Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 10, 2017

B. Weis
Cisco Systems
Y. Nir
Check Point Software Technologies Ltd.
V. Smyslov
ELVIS-PLUS

March 9, 2017

Group Key Management using IKEv2
draft-yeung-g-ikev2-11

Abstract

This document presents a new group key distribution protocol. The protocol is in conformance with MSEC key management architecture it contains two components: member registration and group rekeying, both downloading group security associations from the Group Controller/Key Server to a member of the group. The new protocol is similar to IKEv2 in message and payload formats as well as message semantics.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 10, 2017.

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction and Overview

This document presents a group key management protocol protected by IKEv2. The data communications within the group are protected by a key pushed to the group members (GMs) by the Group Controller/Key Server (GCKS) using IKEv2 [RFC7296]. The GCKS pushes policy and keys for the group to the GM after authenticating it using new payloads included in a new exchange called GSA_AUTH (similar to the IKE_AUTH exchange). This document references IKEv2 [RFC7296] but it intended to be a separate document. GDOI update document [RFC6407] presented GDOI using IKEv1 syntax. This document uses IKEv2 syntax. The message semantics of IKEv2 are preserved, in that all communications consists of message request-response pairs. The exception to this rule are the rekeying messages, which are sent in multicast without a response. A number of payloads were deemed unnecessary since [RFC6407] are described in Appendix A

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

1.2. Relationship to GDOI

GDOI protocol specified in [RFC6407] is protected by IKEv1 phase1 security association defined in [RFC2407], [RFC2408] and [RFC2409]; these documents are obsoleted and replaced by a new version of the IKE protocol defined in RFC 7296. G-IKEv2 provides group key management between the Group Member and GCKS using the new IKEv2 protocol and inherits the following key advantages over GDOI:

1. Provide a simple mechanism for the responder to keep minimal state and avoid DoS attack from forged IP address using cookie challenge exchange.

2. Improve performance and network latency by the reduced number of initial messages to complete the G-IKEv2 protocol from (10 messages in Main mode and Quick mode, 7 messages in Aggressive mode and Quick) to 4 messages.

3. Fix cryptographic weakness with authentication HASH (IKEv1 authentication HASH specified in RFC 2409 does not include all ISAKMP payloads and does not include ISAKMP header). This issue is documented at [IKE-HASH].

4. Improve protocol reliability where all unicast messages are acknowledged and sequenced.

5. Well defined behavior for error conditions to improve interoperability.

1.3. G-IKEv2 Payloads

1. IDg (group ID) - The GM requests the GCKS for membership into the group by sending its IDg payload.

2. GSA (Group Security Association) - The GCKS sends the group policy to the GM using this payload.

3. KD (Key Download) - The GCKS sends the control and data keys to the GM using the KD payload.

2. G-IKEv2 integration into IKEv2 protocol

The G-IKEv2 protocol provides the security mechanisms of IKEv2 (peer authentication, confidentiality, message integrity) to protect the group negotiations required for G-IKEv2. The G-IKEv2 exchange further provides group authorization, and secure policy and key download from the GCKS to its group members.

It is assumed that readers are familiar with the IKEv2 protocol, so this document skips many details that are described in [RFC7296].

2.1. UDP port

G-IKEv2 SHOULD use port 848, the same as GDOI [RFC6407] , because they serve a similar function, and can use the same ports, just as IKEv1 and IKEv2 can share port 500. The version number in the IKEv2 header distinguishes the G-IKEv2 protocol from GDOI protocol [RFC6407].

3. G-IKEv2 Protocol

3.1. G-IKEv2 member registration and secure channel establishment

The registration protocol consists of minimum two exchanges IKE_SA_INIT and GSA_AUTH; member registration may have a few more messages exchanged if the EAP method, cookie challenge (for DoS protection) or negotiation of Diffie-Hellman group is included. Each exchange consists of request/response pairs. The first exchange IKE_SA_INIT is defined in IKEv2 [RFC7296]. This exchange negotiates cryptographic algorithms, exchanges nonces and does a Diffie-Hellman exchange between the group member (GM) and the Group Controller/Key Server (GCKS).

The second exchange GSA_AUTH authenticates the previous messages, exchange identities and certificates. These messages are encrypted and integrity protected with keys established through the IKE_SA_INIT exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated. The GCKS SHOULD authorize group members to be allowed into the group as part of the GSA_AUTH exchange. Once the GCKS accepted a group member to join a group it will download the data security keys (TEKs) and/or group key encrypting key (KEK) or KEK array as part of GSA_AUTH response message. In the following descriptions, the payloads contained in the message are indicated by names as listed below.

Notation	Payload
AUTH	Authentication
CERT	Certificate
CERTREQ	Certificate Request
GSA	Group Security Association
HDR	IKEv2 Header
IDg	Identification - Group
IDi	Identification - Initiator
IDr	Identification - Responder
KD	Key Download
KE	Key Exchange
Ni, Nr	Nonce
SA	Security Association
SAg	Security Association - GM Supported Transforms

The details of the contents of each payload are described in Section 4. Payloads that may optionally appear will be shown in brackets, such as [CERTREQ], to indicate that optionally a certificate request payload can be included.

3.1.1. GSA_AUTH exchange

After the group member and GCKS uses IKE_SA_INIT exchange to negotiate cryptographic algorithms, exchange nonces, and perform a Diffie-Hellman exchange as defined in IKEv2 [RFC7296], the GSA_AUTH MUST complete before any other exchanges can be done. The security properties of the GSA_AUTH exchange are the same as the properties of the IKE_AUTH exchange. It is used to authenticate the IKE_SA_INIT messages, exchange identities and certificates. G-IKEv2 also uses this exchange for group member registration and authorization. Although IKE_AUTH contains SA2, TSi, and TSr payload the GSA_AUTH does not contain them. They are not needed because policy is not negotiated between group member and GCKS, but instead downloaded from the GCKS to the group member.

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

After an unauthenticated secure channel is established by IKE_SA_INIT exchange, the member initiates a registration request to join a group indicated by the IDg payload. The GM MAY include an SAg payload declaring which Transforms that it is willing to accept, and also MAY include the Notify payload status type SENDER_ID_REQUEST to request SIDs for Counter-based cipher from the GCKS.

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

The GCKS responds with IDr, optional CERT, and AUTH material as if it were an IKE_AUTH. It also informs the member the cryptographic policies of the group in the GSA payload and key material in the KD payload. The GCKS can also include Delete (D) payload instructing the group member to delete existing SAs it might have as the result of a previous group member registration.

In addition to the IKEv2 error handling, GCKS can reject the registration request when IDg is invalid or authorization fail, etc. In these cases, see Section 4.10, the GSA_AUTH response will not include the GSA and KD, but will include a Notify payload indicating errors. If the group member included an SAg payload, and the GCKS chooses to evaluate it, and it detects that group member cannot support the security policy defined for the group, then the GCKS SHOULD return a NO_PROPOSAL_CHOSEN. When the GCKS indicates errors, and the group member cannot resolve the errors, the group member MUST delete the registration IKE SA.

```
    Initiator (Member)                Responder (GCKS)
   --------------------              ------------------
                              <--    HDR, SK { N }
```

When the group member found the policy sent by the GCKS is unacceptable, the member SHOULD notify the GCKS by sending IDg and the Notify type NO_PROPOSAL_CHOSEN as shown below.

```
    Initiator (Member)                 Responder (GCKS)
   --------------------               ------------------
    HDR, SK {IDg [N,]}      -->

                              <--      HDR, SK {}
```

3.1.2. GSA_REGISTRATION Exchange

When a secure channel is already established between GM and GCKS, the GM registration for a group can reuse the established secure channel. In this scenario the GM will use the GSA_REGISTRATION exchange by including the desired group ID (IDg) to request data security keys (TEKs) and/or group key encrypting keys (KEKs) from the GCKS. If the group member includes an SAg payload, and the GCKS chooses to evaluate it, and it detects that group member cannot support the security policy defined for the group, then the GCKS SHOULD return a NO_PROPOSAL_CHOSEN. The GM MAY also include the Notify payload status type SENDER_ID_REQUEST to request SIDs for Counter-based cipher from the GCKS. The GCKS response payloads are created and processed as in the GSA_AUTH reply.

```
    Initiator (Member)                Responder (GCKS)
   --------------------              ------------------
    HDR, SK {IDg, [SAg, ][N ] } -->

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

This exchange can also be used when the group member found the policy sent by the GCKS is unacceptable. The group member SHOULD notify the GCKS by sending IDg and the Notify type NO_PROPOSAL_CHOSEN, as shown below. The GCKS MUST unregister the group member.

