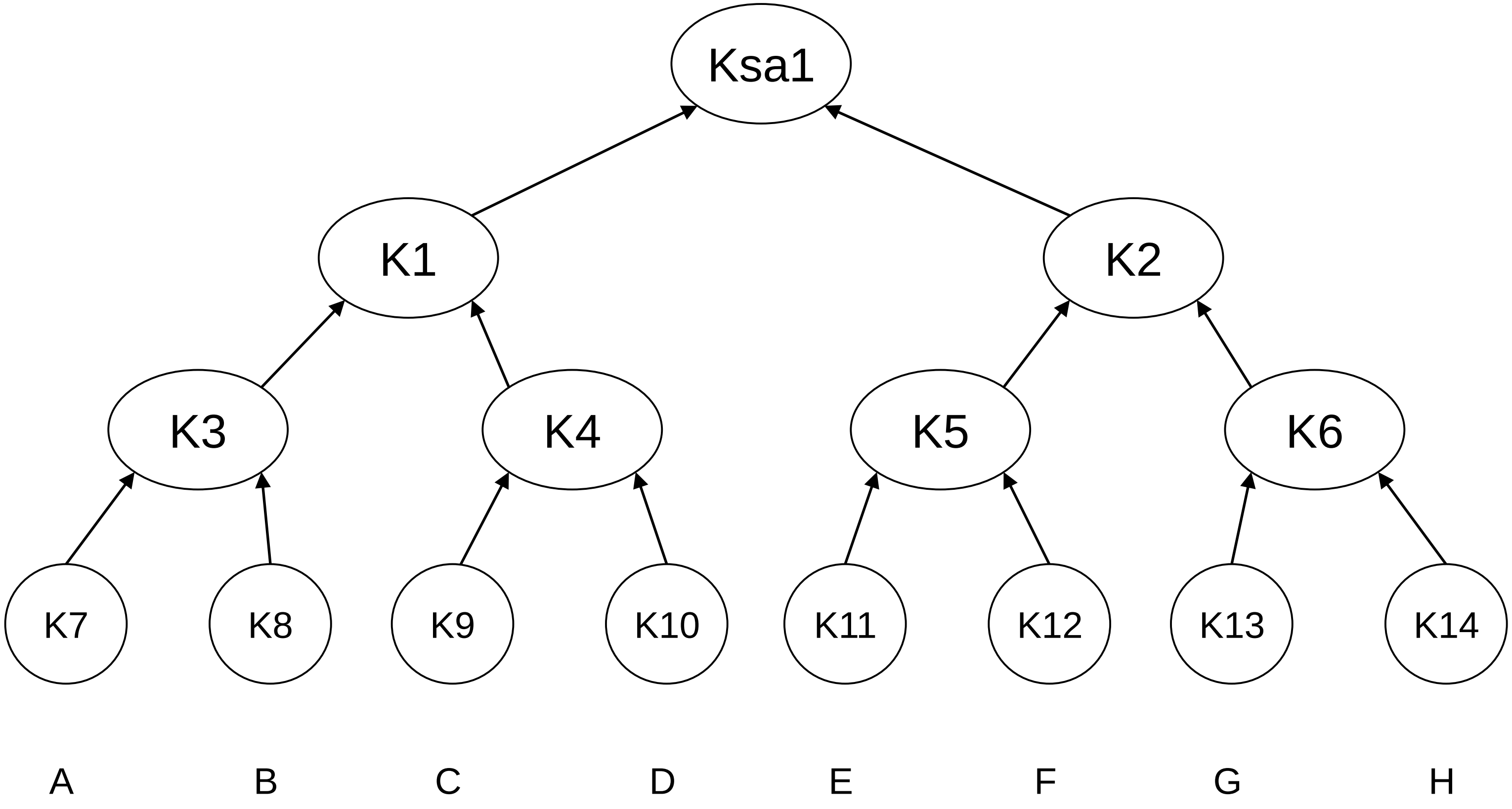
Payloads that have the same types as in IKEv2, but slightly different semantics

