Workgroup: Payload Working Group
Internet-Draft: draft-ietf-avtcore-rtp-scip-04
Published: 17 November 2022
Intended Status: Standards Track
Expires: 21 May 2023
Authors: D. Hanson
General Dynamics Mission Systems, Inc.
M. Faller
General Dynamics Mission Systems, Inc.
K. Maver
General Dynamics Mission Systems, Inc.

RTP Payload Format for the Secure Communication Interoperability Protocol (SCIP) Codec

Abstract

This document describes the RTP payload format of the Secure Communication Interoperability Protocol (SCIP). SCIP is an application layer protocol that defines the establishment of reliable secure end-to-end communications, including capabilities exchange with secure session establishment parameters such as codec selection, encryption algorithms, security levels, and cryptographic initialization values. This document defines the Session Description Protocol (SDP) and RTP parameters needed to support SCIP over RTP.

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 https://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 21 May 2023.

(https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

This document details usage of the "audio/scip" and "video/scip" pseudo-codecs [AUDIOSCIP], [VIDEOSCIP] as a secure session establishment protocol and media transport protocol over RTP. It details how encrypted audio and video codec payloads are transported in RTP packets. It provides a reference for network security policymakers, network equipment OEMs, procurement personnel, and government agency and commercial industry representatives. Note that the IP network layer does not implement SCIP as a protocol since SCIP operates at the application layer in endpoints. However, the IP network layer should enable SCIP traffic to transparently pass through the network.

SCIP is presently implemented in United States and NATO secure voice, video, and data products operating on commercial, private, and tactical IP networks worldwide using the scip media subtype.

1.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Best current practices for writing an RTP payload format specification were followed [RFC2736] [RFC8088].

When referring to the Secure Communication Interoperability Protocol, the uppercase acronym "SCIP" is used. When referring to the media subtype scip, lowercase "scip" is used.

1.2. Abbreviations

The following abbreviations are used in this document.

AVP: Audio/Video Profile
DTX: Discontinuous Transmission
ICWG: Interoperability Control Working Group
IICWG: International Interoperability Control Working Group
NATO: North Atlantic Treaty Organization
SCIP: Secure Communication Interoperability Protocol
SDP: Session Description Protocol

2. Background

The Secure Communication Interoperability Protocol (SCIP) allows the negotiation of several voice, data, and video applications using various encryption suites. SCIP also provides several important characteristics that have led to its broad acceptance in the international user community. These features include end-to-end security at the application layer, authentication of user identity, the ability to apply different security levels for each secure session, and secure communication over any end-to-end data connection.

SCIP began in the United States as the Future Narrowband Digital Terminal (FNBDT) Protocol. A combined Department of Defense and vendor consortium formed a governing organization named the Interoperability Control Working Group (ICWG) to manage the protocol. In time, the group expanded to include NATO, NATO partners and European vendors under the name International Interoperability Control Working Group (IICWG), which was later renamed the SCIP Working Group.

First generation SCIP devices operated on circuit-switched networks. SCIP was then expanded to radio and IP networks. The scip media

subtype transports SCIP secure session establishment signaling and secure application traffic. The built-in negotiation and flexibility provided by the SCIP standards make it a natural choice for many scenarios that require various secure applications and associated encryption suites. SCIP has been endorsed by many NATO nations as the secure end-to-end solution for secure voice, video, and data devices. SCIP standards are currently available to participating government/ military communities and select OEMs of equipment that support SCIP.

However, SCIP must operate over global networks (including private and commercial networks). Without access to necessary information to support SCIP, some networks may not support the SCIP media subtypes. Issues may occur simply because information is not as readily available to OEMs, network administrators, and network architects.

This RFC provides essential information about audio/scip and video/ scip media subtypes that enables network equipment manufacturers to include "scip" as a known audio and video media subtype in their equipment and enables network administrators to define and implement a compatible security policy.

All current IP-based SCIP devices support "scip" as a media subtype. Registration of scip as a media subtype provides a common reference for network equipment manufacturers to recognize SCIP in a payload declaration.

3. Media Format Description

The "scip" media subtype indicates support for and identifies SCIP traffic that is being transferred using RTP. Transcoding, lossy compression, or other data modifications MUST NOT be performed on the SCIP RTP payload. The audio/scip and video/scip media subtype data streams within the network, including the VoIP network, MUST be a transparent relay and be treated as "clear-channel data", similar to the Clearmode media subtype defined by [RFC4040]. However, Clearmode is defined as a gateway protocol and is limited to a sample rate of 8000 Hz and 64 kbps bandwidth only. Clearmode is not defined for the higher sample and data rates required for some SCIP traffic.