```
    Initiator (Member)                 Responder (GCKS)
   --------------------               ------------------
    HDR, SK {IDg [N,]}      -->

                            <--        HDR, SK {}
```

3.1.3. IKEv2 Header Initialization

The Major Version is (2) and Minor Version number is (0) according to IKEv2 [RFC7296], and maintained in this document. The G-IKEv2 IKE_SA_INIT, GSA_AUTH and GSA_REGISTRATION use the IKE SPI according to IKEv2 [RFC7296], section 2.6.

3.1.4. GM Registration Operations

A G-IKEv2 Initiator (GM) requesting registration contacts the GCKS using the IKE_SA_INIT exchange and receives the response from the GCKS. This exchange is unchanged from the IKE_SA_INIT in IKEv2 protocol.

Upon completion of parsing and verifying the IKE_SA_INIT response, the GM sends the GSA_AUTH message with the IKEv2 payloads from IKE_AUTH (without the SAi2, TSi and TSr) along with the Group ID informing the GCKS of the group the initiator wishes to join. The initiator MAY specify how many Sender-ID values it would like to receive in the Notify payload status type SENDER_ID_REQUEST in case the Data Security SA supports a counter mode cipher (see Section 3.2).

An initiator may be limited in the types of Transforms that it is able or willing to use, and may find it useful to inform the GCKS of which Transforms that it is willing to accept. IT OPTIONALLY includes an SAg payload, which can include ESP and/or AH Proposals. Each Proposal contains a list of Transforms that it is willing to support for that protocol. A Proposal of type ESP can include ENCR, INTEG, and ESN Transforms. A Proposal of type AH can include INTEG, and ESN Transforms. The SPI length of each Proposal in an SAg MUST

be zero, and the SPI field is null. Generally, a single Proposal of each type will suffice, because the group member is not negotiating Transform sets, simply alerting the GCKS to restrictions it may have.

Upon receiving the GSA_AUTH response, the initiator then parses the response from the GCKS authenticating the exchange using the IKEv2 method, then processing the GSA, and KD.

The GSA payload contains the security policy and cryptographic protocols used by the group. This policy describes the Rekey SA (KEK), if present, Data-security SAs (TEK), and other group policy (GAP). If the policy in the GSA payload is not acceptable to the GM, it SHOULD notify the GCKS with a NO_PROPOSAL_CHOSEN Notify (see Section 3.1.1 and Section 3.1.2). Finally the KD is parsed providing the keying material for the TEK and/or KEK. The GM interprets the KD key packets, where each key packet includes the keying material for SAs distributed in the GSA payload. Keying material is matched by comparing the SPIs in the key packets to SPIs previously included in the GSA payloads. Once TEK keys and policy are matched, the GM provides them to the data security subsystem, and it is ready to send or receive packets matching the TEK policy.

The GSA KEK policy MUST include KEK attribute KEK_MESSAGE_ID with a Message ID. The Message ID in the KEK_MESSAGE_ID attribute MUST be checked against any previously received Message ID for this group. If it is less than the previously received number, it should be considered stale and ignored. This could happen if two GSA_AUTH exchanges happened in parallel, and the Message ID changed. This KEK_MESSAGE_ID is used by the GM to prevent GSA_REKEY message replay attacks. The first GSA_REKEY message that the GM receives from the GCKS needs to have a Message ID greater or equal to the Message ID received in the KEK_MESSAGE_ID attribute.

3.1.5. GCKS Registration Operations

A G-IKEv2 GCKS passively listens for incoming requests from group members. The GCKS receives the IKE_SA_INIT request, select the IKE proposal, generates nonce and DH to include them in the IKE_SA_INIT response.

Upon receiving the GSA_AUTH request, the GCKS authenticates the group member using the same procedures as in the IKEv2 IKE_AUTH. The GCKS then authorizes the group member according to group policy before preparing to send GSA_AUTH response. If the GCKS fails to authorize the GM, it will respond with the AUTHORIZATION_FAILED notify message.

The GSA_AUTH response will include group policy in GSA payload and keys in the KD payload. If the GCKS policy includes a group rekey

option, this policy is constructed in the GSA KEK and the key is constructed in the KD KEK. The GSA KEK MUST include attribute KEK_MESSAGE_ID specifying the starting Message ID the GCKS will be using when sending the GSA_REKEY message to the group member. This Message ID is used to prevent replay attacks of the GSA_REKEY message and will be increasing each time a GSA_REKEY message is sent to the group. The GCKS data traffic policy is included in the GSA TEK and keys are included in KD TEK. GSA GAP MAY also be included to provide the ATD and/or DTD (Section 4.7.1) specifying activation and deactivation delays for SAs generated from the TEKs. If one or more Data Security SAs distributed in the GSA payload included a counter mode of operation, the GCKS includes at least one SID value in the KD payload, and possibly more depending on the request received in the Notify payload status type SENDER_ID_REQUEST requesting the number of SIDs from the group member.

If the GCKS receives a GSA_REGISTRATION exchange with a request to register a GM to a group, the GCKS will need to authorize the GM with the new group (IDg) and respond with corresponding group policy and keys. If the GCKS fails to authorize the GM, it will respond with the AUTHORIZATION_FAILED notification.

If a group member includes an SAg in its GSA_AUTH or GSA_REGISTRATION request, the GCKS MAY evaluate it according to an implementation specific policy.

- The GCKS could evaluate the list of Transforms and compare it to its current policy for the group. If the group member did not include all of the ESP or AH Transforms in its current policy, then it could return a NO_PROPOSAL_CHOSEN Notify.

- The GCKS could store the list of Transforms, with the goal of migrating the group policy to a different Transform when all of the group members indicate that they can support that Transform.

- The GCKS could store the list of Transforms, and adjust the current group policy based on the capabilities of the devices as long as they fall within the acceptable security policy of the GCKS.

3.2. Counter-based modes of operation

Several new counter-based modes of operation have been specified for ESP (e.g., AES-CTR [RFC3686], AES-GCM [RFC4106], AES-CCM [RFC4309], AES-GMAC [RFC4543]) and AH (e.g., AES-GMAC [RFC4543]). These counter-based modes require that no two senders in the group ever send a packet with the same Initialization Vector (IV) using the same

cipher key and mode. This requirement is met in G-IKEv2 when the following requirements are met:

o The GCKS distributes a unique key for each Data-Security SA.

o The GCKS uses the method described in [RFC6054], which assigns each sender a portion of the IV space by provisioning each sender with one or more unique SID values.

When at least one Data-Security SA included in the group policy includes a counter-mode, the GCKS automatically allocates and distributes one SID to each group member acting in the role of sender on the Data-Security SA. The SID value is used exclusively by the group member to which it was allocated. The group member uses the same SID for each Data-Security SA specifying the use of a counter-based mode of operation. A GCKS MUST distribute unique keys for each Data-Security SA including a counter-based mode of operation in order to maintain a unique key and nonce usage.

During registration, the group member can choose to request one or more SID values. Requesting a value of 1 is not necessary since the GCKS will automatically allocate exactly one to the group member. A group member MUST request as many SIDs matching the number of encryption modules in which it will be installing the TEKs in the outbound direction. Alternatively, a group member MAY request more than one SID and use them serially. This could be useful when it is anticipated that the group member will exhaust their range of Data-Security SA nonces using a single SID too quickly (e.g., before the time-based policy in the TEK expires).

When group policy includes a counter-based mode of operation, a GCKS SHOULD use the following method to allocate SID values, which ensures that each SID will be allocated to just one group member.

1. A GCKS maintains an SID-counter, which records the SIDs that have been allocated. SIDs are allocated sequentially, with the first SID allocated to be zero.

2. Each time an SID is allocated, the current value of the counter is saved and allocated to the group member. The SID-counter is then incremented in preparation for the next allocation.

3. When the GCKS specifies a counter-based mode of operation in the Data Security SA a group member may request a count of SIDs during registration in a Notify payload information type SEND_ID_REQUEST. When the GCKS receives this request, it increments the SID-counter once for each requested SID, and distributes each SID value to the group member.

4. A GCKS allocates new SID values for each GSA_REGISTRATION exchange originated by a sender, regardless of whether a group member had previously contacted the GCKS. In this way, the GCKS does not have a requirement of maintaining a record of which SID values it had previously allocated to each group member. More importantly, since the GCKS cannot reliably detect whether the group member had sent data on the current group Data-Security SAs it does not know what Data-Security counter-mode nonce values that a group member has used. By distributing new SID values, the key server ensures that each time a conforming group member installs a Data- Security SA it will use a unique set of counter-based mode nonces.

5. When the SID-counter maintained by the GCKS reaches its final SID value, no more SID values can be distributed. Before distributing any new SID values, the GCKS MUST delete the Data- Security SAs for the group, followed by creation of new Data- Security SAs, and resetting the SID-counter to its initial value.

6. The GCKS SHOULD send a GSA_REKEY message deleting all Data-Security SAs and the Rekey SA for the group. This will result in the group members initiating a new GSA_REGISTRATION exchange, in which they will receive both new SID values and new Data-Security SAs. The new SID values can safely be used because they are only used with the new Data-Security SAs. Note that deletion of the Rekey SA is necessary to ensure that group members receiving a GSA_REKEY exchange before the re-register do not inadvertently use their old SIDs with the new Data-Security SAs. Using the method above, at no time can two group members use the same IV values with the same Data-Security SA key.

3.3. G-IKEv2 group maintenance channel

The GCKS indicates that it will be delivering group rekey messages when the KEK policy and keys are present in the G-IKEv2 GSA and KD payloads. Though the G-IKEv2 Rekey is optional, it plays a crucial role for large and dynamic groups. The GCKS is responsible for rekeying of the secure group per the group policy. The GCKS uses multicast to transport the rekey message. The G-IKEv2 protocol uses GSA_REKEY exchange type in G-IKEv2 header identifying it as a rekey message. This rekey message is protected by the registration exchanges.

3.3.1. G-IKEv2 GSA_REKEY exchange

The GCKS initiates the G-IKEv2 Rekey securely using IP multicast. Since multicast rekey does not require a response and it sends to multiple GMs, G-IKEv2 rekeying MUST NOT support windowing. The GCKS rekey message replaces the rekey GSA KEK or KEK array, and/or creates

a new Data-Security GSA TEK. The SID Download attribute in the Key Download payload (defined in Section 4.8.4) MUST NOT be part of the Rekey Exchange as this is sender specific information and the Rekey Exchange is group specific. The GCKS initiates the GSA_REKEY exchange as following:

```
    Members (Responder)            GCKS (Initiator)
   --------------------           ------------------
                            <-- HDR, SK { GSA, KD, [D,] AUTH }
```

HDR is defined in Section 4.1. The Message ID in this message will start with the same value the GCKS sent to group member in the KEK attribute KEK_MESSAGE_ID during registration; this Message ID will be increasing each time a new GSA_REKEY message is sent to the group members.

The GSA payload contains the current rekey and data security SAs. The GSA may contain a new data security SA and/or a new rekey SA, which, optionally contains an LKH rekey SA, Section 4.4.

The KD represents the keys for the policy included in the GSA. If the data security SA is being refreshed in this rekey message, the IPsec keys are updated in the KD, and/or if the rekey SA is being refreshed in this rekey message, the rekey Key or the LKH KEK array is updated in the KD payload.

The Delete payload MAY be included to instruct the GM to delete existing SAs.

The AUTH payload is included to authenticate GSA_REKEY message using a method defined in the IKEv2 Authentication Method IANA registry [IKEV2-IANA]. The method SHOULD be a digital signature authentication scheme to ensure that the message was originated from an authorized GCKS. Shared Key Integrity Code SHOULD NOT be used as it doesn’t provide source origin authentication (although a small group may not require source origin authentication). During group member registration, the GCKS sends the authentication key in the GSAK payload KEK_AUTH_KEY attribute, which the group member uses to authenticate the key server. Before the current Authentication Key expires, the GCKS will send a new KEK_AUTH_KEY to the group members in a GSA_REKEY message. The AUTH key that is used in the rekey message may not be the same as the authentication key used in GSA_AUTH. Typically rekey message is sent as multicast and received by all group members, the same AUTH key is distributed to all group members.

After adding the AUTH payload to the rekey message, the current KEK encryption key encrypts all payloads following the HDR.

3.3.2. Forward and Backward Access Control

Through G-IKEv2 rekey, the G-IKEv2 supports algorithms such as LKH that have the property of denying access to a new group key by a member removed from the group (forward access control) and to an old group key by a member added to the group (backward access control). An unrelated notion to PFS, "forward access control" and "backward access control" have been called "perfect forward security" and "perfect backward security" in the literature [RFC2627].

Group management algorithms providing forward and backward access control other than LKH have been proposed in the literature, including OFT [OFT] and Subset Difference [NNL]. These algorithms could be used with G-IKEv2, but are not specified as a part of this document.

Support for group management algorithms is supported via the KEY_MANAGEMENT_ALGORITHM attribute which is sent in the GSA KEK policy. G-IKEv2 specifies one method by which LKH can be used for forward and backward access control. Other methods of using LKH, as well as other group management algorithms such as OFT or Subset Difference may be added to G-IKEv2 as part of a later document.

3.3.3. Forward Access Control Requirements

When group membership is altered using a group management algorithm new GSA TEKs (and their associated keys) are usually also needed. New GSAs and keys ensure that members who were denied access can no longer participate in the group.

If forward access control is a desired property of the group, new GSA TEKs and the associated key packets in the KD payload MUST NOT be included in a G-IKEv2 rekey message which changes group membership. This is required because the GSA TEK policy and the associated key packets in the KD payload are not protected with the new KEK. A second G-IKEv2 rekey message can deliver the new GSA TEKS and their associated keys because it will be protected with the new KEK, and thus will not be visible to the members who were denied access.

If forward access control policy for the group includes keeping group policy changes from members that are denied access to the group, then two sequential G-IKEv2 rekey messages changing the group KEK MUST be sent by the GCKS. The first G-IKEv2 rekey message creates a new KEK for the group. Group members, which are denied access, will not be able to access the new KEK, but will see the group policy since the G-IKEv2 rekey message is protected under the current KEK. A subsequent G-IKEv2 rekey message containing the changed group policy and again changing the KEK allows complete forward access control. A

G-IKEv2 rekey message MUST NOT change the policy without creating a new KEK.

If other methods of using LKH or other group management algorithms are added to G-IKEv2, those methods MAY remove the above restrictions requiring multiple G-IKEv2 rekey messages, providing those methods specify how forward access control policy is maintained within a single G-IKEv2 rekey message.

3.3.4. Deletion of SAs

There are occasions when the GCKS may want to signal to group members to delete policy at the end of a broadcast, or if group policy has changed. Deletion of keys MAY be accomplished by sending the G-IKEv2 Delete Payload [RFC7296], section 3.11 as part of the GSA_REKEY Exchange as shown below.