- SAg (GM Supported Transforms)
  - has the same format as IKEv2 SA payload
  - declares which Transforms a GM is willing to accept
- D (Delete Payload)
  - used when the GCKS may want to signal to group members to delete policy (e.g., data flows finished, change of policy)

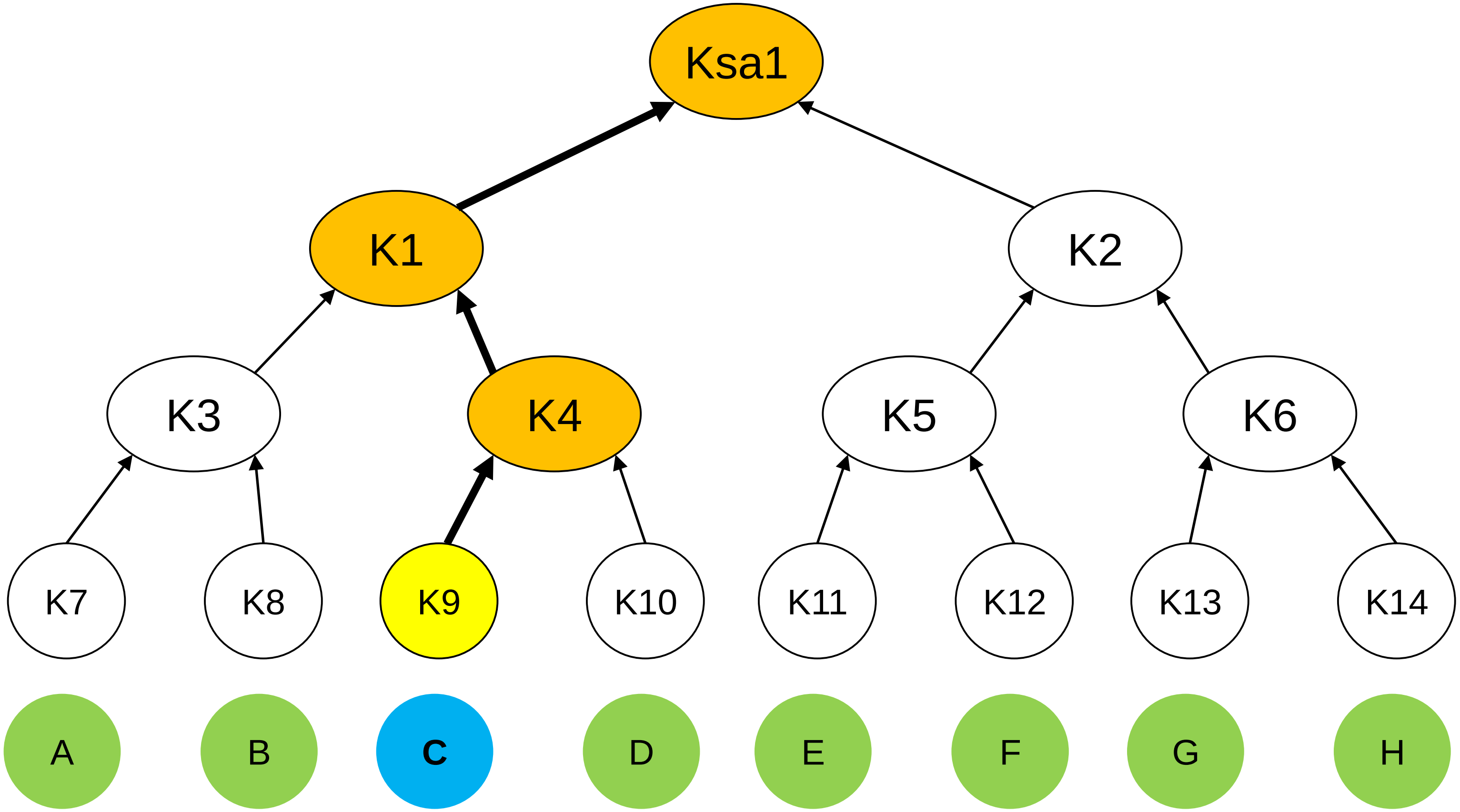
New Notifications

- INVALID_GROUP_ID (error notify)
  - GCKS informs GM that the requested Group ID in a registration protocol is invalid
- AUTHORIZATION_FAILED (error notify)
  - GCKS informs GM that it is not authorized to join the requested Group ID
- REGISTRATION_FAILED (error notify)
  - GCKS informs GM that for some reason not related to this GM it cannot join the group
- GROUP_SENDER (status notify)
  - GM informs the GCKS about its intention to be a sender in the group
  - requests a number of Sender-ID values, that are used as part of a counter-mode transform nonce

