

SSE BOF
Internet-Draft
Intended status: Standards Track
Expires: December 29, 2017

R. Moskowitz
L. Xia
Huawei
I. Faynberg
Stargazers Consulting, LLC
S. Hares
Hickory Hill Consulting
P. Giacomini
Freelance
June 27, 2017

Secure Session Layer Services KMP via HIP
draft-moskowitz-ssls-hip-02

Abstract

This memo specifies the details for establishing and maintaining a Secure Session Layer Services (SSLS) association between two applications using the Host Identity Protocol (HIP [[RFC7401](#)]). This is primarily achieved by adding SSLS specific HIP parameters for the HIP base exchange. The SSLS association state and security boundaries are also defined.

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 December 29, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect 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	2
2.	Terms and Definitions	3
2.1.	Requirements Terminology	3
2.2.	Notations	3
2.3.	Definitions	3
3.	Discovering an SSLS application peer	3
4.	HIP parameters to negotiate and manage SSLS	3
4.1.	SSE_INFO	4
4.2.	SSE_TRANSFORM	5
4.3.	SSE_FORMAT	6
4.4.	GPCOMP_INFO	7
4.5.	SSLS_INFO	7
4.6.	NOTIFICATION Parameter	8
5.	Security Boundaries and APIs	8
5.1.	Application to HIP API	9
6.	HIP mobility and SSLS	10
7.	IANA Considerations	10
8.	Security Considerations	10
9.	Acknowledgments	11
10.	References	11
10.1.	Normative References	11
10.2.	Informative References	11
	Authors' Addresses	13

[1.](#) Introduction

The Secure Session Layer Services (SSLS) [[I-D.hares-i2nsf-ssls](#)] provides a well defined session layer that can be implemented in any application to provide any or all of the following:

- o data compression
- o chunking of data

- o secure envelope
- o fragmentation and reassembly

Applications implementing SSLS may need to negotiate the use of this service and its components. They must be able to negotiate the security association to support the use of the Session Security Envelope (SSE [[I-D.moskowitz-sse](#)]). HIP is an ideal protocol to support this association management. The SSE management requirement closely parallels HIP support of ESP [[RFC7402](#)] to the extent that [Section 4](#) need only define the new parameter and point to [[RFC7402](#)] for the processing details.

[2.](#) Terms and Definitions

[2.1.](#) Requirements 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 [RFC 2119](#) [[RFC2119](#)].

[2.2.](#) Notations

This section will contain notations

[2.3.](#) Definitions

GPcomp: General Purpose Compression.

SSE: Session Specific Envelope.

[3.](#) Discovering an SSLS application peer

A HIP enabled SSLS application needs to discover its peer application. This could be manually configured, discovered via DNS, or some other services discovery mechanism.

In the DNS example, the application recognizes the returned address as a HIT and the HI RR record. It next needs to discover the IP address for this HIT. If the HIT is Hierarchical

[[I-D.moskowitz-hierarchical-hip](#)], it can use the HHIT DNS reverse lookup mechanism. In either case, the IP address may be that of the peer application's RVS [[RFC8004](#)].

Any other service discovery mechanism still has to provide the HIT, HI, and IP address as a minimal set of information.

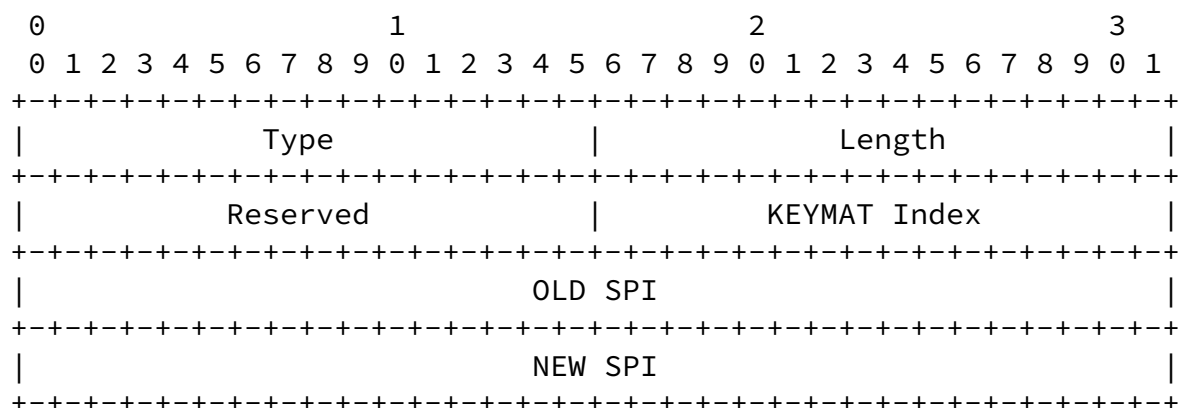
4. HIP parameters to negotiate and manage SSLs