```
    Members (Responder)            GCKS (Initiator)
   --------------------           ------------------
                          <--   HDR, SK {
                                  [GSA ], [KD ], [D, ] AUTH }
```

The GSA MAY specify the remaining active time of the remaining policy by using the DTD attribute in the GSA GAP. If a GCKS has no further SAs to send to group members, the GSA and KD payloads MUST be omitted from the message. There may be circumstances where the GCKS may want to start over with a clean slate. If the administrator is no longer confident in the integrity of the group, the GCKS can signal deletion of all policy of a particular TEK protocol by sending a TEK with a SPI value equal to zero in the delete payload. For example, if the GCKS wishes to remove all the KEKs and all the TEKs in the group, the GCKS SHOULD send a Delete payload with a SPI of zero and a protocol_id of a TEK protocol_id value defined in Section 4.6, followed by another Delete payload with a SPI of zero and protocol_id of zero, indicating that the KEK SA should be deleted.

3.3.5. GSA_REKEY GCKS Operations

The GCKS may initiate a rekey message if group membership and/or policy has changed, or if the keys are about to expire. The GCKS builds the rekey message with a Message ID value that is one greater than the value included in the previous rekey. If the message is using a new KEK attribute, the Message ID is reset to 1 in this message. The GSA and KD follow with the same characteristics as in the GSA Registration exchange. The AUTH payload is the final payload added to the message. It is created by hashing the string "G-IKEv2" and the message created so far, and then digitally signed. Finally,

the payloads following the HDR are encrypted and authenticated using the current KEK keys.

Because GSA_REKEY messages are not acknowledged and could be discarded by the network, one or more GMs may not receive the message. To mitigate such lost messages, during a rekey event the GCKS SHOULD transmit several GSA_REKEY messages with the new policy. A GCKS MUST NOT re-transmit the same GSA_REKEY message, because time-to-live lifetimes in the message will be incorrect, resulting in GMs with unsynchronized TEK and KEK lifetimes.

3.3.6. GSA_REKEY GM Operations

The group member receives the Rekey Message from the GCKS, decrypts the message using the current KEK, validates the signature using the public key retrieved in a previous G-IKEv2 exchange, verifies the Message ID, and processes the GSA and KD payloads. The group member then downloads the new data security SA and/or new Rekey GSA. The parsing of the payloads is identical to the registration exchange.

Replay protection is achieved when the group member rejects GSA_REKEY message which has a Message ID smaller than the current Message ID that the GM is expecting. The GM expects the Message ID in the first GSA_REKEY message it receives to be equal or greater than the message id it receives in the KEK_MESSAGE_ID attribute. The GM expects the message ID in the subsequence GSA_REKEY message to be greater than the last valid GSA_REKEY message it received.

If the GSA payload includes Data-Security SA including a counter-modes of operation and the receiving group member is a sender for that SA, the group member uses its current SID value with the Data-Security SAs to create counter-mode nonces. If it is a sender and does not hold a current SID value, it MUST NOT install the Data-Security SAs. It MAY initiate a GSA_REGISTRATION exchange to the GCKS in order to obtain an SID value (along with current group policy).

If the GM receives a notification that a Data-Security SA is about to expire (such as a "soft lifetime" expiration described in Section 4.4.2.1 of [RFC4301]), it SHOULD initiate a registration to the GCKS. This registration serves as a request for current SAs, and will result in the download of replacement SAs, assuming the GCKS policy has created them.

4. Header and Payload Formats

Refer to IKEv2 [RFC7296] for existing payloads.

4.1. The G-IKEv2 Header

G-IKEv2 uses the same IKE header format as specified in RFC 7296 section 3.1.

Several new payload formats are required in the group security exchanges.

Next Payload Type	Value
Group Identification (IDg)	50
Group Security Association (GSA)	51
Key Download (KD)	52

New exchange types GSA_AUTH, GSA_REGISTRATION and GSA_REKEY are added to the IKEv2 [RFC7296] protocol.

Exchange Type	Value
GSA_AUTH	39
GSA_REGISTRATION	40
GSA_REKEY	41

Major Version is 2 and Minor Version is 0 as in IKEv2 [RFC7296]. IKE SA Initiator's SPI, IKE SA Responder's SPI, Flags, Message ID, and Length are as specified in [RFC7296].

4.2. Group Identification (IDg) Payload

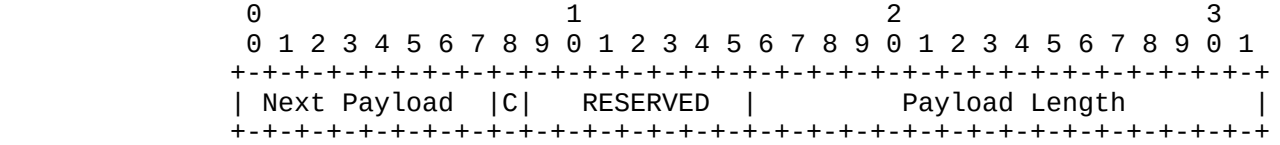
The IDg Payload allows the group member to indicate which group it wants to join. The payload is constructed by using the IKEv2 Identification Payload (section 3.5 of [RFC7296]). ID type ID_KEY_ID MUST be supported. ID types ID_IPV4_ADDR, ID_FQDN, ID_RFC822_ADDR, ID_IPV6_ADDR SHOULD be supported. ID types ID_DER_ASN1_DN and ID_DER_ASN1_GN are not expected to be used.

4.3. Security Association - GM Supported Transforms (SAg)

The SAg payload declares which Transforms that a GM is willing to accept. The payload is constructed by using the IKEv2 Security Association payload (section 3.3 of [RFC7296]).

4.4. Group Security Association Payload

The Group Security Association payload is used by the GCKS to assert security attributes for both Rekey and Data-security SAs.



The Security Association Payload fields are defined as follows:

- Next Payload (1 octet) -- Identifies the next payload type for the G-IKEv2 registration or the G-IKEv2 rekey message.
- Critical (1 bit) -- Set according to [RFC7296].
- RESERVED (7 bits) -- Must be zero.
- Payload Length (2 octets) -- Is the octet length of the current payload including the generic header and all TEK and KEK policies.

4.4.1. GSA Policy

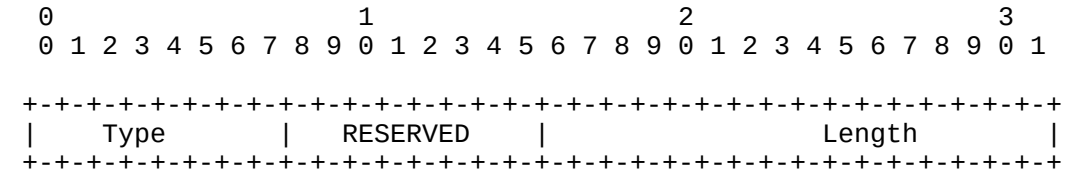
Following GSA generic payload header are GSA policies for group rekeying (KEK) and/or data traffic SAs (TEK) and/or Group Associated Policy (GAP). There may be zero or one GSA KEK policy, zero or more GAP policy, and zero or more GSA TEK policies, where either one GSA KEK or GSA TEK payload MUST be present.

This latitude allows various group policies to be accommodated. For example if the group policy does not require the use of a Rekey SA, the GCKS would not need to send an GSA KEK attribute to the group member since all SA updates would be performed using the Registration SA. Alternatively, group policy might use a Rekey SA but choose to download a KEK to the group member only as part of the Registration SA. Therefore, the GSA KEK policy would not be necessary as part of the GSA_REKEY message.

Specifying multiple GSA TEKs allows multiple related data streams (e.g., video, audio, and text) to be associated with a session, but each protected with an individual security association policy.

A GAP payload allows for the distribution of group-wise policy, such as instructions as to when to activate and de-activate SAs.

Policies following the GSA payload has common header

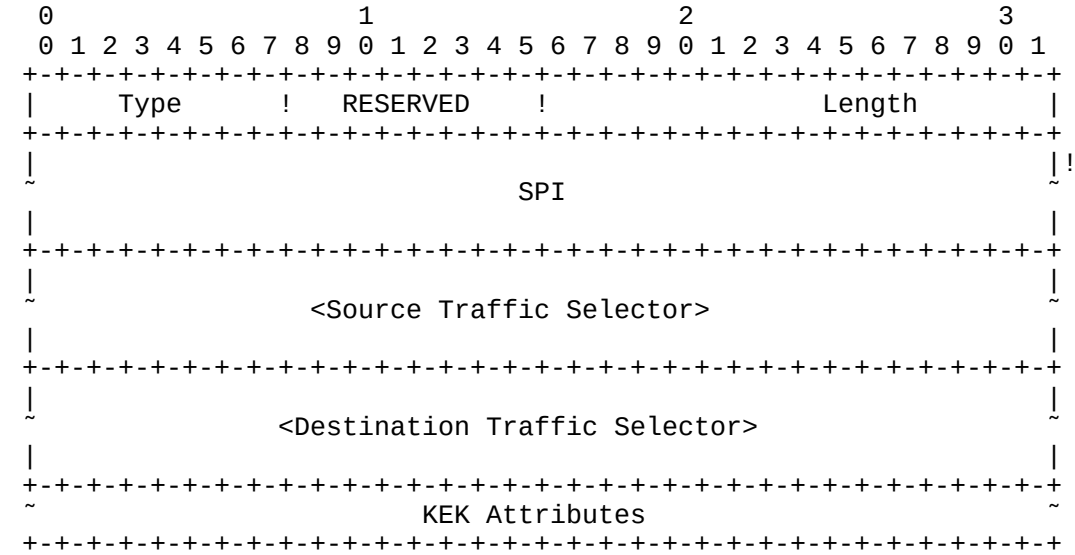


Type is defined as follows:

ID Class	Value
RESERVED	0
KEK	1
GAP	2
TEK	3
Expert Review	4-127
Private Use	128-255

4.5. KEK Policy

The GSA KEK (GSAK) policy contains security attributes for the KEK method for a group and parameters specific to the G-IKEv2 registration operation. The source and destination traffic selectors describe the network identities used for the rekey messages.



The GSAK Payload fields are defined as follows:

- Type (1 octet) -- Identifies the GSA payload type KEK present in the G-IKEv2 registration or the G-IKEv2 rekey message.

- RESERVED (1 octet) -- Must be zero.

- Length (2 octets) -- Length of this structure including KEK attributes.