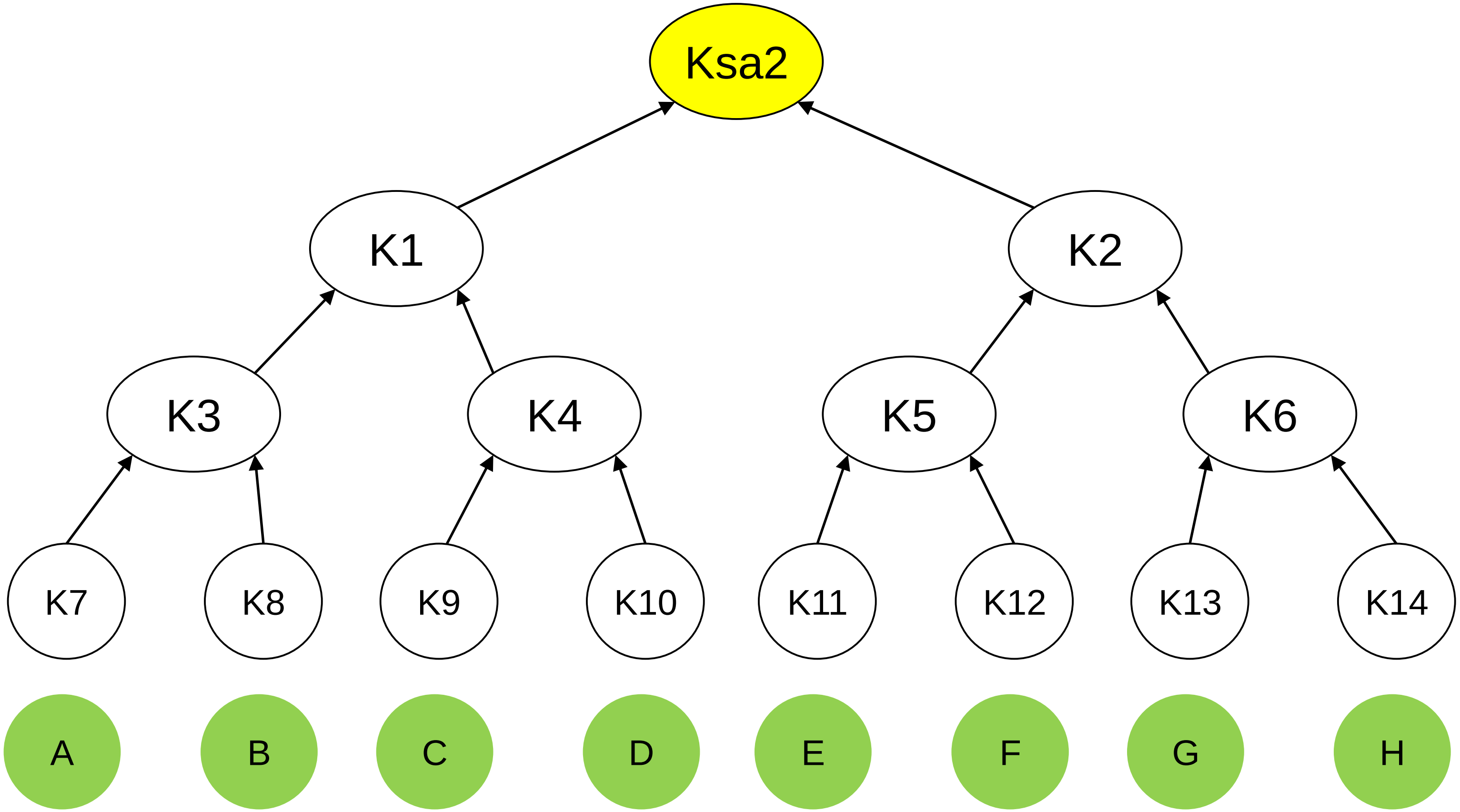
Logical Key Hierarchy (LKH)