Five HIP parameters are defined for setting up SSLS associations in HIP communication and for restarting existing ones. Also, the

NOTIFICATION parameter, described in [[RFC7401](#)], has four new error parameters.

Parameter	Type	Length	Data
SSE_INFO	[TBD-IANA]	12	Remote's old SPI, new SPI
SSE_TRANSFORM	[TBD-IANA]	variable	SSE Encryption and Authentication Transform(s)
SSE_FORMAT	[TBD-IANA]	variable	SSE Format
GPCOMP_INFO	[TBD-IANA]	12	Compression Algorithm
SSLS_INFO	[TBD-IANA]	8	SSLS chunking and fragmenting

4.1. SSE INFO



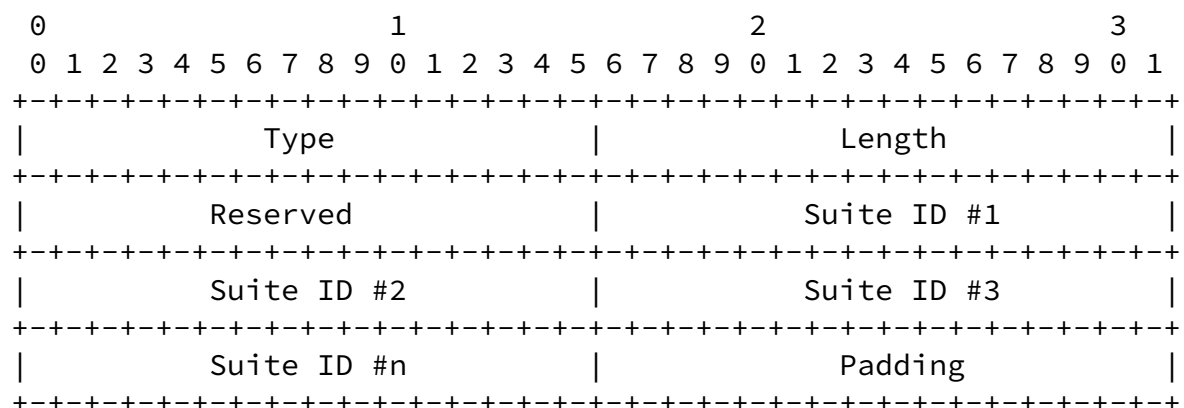
Type	[TBD-IANA]
------	------------

Length	12
KEYMAT Index	index, in bytes, where to continue to draw SSE keys from KEYMAT. If the packet includes a new Diffie-Hellman key and the SSE_INFO is sent in an UPDATE packet, the field MUST be zero. If the SSE_INFO is included in base exchange messages, the KEYMAT Index must have the index value of the point from where the SSE SA keys are drawn. Note that the length of this field limits the amount of keying material that can be drawn from KEYMAT. If that amount is exceeded, the packet MUST contain a new Diffie-Hellman key.
OLD SPI	old SPI for data sent to address(es) associated with this SA. If this is an initial SA setup, the OLD SPI value is zero.
NEW SPI	new SPI for data sent to address(es) associated with this SA.

The processing of SSE_INFO is similar to ESP_INFO, [section 5.1.1 of RFC7402](#) [RFC7402], without the KEYMAT generation.

