PIM
Internet-Draft
Intended status: Standards Track
Expires: January 22, 2015

W. Atwood
B. Li
Concordia University/CSE

July 21, 2014

Group Security Association Management Protocol
draft-atwood-pim-gsam-00

Abstract

This document specifies a Group Security Association Management (GSAM) protocol, which manages the IPsec Group Security Associations that are used to protect some packets of Secure IGMP (SIGMP) and Secure MLD (SMLD). In GSAM, one router is elected as the group controller / key server to create group security associations for all the interesting secure groups and distribute them to authorized users and other routers.

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 January 22, 2015.

Table of Contents

1. Introduction 2
1.1. Terminology 3
2. Assumption 4
3. GSAM Overview 4
4. Phase 1: Registration 4
4.1. Message Exchanges 5
4.1.1. GSAM_INIT Exchange 5
4.1.2. GSAM_AUTH Exchange 5
4.2. EU Operations 6
4.3. Non-Querier Operations 7
4.4. Querier Operations 8
5. Phase 2: GSA Distribution 9
5.1. Message Exchanges 9
5.1.1. GSAM_PUSH Exchange 9
5.1.2. GSAM_RE_DISTRIBUTION Exchange 10
5.2. Querier Operations 11
5.3. GM Operations 12
6. Handover of Q 13
7. IANA Considerations 13
8. References 13
8.1. Normative References 14
8.2. Informative References 14
Authors' Addresses 14

1. Introduction

This document specifies a Group Security Association Management (GSAM) protocol, which manages the IPsec Group Security Associations (GSAs) that are used to protect some packets of Secure IGMP (SIGMP) [I-D.atwood-pim-sigmp]and Secure MLD (SMLD) (not yet issued). GSAM is implemented in the multicast enabled segment. The Querier on this segment is responsible for distributing GSAs to all the authorized users and other routers. Negotiation of certain parameters of the GSA may be triggered if necessary.

GSAM is similar to GDOI [RFC6407] and g-ikev2 [I-D.yeung-g-ikev2], although it is different from these protocols in important ways. First, GDOI and g-ikev2 deliver only the necessary keys for IPsec, while all the parameters of the GSAs of the IPsec system are distributed in GSAM. The GSAs include not only keys, but also security parameter indexes (SPIs) of the IPsec system [RFC4301]. Second, there is a super group, 224.0.0.22 in IPv4 system or FF02:0:0:0:0:0:0:16 in IPv6 system, in GSAM. All the group members

registered in the super group are also registered in all other active groups on this network segment. Third, GSAM is a link-local protocol while GDOI and g-ikev2 are group domain protocols. In GSAM, the TTL of all the messages is equal to 1.

1.1. Terminology

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 [RFC2119].

In addition, the following terms are used in this document

Querier (Q):

A Querier is an edge router that has won in the querier election in SIGMP or SMLD. In GSAM, it takes the role of group controller / key server (GCKS).

Non-Querier (NQ):

A Non-Querier is an edge router that has lost in the querier election in SIGMP or SMLD.

Group Member (GM):

Group Member is an end user or an edge router that has registered in Q.

Secure Group Table (SGT):

Secure Group Table is a table in Q that records the secure groups and the GMs in the secure groups. It consists of two fields: multicast address (MA) and group member set (GMS). MA is an index of SGT and its value is a secure multicast group address. GMS contains the unicast addresses of GMs in a group identified by the value of MA. The initial SGT only has one record whose MA field is 224.0.0.22 in IPv4 system or FF02:0:0:0:0:0:0:16 in IPv6 system and whose GMS field is empty.

GSAM_TEK_SA:

GSAM_TEK_SA is a pair of GSAs, including GSA_q and GSA_r. GSA_q is a GSA of IPsec system used to protect a secure group query in SIGMP or SMLD. GSA_r is a GSA of IPsec system used to protect the secure group report in SIGMP or SMLD.

GSAM_KEK_SA:

GSAM_KEK_SA is a pair of SAs, including KEK_USA and KEK_GSA. KEK_USA is a unicast SA whose direction is from a GM to Q. It is used to protect the messages in Phase 2 sent by GMs. KEK_GSA is a GSA whose direction is from Q to a secure group. It is used to protect the messages in Phase 2 sent by Q.