- SPI (16 octets) -- Security Parameter Index for the rekey message. The SPI must be the IKEv2 Header SPI pair where the first 8 octets become the "Initiator's SPI" field of the G-IKEv2 rekey message IKEv2 HDR, and the second 8 octets become the "Responder's SPI" in the same HDR. As described above, these SPIs are assigned by the GCKS.

- Source & Destination Traffic Selectors - Substructures describing the source and destination of the network identities. These identities refer to the source and destination of the next KEK rekey SA. Defined format and values are specified by IKEv2 [RFC7296], section 3.13.1.

- KEK Attributes -- Contains KEK policy attributes associated with the group. The following sections describe the possible attributes. Any or all attributes may be optional, depending on the group policy.

4.5.1. KEK Attributes

The following attributes may be present in a GSA KEK policy. The attributes must follow the format defined in IKEv2 [RFC7296] section 3.3.5. In the table, attributes that are defined as TV are marked as Basic (B); attributes that are defined as TLV are marked as Variable (V). The terms Reserved, Unassigned, and Private Use are to be applied as defined in [RFC5226]. The registration procedure is Expert Review.

ID Class	Value	Type
Reserved	0	
KEK_MANAGEMENT_ALGORITHM	1	B
KEK_ENCR_ALGORITHM	2	B
KEK_KEY_LENGTH	3	B
KEK_KEY_LIFETIME	4	V
KEK_INTEGRITY_ALGORITHM	5	B
KEK_AUTH_METHOD	6	B
KEK_AUTH_HASH	7	B
KEK_MESSAGE_ID	8	V
Unassigned	9-16383	
Private Use	16384-32767	

The following attributes may only be included in a G-IKEv2 registration message: KEK_MANAGEMENT_ALGORITHM.

Minimum attributes that must be sent as part of an GSA KEK: KEK_ENCR_ALGORITHM, KEK_KEY_LENGTH (if the cipher definition includes a variable length key), KEK_MESSAGE_ID, KEK_KEY_LIFETIME, KEK_INTEGRITY_ALGORITHM, KEK_AUTH_METHOD and KEK_AUTH_HASH (except for DSA based algorithms).

4.5.2. KEK_MANAGEMENT_ALGORITHM

The KEK_MANAGEMENT_ALGORITHM attribute specifies the group KEK management algorithm used to provide forward or backward access control (i.e., used to exclude group members). Defined values are specified in the following table. The terms Reserved, Unassigned, and Private Use are to be applied as defined in [RFC5226]. The registration procedure is Expert Review.

KEK Management Type	Value
Reserved	0
LKH	1
Unassigned	2-16383
Private Use	163848-32767

4.5.3. KEK_ENCR_ALGORITHM

The KEK_ENCR_ALGORITHM attribute specifies the encryption algorithm using with the KEK. This value is a value from the IKEv2 Transform Type 1 - Encryption Algorithm Transform IDs registry[IKEV2-IANA]. If a KEK_MANAGEMENT_ALGORITHM is defined which defines multiple keys (e.g., LKH), and if the management algorithm does not specify the algorithm for those keys, then the algorithm defined by the

KEK_ENCR_ALGORITHM attribute MUST be used for all keys which are included as part of the management.

4.5.4. KEK_KEY_LENGTH

The KEK_KEY_LENGTH attribute specifies the KEK Algorithm key length (in bits).

The Group Controller/Key Server (GCKS) adds the KEK_KEY_LENGTH attribute to the GSA payload when distributing KEK policy to group members. The group member verifies whether or not it has the capability of using a cipher key of that size. If the cipher definition includes a fixed key length, the group member can make its decision solely using KEK_ENCR_ALGORITHM attribute and does not need the KEK_KEY_LENGTH attribute. Sending the KEK_KEY_LENGTH attribute in the GSA payload is OPTIONAL if the KEK cipher has a fixed key length.

4.5.5. KEK_KEY_LIFETIME

The KEK_KEY_LIFETIME attribute specifies the maximum time for which the KEK is valid. The GCKS may refresh the KEK at any time before the end of the valid period. The value is a four (4) octet number defining a valid time period in seconds.

4.5.6. KEK_INTEGRITY_ALGORITHM

The KEK_INTEGRITY attribute specifies the integrity algorithm used to protect the rekey message. This integrity algorithm is a value from the IKEv2 Transform Type 3 - Integrity Algorithm Transform IDs registry [IKEV2-IANA].

4.5.7. KEK_AUTH_METHOD

The KEK_AUTH_METHOD attribute specifies the method of authentication used. This value is from the IKEv2 IKEv2 Authentication Method registry [IKEV2-IANA].

4.5.8. KEK_AUTH_HASH

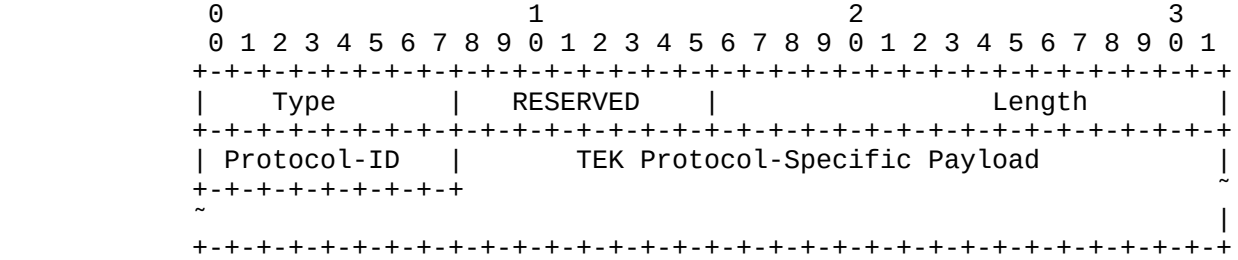
The KEK_AUTH_HASH attribute specifies the hash algorithm uses to generate AUTH key to authenticate GSA_REKEY message. Hash algorithms are defined in IANA registry IKEv2 Hash Algorithms [IKEV2-IANA]. This attribute can be used by group member to determine in advance if it support the algorithm used in the rekey message.

4.5.9. KEK_MESSAGE_ID

The KEK_MESSAGE_ID attribute defines the initial Message ID to be used by the GCKS in the GSA_REKEY messages. The Message ID is 4 octets unsigned integer in network byte order.

4.6. GSA TEK Policy

The GSA TEK (GSAT) policy contains security attributes for a single TEK associated with a group.



The GSAT Payload fields are defined as follows:

- Type (1 octet) -- Identifies the GSA payload type TEK present in the G-IKEv2 registration or the G-IKEv2 rekey message.

- RESERVED (1 octet) -- Must be zero.

- Length (2 octets) -- Length of this structure, including the TEK Protocol-Specific Payload.

- Protocol-ID (1 octet) -- Value specifying the Security Protocol. The following table defines values for the Security Protocol. Support for the GSA_PROTO_IPSEC_AH GSA TEK is OPTIONAL. The terms Reserved, Unassigned, and Private Use are to be applied as defined in [RFC5226]. The registration procedure is Expert Review.

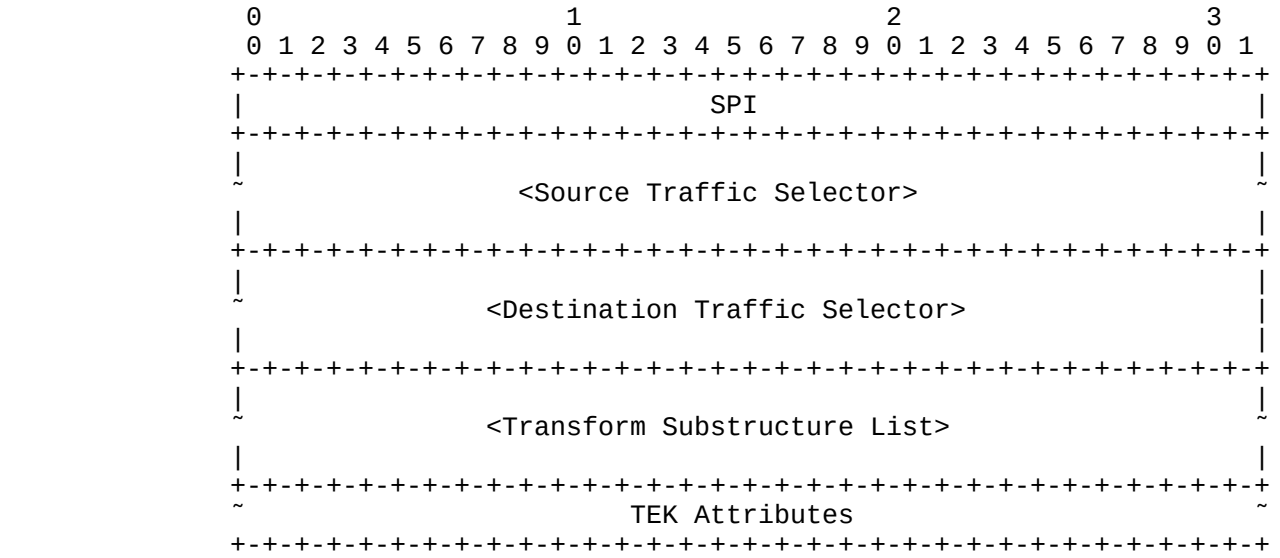
Protocol ID	Value
Reserved	0
GSA_PROTO_IPSEC_ESP	1
GSA_PROTO_IPSEC_AH	2
Unassigned	3-127
Private Use	128-255

- TEK Protocol-Specific Payload (variable) -- Payload which describes the attributes specific for the Protocol-ID.

4.6.1. TEK ESP and AH Protocol-Specific Policy

The TEK Protocol-Specific policy contains of two traffic selectors for source and destination of the protecting traffic, SPI, Transforms, and Attributes.

The TEK Protocol-Specific policy for ESP and AH is as follows:



The GSAT Policy fields are defined as follows:

- SPI (4 octets) -- Security Parameter Index.
- Source & Destination Traffic Selectors - The traffic selectors describe the source and the destination of the protecting traffic. The format and values are defined in IKEv2 [RFC7296], section 3.13.1.
- Transform Substructure List -- A list of Transform Substructures specifies the transform information. The format and values are defined in IKEv2 [RFC7296], section 3.3.2. Valid Transform Types for ESP are ENCR, INTEG, and ESN. Valid Transform Types for AH are INTEG and ESN. As described in the IKEv2 registries [IKEV2-IANA]. The Last Substruc value in each Transform Substructure will be set to 3 except for the last one in the list, which is set to 0.

o TEK Attributes -- Contains TEK policy attributes associated with the group, in the format defined in Section 3.3.5 of [RFC7296]. All attributes are optional, depending on the group policy.

Attribute Types are as follows. The terms Reserved, Unassigned, and Private Use are to be applied as defined in [RFC5226]. The registration procedure is Expert Review.

ID Class	Value	Type
Reserved	0	
TEK_KEY_LIFETIME	1	V
TEK_MODE	2	B
Unassigned	3-16383	
Private Use	16384-32767	

It is NOT RECOMMENDED that the GCKS distribute both ESP and AH Protocol-Specific Policy for the same set of Traffic Selectors.

4.6.1.1. TEK_KEY_LIFETIME

The TEK_KEY_LIFETIME attribute specifies the maximum time for which the TEK is valid. When the TEK expires, the AH or ESP security association and all keys downloaded under the security association are discarded. The GCKS may refresh the KEK at any time before the end of the valid period.

The value is a four (4) octet number defining a valid time period in seconds. If unspecified, the default value shall be assumed to be 28800 seconds (8 hours).

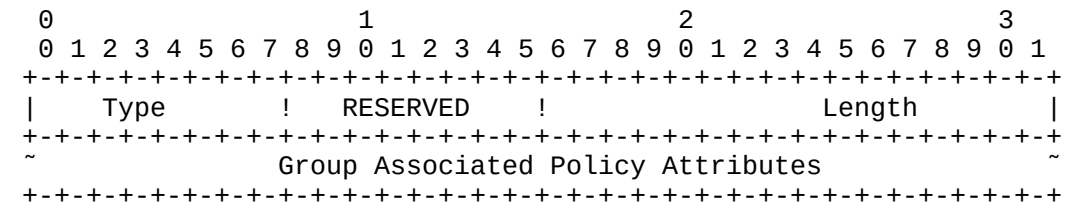
4.6.1.2. TEK_MODE

In the absence of this attribute tunnel mode will be used. Value of 1 is used for transport mode.