4.2. SSE_TRANSFORM

The SSE_TRANSFORM parameter is used during SSE SA establishment. The first party sends a selection of transform families in the SSE_TRANSFORM parameter, and the peer must select one of the proposed values and include it in the response SSE_TRANSFORM parameter.



Type	[TBD-IANA]
Length	length in octets, excluding Type, Length, and padding.
Reserved	zero when sent, ignored when received.
Suite ID	defines the SSE Suite to be used.

The following Suite IDs can be used:

Suite ID	Value	
RESERVED	0	[this draft]
RESERVED	1 - 9	[this draft]
AES-CCM-8	10	[RFC4309]
AES-CCM-16	11	[RFC4309]
AES-GCM with an 8-octet ICV	12	[RFC4106]
AES-GCM with a 16-octet ICV	13	[RFC4106]
AES-CMAC-96	14	[RFC4493], [RFC4494]
AES-GMAC	15	[RFC4543]

SSE only supports the newer CCM and GCM modes of operation. The Suite ID assignments are as above to align with [[RFC7402](#)].

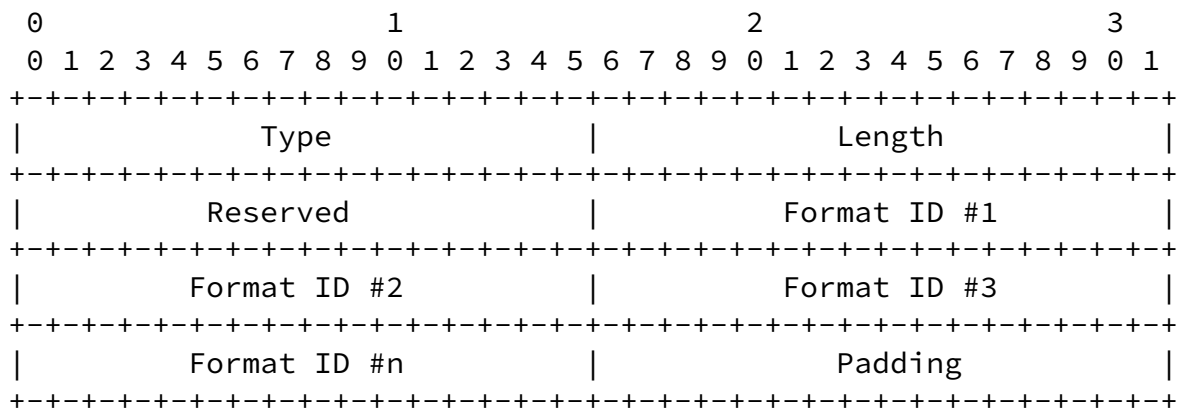
The sender of an SSE transform parameter MUST make sure that there are no more than six (6) Suite IDs in one SSE transform parameter. Conversely, a recipient MUST be prepared to handle received transform parameters that contain more than six Suite IDs. The limited number

of Suite IDs sets the maximum size of the SSE_TRANSFORM parameter. As the default configuration, the SSE_TRANSFORM parameter MUST contain at least one of the mandatory Suite IDs. There MAY be a configuration option that allows the administrator to override this default.

Mandatory implementations: AES-CCM-16. AES-CMAC-96 SHOULD also be supported.

[4.3.](#) SSE_FORMAT

The SSE_FORMAT parameter is used during SSE SA establishment. The first party sends a selection of formats in the SSE_FORMAT parameter, and the peer must select one of the proposed values and include it in the response SSE_FORMAT parameter.



Type	[TBD-IANA]
Length	length in octets, excluding Type, Length, and padding.
Reserved	zero when sent, ignored when received.
Format ID	defines the SSE Format to be used.