2. Assumption

The protocol GSAM is based on two assumptions as follows:

The end users have been authenticated and authorized at the application layer. The authorized EU and its Q have shared the same secret key, call MSSK, as a pre-shared key. The details of how to authenticate and authorize users is not specified in this document. It is implemented based on PANA [RFC5191] as shown in draft-atwood-mboned-mrac-pana (not yet issued).

Instead of IGMP or MLD, SIGMP or SMLD is used by users (or routers) to report (or learn) IP multicast group memberships to neighboring multicast routers (or from the users that are only one IP hop away) in an IPv4 network or an IPv6 network.

3. GSAM Overview

GSAM is a protocol that manages group security associations (GSAs) of the IPsec system used to protect some packets of SIGMP or SMLD. The network entities mentioned in GSAM are the same as those in SIGMP or SMLD, including edge routers (ERs) and end users (EUs). In GSAM, an ER (called Querier) plays the role of GCKS. It accepts the registration from EUs and NQs and grants them the status of GMs in secure groups. It creates or updates GSAs of IPsec system for secure groups and distributes them to all GMs in the secure group.

Security parameter index (SPI) as a parameter of GSAs must be paid specific attention. Different from a unicast SA that is used by only one receiver, a GSA is shared by multiple receivers. As a result, instead of one receiver to determine the SPI value, all the GMs in the same secure group should negotiate the SPI value together in order to avoid SPI collisions at GMs. In GSAM, Q suggests SPI values first. If any GM rejects the offered suggestion, a negotiation will be triggered to determine suitable SPI values.

4. Phase 1: Registration

In Phase 1, both NQs and EUs should register themselves in Q in order to become GMs in a group. A pair of SAs, named GSAM_KEK_SA is distributed to GMs.

4.1. Message Exchanges

The registration involves two message exchanges: GSAM_INIT exchange and GSAM_AUTH exchange. An EU / NQ performs GSAM_INIT exchange only once as long as no new Q is elected in SIGMP or SMLD. However, an EU may perform a GSAM_AUTH exchange many times. The number of GSAM_AUTH exchanges for an EU is equal to the number of secure groups that an EU is authorized to join at the application layer.

4.1.1. GSAM_INIT Exchange

GSAM_INIT exchange is identical to IKE_SA_INIT of IKE v2 defined in [RFC5996]. An EU / NQ takes the role of an initiator and Q takes the role of a responder.

4.1.2. GSAM_AUTH Exchange

GSAM_AUTH exchange as shown in Figure 1 is similar to IKE_AUTH of IKE v2. In this exchange, an EU / NQ and Q mutual authenticate for a secure group. However, instead of being negotiated between two peers as in IKE v2, an SA pair, named GSAM_KEK_SA, is downloaded from Q to an EU / NQ.

```
EU / NQ -> Q: HDR, SK{ IDg, IDh, AUTH }
Q -> EU / NQ: HDR, SK{ IDg, SA, KD, AUTH}
```

Figure 1: GSAM_AUTH Exchange

HDR is a header payload whose format is identical to that in IKE v2. The notation SK { ... } indicates that all the payloads in "{}" are encrypted and integrity protected using an SA, called GSAM_INIT_SA, which is negotiated in the GSAM_INIT Exchange. The message exchange is explained as follows:

In the first message, an EU / NQ asserts its identification and the identification of a secure group (i.e., for an EU, it is the group that an EU requests to join in SIGMP or SMLD; for an NQ, it is the group 224.0.0.22 in IPv4 system or FF02:0:0:0:0:0:0:16 in IPv6 system listened to by all ERs) in the payload of IDh and IDg respectively. Moreover, an EU / NQ also declares a message authentication code (MAC) or its signature in the AUTH payload. The AUTH payload is used by the message receiver (Q) to authenticate the two identifications in IDh and IDg and to protect the integrity of the first message in the GSAM_INIT exchange.

In the second message, Q asserts its identification in payload IDq and distributes an SA pair, called GSAM_KEK_SA, (and more KEK_GSAs

sometimes) in payloads SA and KD. Moreover, Q also declares a MAC or its signature in AUTH payload. The AUTH payload is used by the message receiver (an EU / NQ) to authenticate the identification in payload IDq and protect the integrity of the second message in the GSAM_INIT exchange.

4.2. EU Operations

An EU initiates a GSAM_INIT exchange when an EU requests GSAs to secure SIGMP packets or SMLD packets for the first time or when an EU discovers a new Q. The EU operations in a GSAM_INIT exchange are identical to the initiator operations in the IKE_SA_INIT exchange of IKE v2.

