

SSE BOF
Internet-Draft
Intended status: Standards Track
Expires: January 4, 2018

R. Moskowitz
Huawei
S. Hares
Hickory Hill Consulting
L. Xia
Huawei
July 3, 2017

Secure Session Layer Services KMP via HIP
draft-moskowitz-ssls-iot-00

Abstract

This memo addresses the need for secure, end-to-end communications from IoT devices to collectors, where the IoT devices may be too resource constrained for typical IETF solutions or may be deployed over non-IP networks (e.g. CAN FD, IEEE 802.15.6, serial SCADA). For such deployments, the Secure Session Layer Service [[draft-hares-ssls-00](#)] the needed, and sufficient features to ensure successful and safe communications.

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 4, 2018.

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

Internet-Draft

SSLS kmp via HIP

July 2017

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.	Minimal feature set	3
4.	IANA Considerations	4
5.	Security Considerations	4
6.	Acknowledgments	4
7.	References	4
7.1.	Normative References	4
7.2.	Informative References	5
	Authors' Addresses	5

[1.](#) Introduction

The IETF has a plethora of security solutions targeted at IoT. Yet all too many IoT products are deployed with no or improperly configured security. In particular resource constrained IoT devices and non-IP IoT networks have not been well served in the IETF.

This effort focuses on a minimal-to-have set of security features and related communications functions for these special, yet rather common collection of IoT devices. This effort need not be restricted to these special cases; it will work for any IoT device on any network. The goal is that all are serviced and protected.

A IoT device can be resource constrained by its CPU, memory, and/or power. Any one of these could result in non-applicablity of common secure communications tools. All three together occurs in many devices. The IoT network can be constrained by bandwidth, MTU, and/or high packet loss. An additional set of constraints can be legal; in terms of mandated end-to-end privacy (e.g. HIPPA).

All this points to a need for a constrained solution for constrained

environments.

Internet-Draft

SSLS kmp via HIP

July 2017

[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

TBD

[3.](#) Minimal feature set

Minimal still implies something done. In this case that something is:

Secure communications envelope: The data on the 'wire' must at least have a cryptographic integrity check and optionally content privacy.

Security key management: The keying material for securing the communications envelope must be fresh and unique.

Unique device Identity: The device must have an Identity that uniquely identifies it in a trusted manner.

Minimal means the least amount of tools and one for each function, with perhaps one for many functions. Much of this is standard, but later will be shown how to minimize its size and performance impact.

ECC for Identity: An Elliptic Curve public key can be the base of the

Identity.

ECC key management: ECC can be 'reused' for the key management protocol.

Symmetric cryptography for message protection: Four functions are needed: privacy, integrity, hashing, randomness.

Message management: Three functions are needed: data chunking, message fragmentation/reassembly, and receipt acknowledgment. Data compression is an optional fourth function.

Moskowitz, et al.

Expires January 4, 2018

[Page 3]

Internet-Draft

SSLS kmp via HIP

July 2017

ECC has been perceived as still too much. It does set a barrier of an 8-bit CPU, time and memory. ECDH based on ECC25519 [[RFC7748](#)] has been implemented on 8-bit CPUs, running 9 seconds.

HIP DEX [[I-D.ietf-hip-dex](#)] is a minimalist KMP and defined for application use in [[I-D.moskowitz-ssls-hip](#)].

The Secure Session Layer Services (SSLS) [[draft-hares-ssls-00](#)] 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

[4.](#) IANA Considerations

TBD. May be nothing for IANA.

[5.](#) Security Considerations

TBD.

[6.](#) Acknowledgments

[7.](#) References

[7.1.](#) 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>>.

Moskowitz, et al.

Expires January 4, 2018

[Page 4]

Internet-Draft

SSLS kmp via HIP

July 2017

- [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>>.

[7.2.](#) 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-ssls-hip]
Moskowitz, R., Xia, L., Faynberg, I., Hares, S., and P. Giacomin, "Secure Session Layer Services KMP via HIP", [draft-moskowitz-ssls-hip-02](#) (work in progress), June 2017.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", [RFC 7748](https://www.rfc-editor.org/info/rfc7748), DOI 10.17487/RFC7748, January 2016, <<http://www.rfc-editor.org/info/rfc7748>>.

Authors' Addresses

Robert Moskowitz
Huawei
Oak Park, MI 48237

Email: rgm@labs.htt-consult.com

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

Email: shares@ndzh.com

Moskowitz, et al.

Expires January 4, 2018

[Page 5]

Internet-Draft

SSLS kmp via HIP

July 2017

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

Email: Frank.xialiang@huawei.com