The following Format IDs can be used:

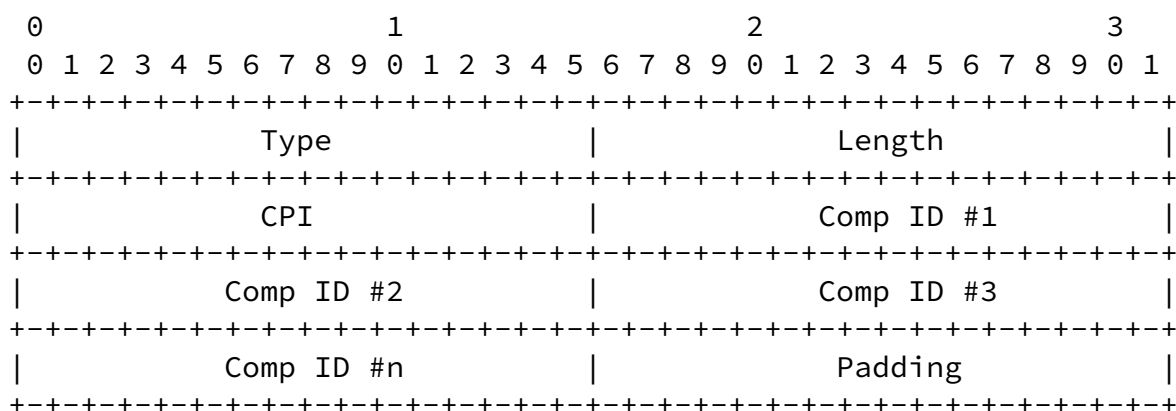
Format ID	Value	
RESERVED	0	[this draft]
Compact	1	[I-D.moskowitz-sse]
Large	2	[I-D.moskowitz-sse]
Extreme	3	[I-D.moskowitz-sse]

The sender of an SSE format parameter MUST make sure that there are no more than six (6) Format IDs in one SSE format parameter. Conversely, a recipient MUST be prepared to handle received format parameters that contain more than six Format IDs. The limited number

of Format IDs sets the maximum size of the SSE_FORMAT parameter. As the default configuration, the SSE_FORMAT parameter MUST contain at least one of the mandatory Format IDs. There MAY be a configuration option that allows the administrator to override this default.

Mandatory implementations: Compact

[4.4.](#) GPCOMP_INFO



Type [TBD-IANA]

Length length in octets, excluding Type, Length, and padding.

Suite ID defines the SSE Suite to be used.

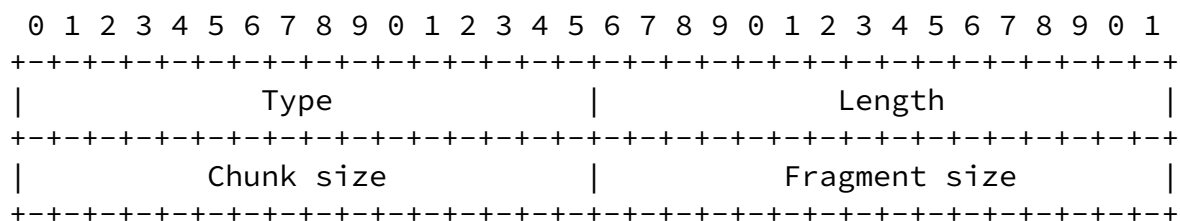
The following Comp IDs can be used:

Comp ID	Value		
RESERVED	0	[this draft]	
GPCOMP_OUI	1	(UNSPECIFIED)	
GPCOMP_DEFLATE	2	[RFC 2394]	
GPCOMP_LZS	3	[RFC 2395]	
GPCOMP_LZJH	4	[RFC 3051]	

The Comp ID has the same interpretation as IPcomp, [section 2.22 of RFC7402](#) [\[RFC7296\]](#).

The processing of GPCOMP_INFO is similar to ESP_TRANSFORM, [section 5.1.2 of RFC7402](#) [\[RFC7402\]](#).

[4.5.](#) SSLS_INFO



Type

[TBD-IANA]

Length

8

Chunk size

Maximum data chunk supported. 0 if no chunking.

Fragment size

Maximum data fragment supported. 0 if no fragmenting.

4.6. NOTIFICATION Parameter

The HIP base specification defines a set of NOTIFICATION error types. The following error types are required for describing errors in ESP Transform crypto suites during negotiation.