After the GSAM_INIT exchange, a new security association, named GSAM_INIT_SA, has been negotiated. It will be used to protect the GSAM_AUTH exchange and achieve private communication between an EU and Q. Moreover, GSAM_INIT_SA will be maintained as a long-term security association. No new GSAM_INIT exchange between an EU and Q will be required for the subsequent request for GSAs as long as an EU does not discover a new Q.

An EU initiates a GSAM_AUTH exchange when a request for GSAs is received from SIGMP and GSAM_INIT_SA has been negotiated between an EU and Q. An EU must use the pre-shared key authentication method to finish the registration in the GSAM_AUTH exchange.

An EU calculates a MAC and encapsulates it in the AUTH payload of the first message of GSAM_AUTH. The calculation of the MAC is the same as that in IKE v2. The secret key used in the MAC is the MSSK for the secure group calculated at the network layer. It has been independently derived by the EU and the Q as a pre-shared key when an EU has been authorized to join in the secure group at the application layer.

Upon receiving the second message of GSAM_AUTH, an EU verifies the value in the received AUTH payload using the MSSK to authenticate Q. If verification fails, the EU will discard the received message. Otherwise, verification succeeds and the EU will accept the GSAM_KEK_SA specified in the SA and KD payloads. Moreover, an EU marks itself as a GM in the requested secure group. The EU updates its local GSPD [RFC5374] as shown in Table 1. G_IP is the IP address of the group identified in the IDg payload. Q_IP and H_IP are the IP addresses of the Q and the EU. The updated records in the GSPD indicate that the SIGMP/SMLD packets that are sent from a GM / Q to the group that a GM wants to join must be protected by IPsec.

Destination address	Source address	Protocol number	Action
G_IP	Q_IP	SIGMP(2)	IPsec protect
G_IP	H_IP	SIGMP(2)	IPsec protect
G_IP	*	SIGMP(2)	Discard
G_IP	*	*	Bypass

Table 1: Updated Records in local GSPD

Finally, the EU must update the SAD, to record the SA paremeters that have been given to it.

4.3. Non-Querier Operations

An NQ initiates a GSAM_INIT exchange when an ER has just lost in the querier election for SIGMP/SMLD and has become an NQ. NQ operations in the GSAM_INIT exchange are identical to the initiator operations in IKE_SA_INIT of IKE v2.

After the GSAM_INIT exchange, GSAM_INIT_SA has been negotiated. It will be used to protect the GSAM_AUTH exchange and achieve private communication between an NQ and Q. Moreover, the GSAM_INIT_SA will be maintained as a long-term security association. No new GSAM_INIT exchange between an NQ and Q is necessary as long as an NQ does not discover a new Q.

An NQ initiates a GSAM_AUTH exchange when an ER where an NQ is located has just lost in a querier election in SIGMP / SMLD and a GSAM_INIT_SA has been negotiated between an NQ and Q. An NQ could use any authentication method configured by the network administrator to finish registration in GSAM_AUTH.

An NQ calculates a MAC or a signature according to the assigned authentication method and encapsulates it into the AUTH payload of the first message. Here the authentication method depends on the configuration of the network administrator.

Upon receiving the second message of GSAM_AUTH, an NQ verifies the value in the received AUTH payload to authenticate Q using the assigned method. If verification fails, an NQ will discard the received message. Otherwise, verification succeeds and an NQ will accept the GSAM_KEK_SA (and more KEK_GSAs if existing) specified in the SA and KD payloads. Moreover, an NQ marks itself as a GM in the

group 224.0.0.22 for IPv4 system or FF02:0:0:0:0:0:0:16 for IPv6 system (and also a GM in all the groups mentioned in KEK_GSAs). If additional KEK_GSAs are specified in SA and KD payloads, NQ also updates its local GSPD as shown in Table 1 and G_IP indicates all the IP addresses of the groups mentioned in additional KEK_GSAs.

4.4. Querier Operations

Q operations in the GSAM_INIT exchange are identical to the responder operations in IKE_SA_INIT of IKE v2.

Upon receiving the first message of GSAM_AUTH exchange, Q parses the payload of IDg. If IDg identifies a super group (224.0.0.22 for IPv4 system or FF02:0:0:0:0:0:0:16 for IPv6 system), the sender of the message is considered to be an NQ. Otherwise, the sender is considered to be an EU.