4.7. GSA Group Associated Policy

Group specific policy that does not belong to rekey policy (GSA KEK) or traffic encryption policy (GSA TEK) can be distributed to all group member using GSA GAP (Group Associated Policy).

The GSA GAP payload is defined as follows:



The GSA GAP payload fields are defined as follows:

- Type (1 octet) -- Identifies the GSA payload type GAP present in the G-IKEv2 registration or the G-IKEv2 rekey message.

- RESERVED (1 octet) -- Must be zero.

- Length (2 octets) -- Length of this structure, including the GSA GAP header and Attributes.

- Group Associated Policy Attributes (variable) -- Contains attributes following the format defined in Section 3.3.5 of [RFC7296].

Attribute Types are as follows. The terms Reserved, Unassigned, and Private Use are to be applied as defined in [RFC5226]. The registration procedure is Expert Review.

Attribute Type	Value	Type
Reserved	0	
ACTIVATION_TIME_DELAY	1	B
DEACTIVATION_TIME_DELAY	2	B
Unassigned	3-16383	
Private Use	16384-32767	

4.7.1. ACTIVATION_TIME_DELAY/DEACTIVATION_TIME_DELAY

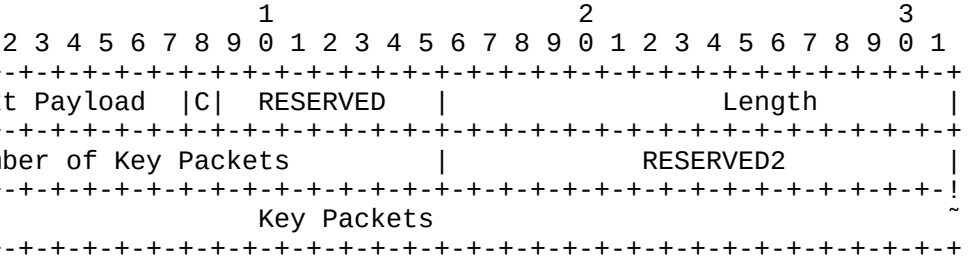
Section 4.2.1 of RFC 5374 specifies a key rollover method that requires two values be provided to group members. The ACTIVATION_TIME_DELAY attribute allows a GCKS to set the Activation Time Delay (ATD) for SAs generated from TEKs. The ATD defines how long after receiving new SAs that they are to be activated by the GM. The ATD value is in seconds.

The DEACTIVATION_TIME_DELAY allows the GCKS to set the Deactivation Time Delay (DTD) for previously distributed SAs. The DTD defines how long after receiving new SAs it should deactivate SAs that are destroyed by the rekey event. The value is in seconds.

The values of ATD and DTD are independent. However, the DTD value should be larger, which allows new SAs to be activated before older SAs are deactivated. Such a policy ensures that protected group traffic will always flow without interruption.

4.8. Key Download Payload

The Key Download Payload contains group keys for the group specified in the GSA Payload. These key download payloads can have several security attributes applied to them based upon the security policy of the group as defined by the associated GSA Payload.



The Key Download Payload fields are defined as follows:

- Next Payload (1 octet) -- Identifier for the payload type of the next payload in the message. If the current payload is the last in the message, then this field will be zero.

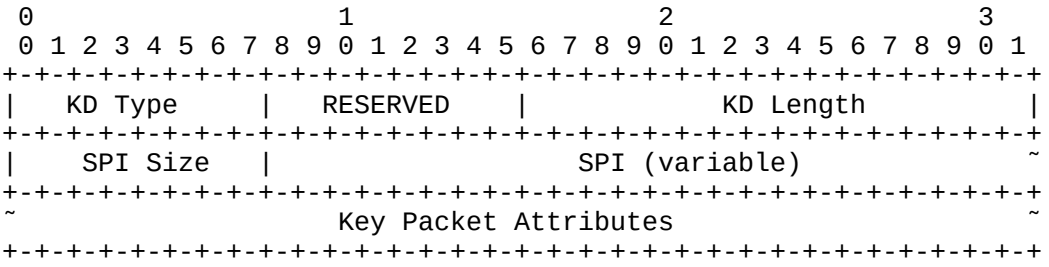
- Critical (1 bit) -- Set according to [RFC7296].

- RESERVED (7 bits) -- Unused, set to zero.

- Payload Length (2 octets) -- Length in octets of the current payload, including the generic payload header.

- Number of Key Packets (2 octets) -- Contains the total number of Key Packets passed in this data block.

- Key Packets (variable) -- Contains Key Packets. Several types of key packets are defined. Each Key Packet has the following format.



- Key Download (KD) Type (1 octet) -- Identifier for the Key Data field of this Key Packet. In the following table the terms Reserved, Unassigned, and Private Use are to be applied as defined in [RFC5226]. The registration procedure is Expert Review.

Key Download Type	Value
Reserved	0
TEK	1
KEK	2
LKH	3
SID	4
Unassigned	5-127
Private Use	128-255

- RESERVED (1 octet) -- Unused, set to zero.

- Key Download Length (2 octets) -- Length in octets of the Key Packet data, including the Key Packet header.

- SPI Size (1 octet) -- Value specifying the length in octets of the SPI as defined by the Protocol-Id.

- SPI (variable length) -- Security Parameter Index which matches a SPI previously sent in an GSAK or GSAT Payload.

- Key Packet Attributes (variable length) -- Contains Key information. The format of this field is specific to the value of the KD Type field. The following sections describe the format of each KD Type.

4.8.1. TEK Download Type

The following attributes may be present in a TEK Download Type. Exactly one attribute matching each type sent in the GSAT payload MUST be present. The attributes must follow the format defined in IKEv2 (Section 3.3.5 of [RFC7296]). In the table, attributes defined as TV are marked as Basic (B); attributes defined as TLV are marked

as Variable (V). The terms Reserved, Unassigned, and Private Use are to be applied as defined in [RFC5226]. The registration procedure is Expert Review.

TEK Class	Value	Type
Reserved	0	
TEK_ALGORITHM_KEY	1	V
TEK_INTEGRITY_KEY	2	V
Unassigned	3-16383	
Private Use	16384-32767	

It is possible that the GCKS will send no TEK key packets in a Registration KD payload (as well as no corresponding GSAT payloads in the GSA payload), after which the TEK payloads will be sent in a rekey message. At least one TEK MUST be included in each Rekey KD payload.

4.8.1.1. TEK_ALGORITHM_KEY

The TEK_ALGORITHM_KEY attribute contains encryption keying material for the corresponding SPI. This keying material will be used with the encryption algorithm specified in the GSAT payload, and according to the IPsec transform describing that encryption algorithm. The keying material is treated equivalent to IKEv2 KEYMAT derived for that IPsec transform. If the encryption algorithm requires a nonce (e.g., AES-GCM), the nonce is chosen as shown in Section 3.2.

4.8.1.2. TEK_INTEGRITY_KEY

The TEK_INTEGRITY_KEY class declares that the integrity key for the corresponding SPI is contained as the Key Packet Attribute. Readers should refer to [IKEV2-IANA] for the latest values.

4.8.2. KEK Download Type

The following attributes may be present in a KEK Download Type. Exactly one attribute matching each type sent in the GSAK payload MUST be present. The attributes must follow the format defined in IKEv2 (Section 3.3.5 of [RFC7296]). In the table, attributes defined as TV are marked as Basic (B); attributes defined as TLV are marked as Variable (V). The terms Reserved, Unassigned, and Private Use are to be applied as defined in [RFC5226]. The registration procedure is Expert Review.

KEK Class	Value	Type
Reserved	0	
KEK_ENCR_KEY	1	V
KEK_INTEGRITY_KEY	2	V
KEK_AUTH_KEY	3	V
Unassigned	4-16383	
Private Use	16384-32767	

If the KEK Key Packet is included, there MUST be only one present in the KD payload.

4.8.2.1. KEK_ENCR_KEY

The KEK_ENCR_KEY attribute declares that the encryption key for the corresponding SPI is contained in the Key Packet Attribute. The encryption algorithm that will use this key was specified in the GSAK payload.

If the mode of operation for the algorithm requires an Initialization Vector (IV), an explicit IV MUST be included in the KEK_ALGORITHM_KEY before the actual key.

4.8.2.2. KEK_INTEGRITY_KEY

The KEK_INTEGRITY_KEY class declares the integrity key for this SPI is contained in the Key Packet Attribute. The integrity algorithm that will use this key was specified in the GSAK payload.

4.8.2.3. KEK_AUTH_KEY

The KEK_AUTH_KEY class declares that the authentication key for this SPI is contained in the Key Packet Attribute. The signature algorithm that will use this key was specified in the GSAK payload. An RSA public key format is defined in RFC 3447, Section A.1.1. DSS public key format is defined in RFC 3279 Section 2.3.2. For ECDSA Public keys, use format described in RFC 5480 Section 2.2.

4.8.3. LKH Download Type

The LKH key packet is comprised of attributes representing different leaves in the LKH key tree.

The following attributes are used to pass an LKH KEK array in the KD payload. The attributes must follow the format defined in IKEv2 (Section 3.3.5 of [RFC7296]). In the table, attributes defined as TV are marked as Basic (B); attributes defined as TLV are marked as Variable (V). The terms Reserved, Unassigned, and Private Use are to

be applied as defined in [RFC5226]. The registration procedure is Expert Review.

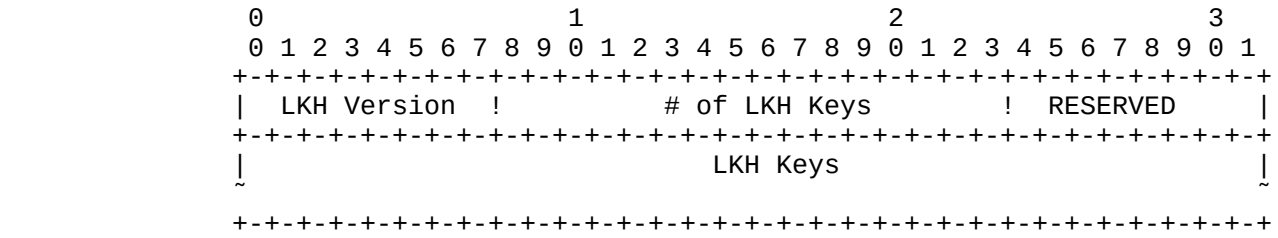
LKH Download Class	Value	Type
Reserved	0	
LKH_DOWNLOAD_ARRAY	1	V
LKH_UPDATE_ARRAY	2	V
Unassigned	3-16383	