NOTIFICATION PARAMETER – ERROR TYPES	Value
NO_SSE_PROPOSAL_CHOSEN	20
None of the proposed SSE Transform crypto suites was acceptable.	
INVALID_SSE_TRANSFORM_CHOSEN	21
The SSE Transform crypto suite does not correspond to one offered by the Responder.	
NO_SSE_FORMAT_CHOSEN	22
None of the proposed SSE Format suites was acceptable.	
INVALID_SSE_FORMAT_CHOSEN	23
The SSE Format suite does not correspond to one offered by the Responder.	

5. Security Boundaries and APIs

When an application has direct control over the security of the communication, even when this is done via external modules, extreme care is needed in managing the environment. This is why HIP communicates some values directly to the SSE and GPcomp modules.

This way the application cannot override their action. This does require the application to be able to accept calls from HIP itself whenever an event changes the SPIs for an association.

[5.1.](#) Application to HIP API

It is assumed the application has learned the peer HIT and IP address before invoking HIP. Thus the calling parameters are:

- Source HIT, HI, and IP address
- Destination HIT, HI, and IP address
- SSE acceptable Transform and Format lists
- GPcomp acceptable Algorithms list [Null if no compression]
- Max chunk size [0 = no chunking]
- Max fragment size [0 = no fragmenting]

HIP returns to the calling application:

- Source HIT, HI, and IP address
- Actual destination HIT, HI, and IP address
- SSE SPIs
- SSE agreed format
- GPcomp status [Yes/No]
- Agreed max chunk size [0 = no chunking]
- Agreed max fragment size [0 = no fragment]

HIP sends to the SSE module:

- SSE SPIs
- SSE agreed transform
- SSE session keys [Note: SSE controls HIP rekeying based on transform and Sequence Number. In which case HIP will notify the application of a change to the SPIs]

HIP sends to the GPcomp module:

- SSE SPIs
- GPcomp agreed algorithm

Internet-Draft

SSLS kmp via HIP

June 2017

6. HIP mobility and SSLS

The HIP module SHOULD detect an IP address change for an interface and initiate a HIP Mobility operation [[RFC8046](#)]. It will then inform the SSLS application of the address change and any SPI changes to the application and other components.

An example of this is a CPE gateway managed with RESTCONF on a PPPoE link that has restarted and had a new IP address assigned. The RESTCONF server would be able to apply any configuration changes to the gateway without needing to wait for the gateway to call back first.

7. IANA Considerations

This document defines five Parameter Types and four NOTIFY Message Types for the Host Identity Protocol [[RFC7401](#)].

SSE_INFO: This document defines the new SSE_INFO parameter (see [Section 4.1](#)). The parameter value will be assigned by IANA. Its value should come from the 66-127 range.

SSE_TRANSFORM: This document defines the new SSE_TRANSFORM parameter (see [Section 4.2](#)). The parameter value will be assigned by IANA. Its value should come from the 4096-4480 range.

SSE_FORMAT: This document defines the new SSE_FORMAT parameter (see [Section 4.3](#)). The parameter value will be assigned by IANA. Its value should come from the 4096-4480 range.

GPCOMP_INFO: This document defines the new GPCOMP_INFO parameter (see [Section 4.4](#)). The parameter value will be assigned by IANA. Its value should come from the 66-127 range. It should be greater than SSE_INFO.

SSLS_INFO: This document defines the new SSLS_INFO parameter (see [Section 4.5](#)). The parameter value will be assigned by IANA. Its value should come from the 66-127 range.

The new NOTIFY error types and their values are defined in [Section 4.6](#), and they have been added to the Notify Message Type namespace created by [\[RFC7401\]](#).

[8.](#) Security Considerations

Security boundaries must be rigorously observed. Care is taken in terms of what information is known to which module. Still the

Moskowitz, et al.

Expires December 29, 2017

[Page 10]

Internet-Draft

SSLS kmp via HIP

June 2017

application possesses both the clear and crypto text and can thus be an attack point against the session keys.