If the sender is an EU, Q retrieves the pre-shared key MSSK shared with the EU identified in the received IDh payload for a secure group identified in the received IDg payload. Similarly, if the sender is an NQ, Q retrieves a certification or a secret key of an NQ identified in IDh payload. Then Q uses the retrieved key or certification to verify the received AUTH payload. If retrieval or verification fails, Q will discard the received message and terminate the GSAM_AUTH exchange. Otherwise, it indicates that an EU has been authorized to join the secure group at the application layer or an NQ has been authorized by the network administrator in its configuration file. In this case, Q starts the "registration" to an EU for the secure group or an NQ for all secure groups.

The registration is based on a secure group table (SGT). For an NQ, Q updates all the records in SGT: the source address of the received message is added into GMS field of all the records. It means an NQ becomes a GM in all the groups that Q is maintaining. For an EU, Q searches its SGT to look for a record whose MA is the address of the group identified in the received IDg payload. If the record is found, the source address of the received message is added into GMS of the found record. It means an EU becomes a GM in the group identified in the received IDg payload. Otherwise, Q creates a new record in SGT. In the new record, the value of the MA field is the address of the group identified in the received IDg payload. The addresses showing in the GMS field of the record indexed by 224.0.0.22 (or FF02:0:0:0:0:0:0:16) are copied into the GMS field of the new record. Moreover, the source address of the received message is also filled in the GMS of the new record. It means the EU and all the registered NQs become GMs of the group identified in the received IDg payloads. After the registration of an EU, Q updates its local GSPD as Table 1.

After registration, Q creates an SA pair, named GSAM_KEK_SA, which consists of two SAs: 1) KEK_GSA and 2) KEK_USA. KEK_GSA is a group security association whose direction is from Q to a secure group identified in the received IDg payload. In detail, when the exchange is between an EU and Q, the direction of KEK_GSA is from Q to a secure group that an EU requests to join. When the exchange is between an NQ and Q, the direction is from Q to the group 224.0.0.22 or FF02:0:0:0:0:0:0:16. It is used to protect the messages in Phase 2 sent by Q. KEK_USA is a unicast security association whose direction is from the new GM (an EU/NQ) to Q. It is used to protect the message in Phase 2 sent by GMs.

Moreover, Q also calculates a new MAC or a signature according to the negotiated authentication method. If the exchange is between an EU and Q, the authentication method must be pre-shared key. Q uses the retrieved MSSK as the secret key to calculate a MAC value. If the exchange is between an NQ and Q, the authentication method depends on the network configuration of an NQ. Q may calculate a MAC or a signature for NQ.

After that, Q sends to an EU / NQ the second message as a response. In the response to an EU, SA and KD payloads specify the newly created GSAM_KEK_SA. In the response to an NQ, SA and KD payloads specified not only the newly created GSAM_KEK_SA, but also all other KEK_GSAs that Q is maintaining. the AUTH payload contains the new MAC or signature.

5. Phase 2: GSA Distribution

In Phase 2, Q suggests GSAM_TEK_SA to GMs. If any GM rejects the suggestion due to SPI collisions, a negotiation will be required among GMs.

5.1. Message Exchanges

There are two exchanges in GSA distribution: GSAM_PUSH and GSAM_RE_DISTRIBUTION.

5.1.1. GSAM_PUSH Exchange

GSAM_PUSH exchange is shown in Figure 2 .

Q -> GMs: HDR, SK{ SA, KD, AUTH}

Figure 2: GSAM_PUSH Exchange

In this message, Q distributes an SA pair (i.e., GSAM_TEK_SA, but sometimes more GSAM_TEK_SAs) or an SA (i.e., KEK_GSAs) in the payload SA and KD. Moreover, Q declares a signature in payload AUTH. The notation SK {...} indicates that all the payloads in "{}" are encrypted and integrity protected using a KEK_GSA.

5.1.2. GSAM_RE_DISTRIBUTION Exchange

The GSAM_RE_DISTRIBUTION exchange is triggered when any GM detects an SPI collision and refuses to accept the GSAM_TEK_SA received in the GSAM_PUSH message. In other words, it is just optional: there is no GSAM_RE_DISTRIBUTION exchange if no SPI collisions are detected by any GM. The GSAM_RE_DISTRIBUTION exchange is shown in Figure 3. All the messages are protected by GSAM_KEK_SA. It is explained as follows:

```
GM -> Q :  HDR, SK{ IDg, REJ, AUTH }
Q -> GMs: HDR, SK{ S_REQ, AUTH }
GMs -> Q: HDR, SK{ SPI_LIST, AUTH }
Q -> GMs: HDR, SK{ SAtf, KDtf, AUTH }
```

Figure 3: GSAM_RE_DISTRIBUTION Exchange

In the first message, a GM that detects an SPI collision asserts the identification of the secure group that is the destination address of the rejected GSAM_TEK_GSA in payload IDg and shows its rejection to the suggested GSAM_TEK_GSA in payload REJ. Moreover, GM declares a MAC in payload AUTH.