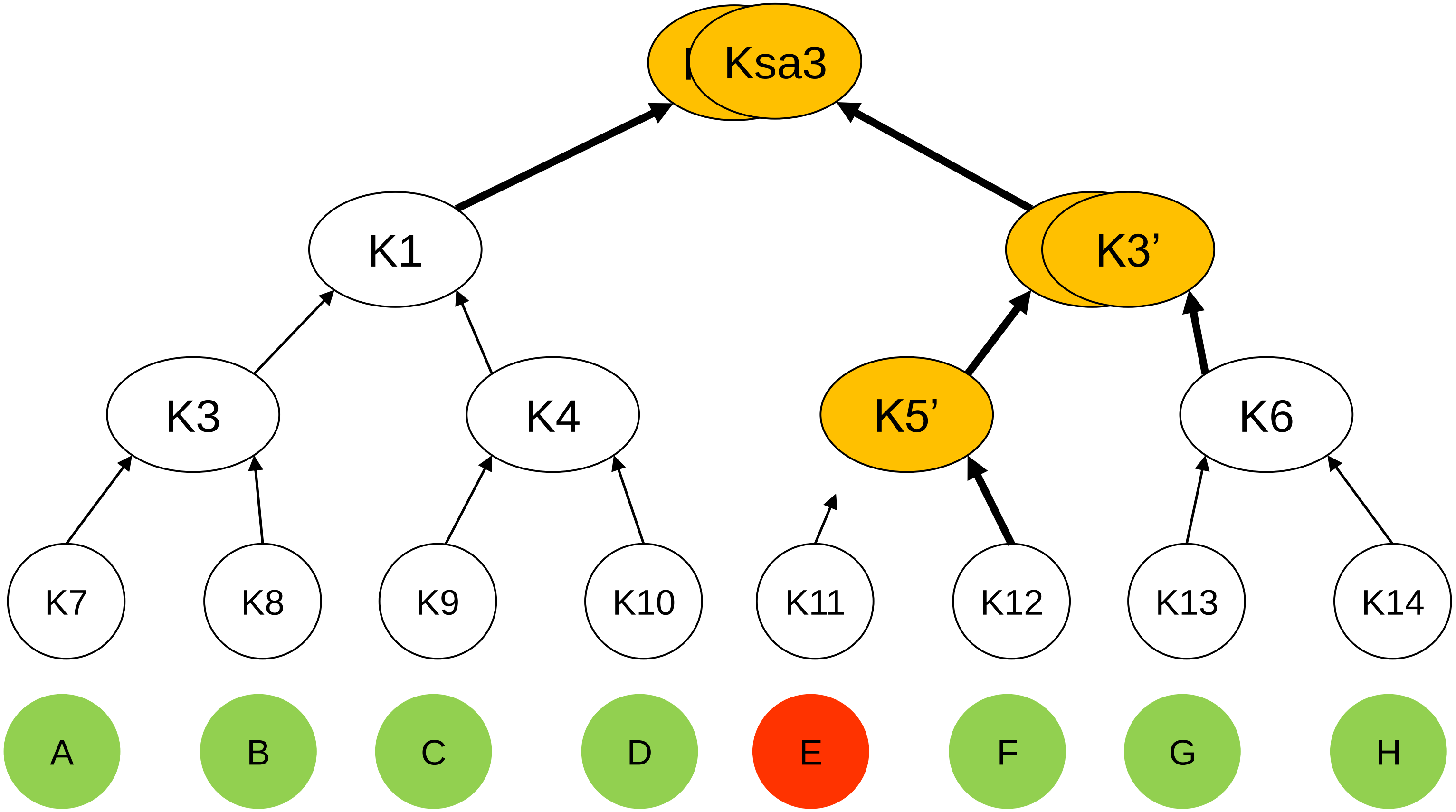
LKH GM Registration



LKH Rekey



LKH GM Removal



Thank you!

Comments?

Questions?