Private Use	16384-32767	

If an LKH key packet is included in the KD payload, there MUST be only one present.

4.8.3.1. LKH_DOWNLOAD_ARRAY

This attribute is used to download a set of keys to a group member. It MUST NOT be included in a IKEv2 rekey message KD payload if the IKEv2 rekey is sent to more than one group member. If an LKH_DOWNLOAD_ARRAY attribute is included in a KD payload, there MUST be only one present.

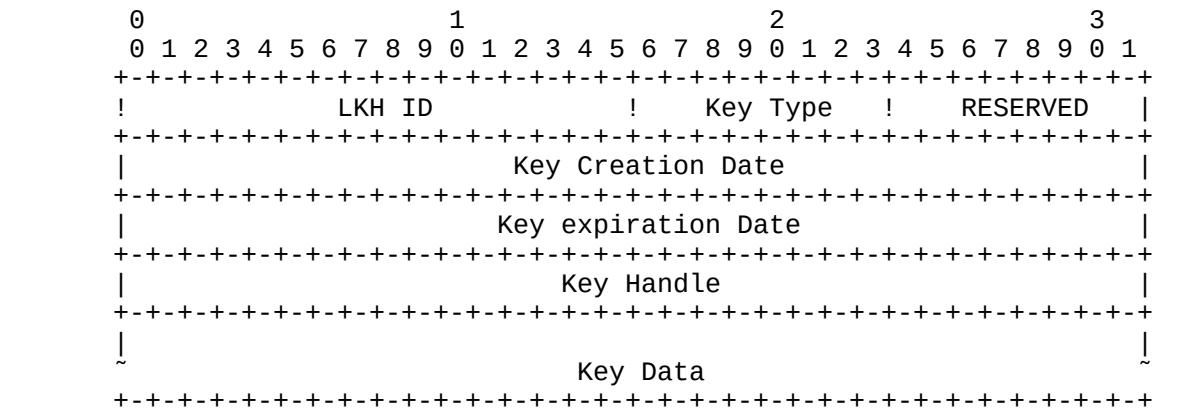
This attribute consists of a header block, followed by one or more LKH keys.



The KEK_LKH attribute fields are defined as follows:

- LKH version (1 octet) -- Contains the version of the LKH protocol which the data is formatted in. Must be one.
- Number of LKH Keys (2 octets) -- This value is the number of distinct LKH keys in this sequence.
- RESERVED (1 octet) -- Unused, set to zero.

Each LKH Key is defined as follows:



- LKH ID (2 octets) -- This is the position of this key in the binary tree structure used by LKH.

- Key Type (1 octet) -- This is the encryption algorithm for which this key data is to be used. This value is specified in Section 4.5.3.

- RESERVED (1 octet) -- Unused, set to zero.

- Key Creation Date (4 octets) -- This is the time value of when this key data was originally generated. A time value of zero indicates that there is no time before which this key is not valid.

- Key Expiration Date (4 octets) -- This is the time value of when this key is no longer valid for use. A time value of zero indicates that this key does not have an expiration time.

- Key Handle (4 octets) -- This is the randomly generated value to uniquely identify a key within an LKH ID.

- Key Data (variable length) -- This is the actual encryption key data, which is dependent on the Key Type algorithm for its format. If the mode of operation for the algorithm requires an Initialization Vector (IV), an explicit IV MUST be included in the Key Data field before the actual key.

The Key Creation Date and Key expiration Dates MAY be zero. This is necessary in the case where time synchronization within the group is not possible.

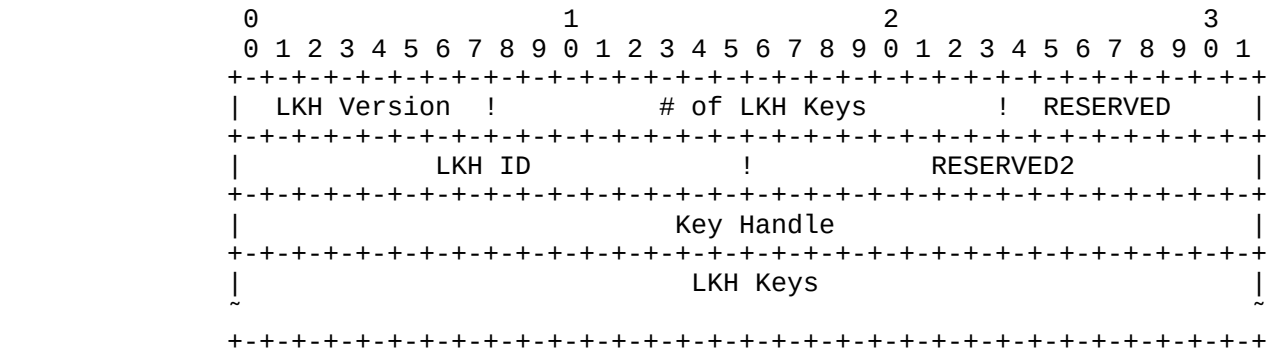
The first LKH Key structure in an LKH_DOWNLOAD_ARRAY attribute contains the Leaf identifier and key for the group member. The rest

of the LKH Key structures contain keys along the path of the key tree in the order starting from the leaf, culminating in the group KEK.

4.8.3.2. LKH_UPDATE_ARRAY

This attribute is used to update the keys for a group. It is most likely to be included in a G-IKEv2 rekey message KD payload to rekey the entire group. This attribute consists of a header block, followed by one or more LKH keys, as defined in Section 4.8.3.1.

There may be any number of UPDATE_ARRAY attributes included in a KD payload.



- LKH version (1 octet) -- Contains the version of the LKH protocol which the data is formatted in. Must be one.

- Number of LKH Keys (2 octets) -- This value is the number of distinct LKH keys in this sequence.

- RESERVED (1 octet) -- Unused, set to zero.

- LKH ID (2 octets) -- This is the node identifier associated with the key used to encrypt the first LKH Key.

- RESERVED2 (2 octets) -- Unused, set to zero.

- Key Handle (4 octets) -- This is the value to uniquely identify the key within the LKH ID which was used to encrypt the first LKH key.

The LKH Keys are as defined in Section 4.8.3.1. The LKH Key structures contain keys along the path of the key tree in the order from the LKH ID found in the LKH_UPDATE_ARRAY header, culminating in the group KEK. The Key Data field of each LKH Key is encrypted with the LKH key preceding it in the LKH_UPDATE_ARRAY attribute. The

first LKH Key is encrypted under the key defined by the LKH ID and Key Handle found in the LKH_UPDATE_ARRAY header.

4.8.4. SID Download Type

This attribute is used to download one or use more Sender-ID (SID) values for the exclusive use of a group member. The terms Reserved, Unassigned, and Private Use are to be applied as defined in [RFC5226]. The registration procedure is Expert Review.

SID Download Class	Value	Type
Reserved	0	
NUMBER_OF_SID_BITS	1	B
SID_VALUE	2	V
Unassigned	3-16383	
Private Use	16384-32767	

Because a SID value is intended for a single group member, the SID Download type MUST NOT be distributed in a GSA_REKEY message distributed to multiple group members.

4.8.4.1. NUMBER_OF_SID_BITS

The NUMBER_OF_SID_BITS class declares how many bits of the cipher nonce in which to represent an SID value. This value applied to each SID value is distributed in the SID Download.

4.8.4.2. SID_VALUE

The SID_VALUE class declares a single SID value for the exclusive use of the a group member. Multiple SID_VALUE attributes MAY be included in a SID Download.

4.8.4.3. GM Semantics

The SID_VALUE attribute value distributed to the group member MUST be used by that group member as the SID field portion of the IV for all Data-Security SAs including a counter-based mode of operation distributed by the GCKS as a part of this group. When the Sender-Specific IV (SSIV) field for any Data-Security SA is exhausted, the group member MUST NOT act as a sender on that SA using its active SID. The group member SHOULD re-register, at which time the GCKS will issue a new SID to the group member, along with either the same Data-Security SAs or replacement ones. The new SID replaces the existing SID used by this group member, and also resets the SSIV value to its starting value. A group member MAY re-register prior to the actual exhaustion of the SSIV field to avoid dropping data

packets due to the exhaustion of available SSIV values combined with a particular SID value.

A group member MUST NOT process an SID Download Type KD payload present in a GSA-REKEY message.

4.8.4.4. GCKS Semantics

If any KD payload includes keying material that is associated with a counter-mode of operation, a SID Download Type KD payload containing at least one SID_VALUE attribute MUST be included. The GCKS MUST NOT send the SID Download Type KD payload as part of a GSA_REKEY message, because distributing the same sender-specific policy to more than one group member will reduce the security of the group.

4.9. Delete Payload

There are occasions when the GCKS may want to signal to receivers to delete policy at the end of a broadcast, or if policy has changed. Deletion of keys MAY be accomplished by sending an IKEv2 Delete Payload, section 3.11 of [RFC7296] as part of the GSA_AUTH or GSA_REKEY Exchange. One or more Delete payloads MAY be placed following the HDR payload in the GSA_AUTH or GSA_REKEY Exchange.

The Protocol ID MUST be 41 for GSA_REKEY Exchange, 2 for AH or 3 for ESP. Note that only one protocol id value can be defined in a Delete payload. If a TEK and a KEK SA for GSA_REKEY Exchange must be deleted, they must be sent in different Delete payloads. Similarly, if a TEK specifying ESP and a TEK specifying AH need to be deleted, they must be sent in different Delete payloads.

There may be circumstances where the GCKS may want to reset the policy and keying material for the group. The GCKS can signal deletion of all policy of a particular TEK protocol by sending a TEK with an SPI value equal to zero in the delete payload. In the event that the administrator is no longer confident in the integrity of the group they may wish to remove all the KEKs and all the TEKs in the group. This is done by having the GCKS send a delete payload with an SPI of zero and a Protocol-ID of AH or ESP Protocol-ID value to delete all TEKs, followed by another delete payload with an SPI value of zero and Protocol-ID of KEK SA to delete the KEK SA.

4.10. Notify Payload

G-IKEv2 uses the same Notify payload as specified in [RFC7296], section 3.10.

There are additional Notify Message types introduced by G-IKEv2 to communicate error conditions and status.

NOTIFY messages - error types	Value
INVALID_GROUP_ID -	45

Indicates the group id sent during registration process is invalid.

AUTHORIZATION_FAILED -	46