Q multicasts the second message into a secure group identified by the received IDg. In this message, Q requests a list, called spi_list, in payload S_REQ and shows its signature in payload AUTH.

All GMs in the secure group will send the third message to respond to the request from Q. In the third message, a GM reports its spi_list in payload SPI_LIST and declares its MAC in the payload AUTH.

The fourth message is the same as the GSAM_PUSH message. In the fourth message, Q multicasts an SA pair (i.e., GSAM_TEK_SA) in payload SA and KD and declares a signature in the AUTH payload. However, the SPI parameter in GSAM_TEK_SA has been negotiated with all GMs in the secure group and therefore it cannot cause any collision.

5.2. Querier Operations

When an EU is registered as the first GM of a secure group in the segment, Q will multicast the GSAM_PUSH exchange message in two groups in order: (1) the group 224.0.0.22 or FF02:0:0:0:0:0:0:16 and (2) the secure group that an EU requests to join.

Q multicasts the first multicast GSAM_PUSH message into group 224.0.0.22 or FF02:0:0:0:0:0:0:16. In this message, the KEK_GSA that is just distributed to an EU using GSAM_AUTH exchange is specified in the payloads of SA and KD.

Q creates a new SA pair, called GSAM_TEK_SA, which consists of two GSAs: (1) GSA_q whose direction is from Q to the secure group that an EU (the new GM) requests to join and (2) GSA_r whose direction is from an EU to the secure group that an EU requests to join. The values of important parameter of SPI in GSA_q and GSA_r are suggested ones since they are assigned by Q with no negotiation with other GMs.

After making sure that all the NQs have received the previous GSAM_PUSH message, Q starts to multicast the other GSAM_PUSH message into the group that the EU has requested to join. In the second message, the payloads SA and KD specify the parameter and key material of the new SA pair (GSAM_TEK_SA).

After that, Q starts two timers, called q-timer and r-timer respectively. When q-timer / r-timer expires, Q will update its local SAD [RFC5374] according to GSA_q / GSA_r. The initial value of q-timer should be large enough to make sure all GMs have updated their local SADs according to the distributed GSA_q.

There must be an interval between the first GSAM_PUSH message and the second one. The interval should be large enough to make sure the first message has been received by GMs in 224.0.0.22 or FF02:0:0:0:0:0:0:16 before the second one is sent.

If the registered EU is not the first GM of a secure group, Q multicasts the second GSAM_PUSH message directly without the first message.

When an NQ is registered as a GM in all the groups, Q will directly multicast GSAM_PUSH exchange message in the group of 224.0.0.22 for IPv4 system or FF02:0:0:0:0:0:0:16 for IPv6 system. In this message, GSAM_TEK_GSAs for all the groups are specified in the payloads SA and KD. If the only group Q is maintaining is the super group, no GSAM_PUSH exchange is needed.

Upon receiving the first message of GSAM_RE_DISTRIBUTION, Q verifies the value in the payload AUTH to authenticate a GM. If authentication fails, Q discards the received message directly. Otherwise, Q deletes the q_timer and r_timer if they exist. It multicasts the second message of GSAM_RE_DISTRIBUTION to negotiate SPI values with all the GMs in the secure group.

Upon receiving the third message, Q verifies the AUTH payload to authenticate a GM. If authentication fails, Q discards the received message directly. Otherwise, Q searches its local SGT and looks for a record that is indexed by a secure group identified in the received IDg. The GMS of the found record contains the addresses of all the GMs in the secure group. Q compares the source addresses of the received third messages with the values in the GMS until it has received the third message from all the GMs in the secure group.

After that, Q starts to calculate a list, called spi_list_all, which is a union of spi_lists received from all GMs in the secure group. Then Q resets the values of SPI in GSAM_TEK_SA. The new SPI values must not be in the spi_list_all to effectively avoid SPI collisions at any GM. Then Q multicasts the fourth message of GSAM_RE_DISTRIBUTION, whose payloads SA and KD specify the revised GSAM_TEK_SA. Finally, Q re-starts q-timer and r-timer. When q-timer / r-timer expires, Q updates its local SAD according to GSA_q / GSA_r whose SPI value has been negotiated among GMs.