[9.](#) Acknowledgments

TBD

[10.](#) References

[10.1.](#) Normative References

- [I-D.hares-i2nsf-ssls]
Hares, S. and R. Moskowitz, "Secure Session Layer Services", [draft-hares-i2nsf-ssls-00](#) (work in progress), March 2016.
- [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>>.
- [RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", [RFC 7401](#), DOI 10.17487/RFC7401, April 2015, <<http://www.rfc-editor.org/info/rfc7401>>.
- [RFC7402] Jokela, P., Moskowitz, R., and J. Melen, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)", [RFC 7402](#), DOI 10.17487/RFC7402, April 2015, <<http://www.rfc-editor.org/info/rfc7402>>.

10.2. Informative References

[I-D.ietf-hip-dex]

Moskowitz, R. and R. Hummen, "HIP Diet EXchange (DEX)", [draft-ietf-hip-dex-05](#) (work in progress), February 2017.

[I-D.moskowitz-hierarchical-hip]

Moskowitz, R. and X. Xu, "Hierarchical HITs for HIPv2", [draft-moskowitz-hierarchical-hip-03](#) (work in progress), June 2017.

[I-D.moskowitz-sse]

Moskowitz, R., Faynberg, I., Lu, H., Hares, S., and P. Giacomin, "Session Security Envelope", [draft-moskowitz-sse-05](#) (work in progress), June 2017.

Moskowitz, et al. Expires December 29, 2017 [Page 11]

Internet-Draft SSLS kmp via HIP June 2017

[RFC2394] Pereira, R., "IP Payload Compression Using DEFLATE", [RFC 2394](#), DOI 10.17487/RFC2394, December 1998, <<http://www.rfc-editor.org/info/rfc2394>>.

[RFC2395] Friend, R. and R. Monsour, "IP Payload Compression Using LZS", [RFC 2395](#), DOI 10.17487/RFC2395, December 1998, <<http://www.rfc-editor.org/info/rfc2395>>.

[RFC3051] Heath, J. and J. Border, "IP Payload Compression Using ITU-T V.44 Packet Method", [RFC 3051](#), DOI 10.17487/RFC3051, January 2001, <<http://www.rfc-editor.org/info/rfc3051>>.

[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>>.

[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>>.

[RFC4493] Song, JH., Poovendran, R., Lee, J., and T. Iwata, "The AES-CMAC Algorithm", [RFC 4493](#), DOI 10.17487/RFC4493, June 2006, <<http://www.rfc-editor.org/info/rfc4493>>.

- [RFC4494] Song, JH., Poovendran, R., and J. Lee, "The AES-CMAC-96 Algorithm and Its Use with IPsec", [RFC 4494](#), DOI 10.17487/RFC4494, June 2006, <<http://www.rfc-editor.org/info/rfc4494>>.
- [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>>.
- [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>>.
- [RFC8004] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", [RFC 8004](#), DOI 10.17487/RFC8004, October 2016, <<http://www.rfc-editor.org/info/rfc8004>>.

Moskowitz, et al.

Expires December 29, 2017

[Page 12]

Internet-Draft

SSLS kmp via HIP

June 2017

- [RFC8046] Henderson, T., Ed., Vogt, C., and J. Arkko, "Host Mobility with the Host Identity Protocol", [RFC 8046](#), DOI 10.17487/RFC8046, February 2017, <<http://www.rfc-editor.org/info/rfc8046>>.

Authors' Addresses

Robert Moskowitz
Huawei
Oak Park, MI 48237

Email: rgm@labs.htt-consult.com

Liang Xia
Huawei
No. 101, Software Avenue, Yuhuatai District
Nanjing

China

Email: Frank.xialiang@huawei.com

Igor Faynberg
Stargazers Consulting, LLC
East Brunswick, NJ 08816
USA

Email: igorfaynberg@gmail.com

Susan Hares
Hickory Hill Consulting
7453 Hickory Hill
Saline, MI 48176
USA

Email: shares@ndzh.com

Pierpaolo Giacomini
FreeLance

Email: yrz@anche.no