Sent in the response to GSA_AUTH message when authorization failed.

NOTIFY messages - status types	Value
SENDER_REQUEST_ID -	16429

Sent in GSA_AUTH or GSA_REGISTRATION to request SIDs from GCKS. The data includes a count of how many SID values it desires.

4.11. Authentication Payload

G-IKEv2 uses the same Authentication payload as specified in [RFC7296], section 3.8, to sign the rekey message.

5. Security Considerations

5.1. GSA registration and secure channel

G-IKEv2 registration exchange uses IKEv2 IKE_SA_INIT protocols, inheriting all the security considerations documented in [RFC7296] section 5 Security Considerations, including authentication, confidentiality, protection against man-in-the-middle, protection against replay/reflection attacks, and denial of service protection. The GSA_AUTH and GSA_REGISTRATION exchanges also take advantage of those protections. In addition, G-IKEv2 brings in the capability to authorize a particular group member regardless of whether they have the IKEv2 credentials.

5.2. GSA maintenance channel

The GSA maintenance channel is cryptographically and integrity protected using the cryptographic algorithm and key negotiated in the GSA member registration exchanged.

5.2.1. Authentication/Authorization

Authentication is implicit, the public key of the identity is distributed during the registration, and the receiver of the rekey message uses that public key and identity to verify the message is come from the authorized GCKS.

5.2.2. Confidentiality

Confidentiality is provided by distributing a confidentiality key as part of the GSA member registration exchange.

5.2.3. Man-in-the-Middle Attack Protection

GSA maintenance channel is integrity protected by using digital signature.

5.2.4. Replay/Reflection Attack Protection

The GSA_REKEY message includes a monotonically increasing sequence number to protect against replay and reflection attacks. A group member will recognize a replayed message by comparing the Message ID number to that of the last received rekey message, any rekey message contains Message ID number less than or equal to the last received value MUST be discarded. Implementations should keep a record of recently received GSA rekey messages for this comparison.

6. IANA Considerations

6.1. New registries

A new set of registries should be created for G-IKEv2, on a new page titled Group Key Management using IKEv2 (G-IKEv2) Parameters. The following registries should be placed on that page. The terms Reserved, Expert Review and Private Use are to be applied as defined in [RFC5226].

GSA Policy Type Registry, see Section 4.4.1

KEK Attributes Registry, see Section 4.5.1

KEK Management Algorithm Registry, see Section 4.5.2

GSA TEK Payload Protocol ID Type Registry, see Section 4.6

TEK Attributes Registry, see Section 4.6

Key Download Type Registry, see Section 4.8

TEK Download Type Attributes Registry, see Section 4.8.1

KEK Download Type Attributes Registry, see Section 4.8.2

LKH Download Type Attributes Registry, see Section 4.8.3

SID Download Type Attributes Registry, see Section 4.8.4

6.2. New payload and exchange types to existing IKEv2 registry

The following new payloads and exchange types specified in this memo have already been allocated by IANA and require no further action, other than replacing the draft name with an RFC number.

The present document describes new IKEv2 Next Payload types, see Section 4.1

The present document describes new IKEv2 Exchanges types, see Section 4.1

The present document describes new IKEv2 notification types, see Section 4.10

7. Acknowledgements

The authors thank Lakshminath Dondeti and Jing Xiang for first exploring the use of IKEv2 for group key management and providing the basis behind the protocol.

8. Contributors

The following individuals made substantial contributions to early versions of this memo.

Sheela Rowles
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA

Phone: +1-408-527-7677
Email: sheela@cisco.com

Aldous Yeung
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA

Phone: +1-408-853-2032
Email: cyyeung@cisco.com

Paulina Tran
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA

Phone: +1-408-526-8902
Email: ptran@cisco.com

9. References

9.1. Normative References

[RFC6054] McGrew, D. and B. Weis, "Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic", RFC 6054, DOI 10.17487/RFC6054, November 2010, <http://www.rfc-editor.org/info/rfc6054>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <http://www.rfc-editor.org/info/rfc7296>.

9.2. Informative References

[IKE-HASH] Kivinen, T., "Fixing IKE Phase 1 & 2 Authentication HASHs", November 2001, <http://tools.ietf.org/html/draft-ietf-ipsec-ike-hash-revised-03>.

[IKEV2-IANA] IANA, "Internet Key Exchange Version 2 (IKEv2) Parameters", February 2016, <http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-7>.

[NNL] Naor, D., Noal, M., and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers", Advances in Cryptology, Crypto '01, Springer-Verlag LNCS 2139, 2001, pp. 41-62, 2001, <http://www.wisdom.weizmann.ac.il/~naor/>.

[OFT] McGrew, D. and A. Sherman, "Key Establishment in Large Dynamic Groups Using One-Way Function Trees", Manuscript, submitted to IEEE Transactions on Software Engineering, 1998, <http://download.nai.com/products/media/nai/misc/oft052098.ps>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, DOI 10.17487/RFC2404, November 1998, <http://www.rfc-editor.org/info/rfc2404>.

[RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, DOI 10.17487/RFC2407, November 1998, <http://www.rfc-editor.org/info/rfc2407>.

[RFC2408] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, DOI 10.17487/RFC2408, November 1998, <http://www.rfc-editor.org/info/rfc2408>.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, DOI 10.17487/RFC2409, November 1998, <http://www.rfc-editor.org/info/rfc2409>.

[RFC2627] Wallner, D., Harder, E., and R. Agee, "Key Management for Multicast: Issues and Architectures", RFC 2627, DOI 10.17487/RFC2627, June 1999, <http://www.rfc-editor.org/info/rfc2627>.

[RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, DOI 10.17487/RFC3686, January 2004, <http://www.rfc-editor.org/info/rfc3686>.

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, DOI 10.17487/RFC4106, June 2005, <http://www.rfc-editor.org/info/rfc4106>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <http://www.rfc-editor.org/info/rfc4301>.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, DOI 10.17487/RFC4309, December 2005, <http://www.rfc-editor.org/info/rfc4309>.

[RFC4543] McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, DOI 10.17487/RFC4543, May 2006, <http://www.rfc-editor.org/info/rfc4543>.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, DOI 10.17487/RFC4868, May 2007, <http://www.rfc-editor.org/info/rfc4868>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, DOI 10.17487/RFC6407, October 2011, <http://www.rfc-editor.org/info/rfc6407>.

Appendix A. Differences between G-IKEv2 and RFC 6407

KE Payload - The KE payload is no longer needed with the availability of newer algorithms such as AES and GCM which provide adequate protection therefore not needing the PFS capability the KE payload offers.

SIG Payload - The AUTH payload is used for the same purpose instead.

DOI/Situation - The DOI and Situation fields in the SA payload are no longer needed in the G-IKEv2 protocol as port 848 will distinguish the IKEv2 messages from the G-IKEv2 messages.

SEQ Payload - The SEQ payload is no longer needed since IKEv2 header has message id which is used to prevent message replay attacks.

Authors' Addresses

Brian Weis
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA

Phone: +1-408-526-4796
Email: bew@cisco.com

Yoav Nir
Check Point Software Technologies Ltd.
5 Hasolelim St.
Tel Aviv 67897
Israel

Email: ynir.ietf@gmail.com

Valery Smyslov
ELVIS-PLUS
PO Box 81
Moscow (Zelenograd) 124460
Russian Federation

Phone: +7 495 276 0211
Email: svan@elvis.ru