5.3. GM Operations

Upon receiving the GSAM_PUSH message, a GM verifies the value in the payload AUTH to authenticate Q. If authentication fails, a GM discards the received message directly. Otherwise, a GM parses the received payloads SA and KD. If payloads SA and KD specify KEK_GSAs and a GM is an NQ, a GM will accept the KEK_GSA directly and wait for receiving the following GSAM_PUSH message protected by KEK_GSA. Otherwise payloads SA and KD specify a GSAM_TEK_SA. In this case, a GM checks SPI, an important parameter of GSAM_TEK_SA. If SPI values in GSAM_TEK_SA have not used in its local SAD, a GM will start q-timer and r-timer and no other exchange is needed. When q-timer/ r-timer expires, a GM updates its local SAD according to GSA_q / GSA_r. If the source address of received GSA_r is the same as a local address, the initial value of r-timer should be large enough to make sure all other GMs and Q have updated their local SADs according to GSA_r. If the suggested SPI values in GSAM_TEK_SA have collided with the used SPI values in local SAD, a GM must start GSAM_RE_DISTRIBUTION exchange as follows.

A GM calculates a MAC and encapsulates it in AUTH payload. Then it sends the first message of GSAM_RE_DISTRIBUTION to Q to show its rejection.

Upon receiving the second message in GSAM_RE_DISTRIBUTION, a GM verifies the received AUTH payload. If the verification fails, a GM discards the received message. Otherwise, a GM deletes the pending q-timer and r-timer at once if they exist. It accesses its local SAD to obtain the all the used SPI values in the SAD and saves them in an spi_list. After that, the status of local SADB is set as "read_only" to prevent any modification from any other processes. The GM encapsulates an spi_list in the payload SPI_LIST. Moreover, a MAC value is calculated and encapsulated in the AUTH payload. After that, the GM sends the third message with the payload SPI_LIST and AUTH payload.

Upon receiving the fourth message in GSAM_RE_DISTRIBUTION, the GM verifies the value in the payload AUTH to authenticate Q. If authentication fails, the GM discards the received message directly. Otherwise, the GM is forced to accept GSAM_TEK_SA specified in the received payload SA and KD. It re-starts q-timer and r-timer. When q-timer/r-timer expires, a GM updates its local SAD according to GSA_q/GSA_r. After that, GMs clears the "read_only" status of its local SAD to permit the modification to the SAD from other processes.

6. Handover of Q

Although ERs are usually stable, a new ER may be added into the network and an old ER may fail to work. In these cases, a querier election is caused and then a new Q may be elected in the link. The new Q will take over the work of old Q automatically and become GCKS soon in the link. All the EUs and NQs will discover the new Q since they will receive the general query sent by the new Q in SIGMP/SMLD. They initiate new GSAM sessions with the new Q. If they are authenticated successfully, the new Q will distribute new GSAM_TEK_SAs to them. SIGMP / SMLD messages will be protected by the new GSAM_TEK_SAs.

7. IANA Considerations

GSAM runs over UDP. A UDP port should be assigned to GSAM.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

[I-D.atwood-pim-sigmp]
william.atwood@concordia.ca, w. and B. Li, "Secure Internet Group Management Protocol", draft-atwood-pim-sigmp-01 (work in progress), July 2014.

[I-D.yeung-g-ikev2]
Rowles, S., Yeung, A., Tran, P., and Y. Nir, "Group Key Management using IKEv2", draft-yeung-g-ikev2-07 (work in progress), November 2013.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

[RFC5374] Weis, B., Gross, G., and D. Ignjatic, "Multicast Extensions to the Security Architecture for the Internet Protocol", RFC 5374, November 2008.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, October 2011.

Authors' Addresses

William Atwood
Concordia University/CSE
1455 de Maisonneuve Blvd, West
Montreal, QC H3G 1M8
Canada

Phone: +1(514)848-2424 ext3046
Email: william.atwood@concordia.ca
URI: http://users.encs.concordia.ca/~bill

Bing Li
Concordia University/CSE
1455 de Maisonneuve Blvd, West
Montreal, QC H3G 1M8
Canada

Email: leebingice@gmail.com