4. Payload Format

The RTP Packet content of SCIP traffic is dependent upon the SCIP session state. SCIP secure session establishment uses protocols defined in SCIP-210 [SCIP210] to negotiate an application. SCIP secure traffic may consist of the encrypted output of codecs such as MELPe [RFC8130], G.729D [RFC3551], H.264 [RFC6184] based on the application negotiated during SCIP secure session establishment. SCIP traffic is highly variable and the bit rate specified in the SDP [RFC8866] is OPTIONAL since discontinuous transmission (DTX) or other

mechanisms may be used. The SCIP payload size will vary considerably, especially during SCIP secure session establishment.

The SCIP codec produces an encrypted bitstream that is transported over RTP. Unlike other codecs, SCIP does not have its own upper layer syntax (e.g., no Network Adaptation Layer (NAL) units), but rather secures the output of the codecs that it uses (e.g., G.729D, H.264, etc.). SCIP achieves this by encapsulating the encrypted codec output that has been previously formatted according to the relevant RTP payload specification (e.g., RFC 6184 for H.264).

4.1. RTP Header Fields

The SCIP RTP header fields SHALL conform to RFC 3550.

SCIP traffic may be continuous or discontinuous. The Timestamp field MUST increment based on the sampling clock for discontinuous transmission as described in [RFC3550], Section 5.1. The Timestamp field for continuous transmission applications is dependent on the sampling rate of the media as specified in the media subtype's specification (e.g., MELPe [RFC8130]). Note that during a SCIP session, both discontinuous and continuous traffic are highly probable. Therefore, a jitter buffer MAY be implemented in endpoint devices only but SHOULD NOT be implemented in network devices. Additionally, network devices SHOULD NOT repacketize SCIP packets.

The Marker bit SHALL be set to zero for discontinuous traffic. The Marker bit for continuous traffic is based on the underlying media subtype specification. The underlying media is opaque within SCIP RTP packets.

5. Payload Format Parameters

The SCIP RTP payload format is identified using the scip media subtype, which is registered in accordance with [RFC4855] and per the media type registration template form [RFC6838]. A clock rate of 8000 Hz SHALL be used for "audio/scip". A clock rate of 90000 Hz SHALL be used for "video/scip".

5.1. Media Subtype "audio/scip"

Media type name: audio

Media subtype name: scip

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: Binary. This media subtype is only defined for transfer via RTP. There SHALL be no encoding/decoding (transcoding) of the audio stream as it traverses the network.

Security considerations: See Section 6.

Interoperability considerations: N/A

Published specifications: [SCIP210]

Applications which use this media: N/A

Fragment Identifier considerations: none

Restrictions on usage: N/A

Additional information:

1. Deprecated alias names for this type: N/A

2. Magic number(s): N/A

3. File extension(s): N/A

4. Macintosh file type code: N/A

5. Object Identifiers: N/A

Person to contact for further information:

1. Name: Michael Faller and Daniel Hanson

2. Email: michael.faller@gd-ms.com and dan.hanson@gd-ms.com

Intended usage: Common, Government and Military

Authors:

Michael Faller - michael.faller@gd-ms.com

Daniel Hanson - dan.hanson@gd-ms.com

Change controller:

SCIP Working Group - ncia.cis3@ncia.nato.int

5.2. Media Subtype "video/scip"

Media type name: video

Media subtype name: scip

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: Binary. This media subtype is only defined for transfer via RTP. There SHALL be no encoding/decoding (transcoding) of the video stream as it traverses the network.

Security considerations: See Section 6.

Interoperability considerations: N/A

Published specifications: [SCIP210]

Applications which use this media: N/A

Fragment Identifier considerations: none

Restrictions on usage: N/A

Additional information:

1. Deprecated alias names for this type: N/A

2. Magic number(s): N/A

3. File extension(s): N/A

4. Macintosh file type code: N/A

5. Object Identifiers: N/A

Person to contact for further information:

1. Name: Michael Faller and Daniel Hanson

2. Email: michael.faller@gd-ms.com and dan.hanson@gd-ms.com

Intended usage: Common, Government and Military

Authors:

Michael Faller - michael.faller@gd-ms.com

Daniel Hanson - dan.hanson@gd-ms.com

Change controller:

SCIP Working Group - ncia.cis3@ncia.nato.int

5.3. Mapping to SDP

The mapping of the above defined payload format media subtype and its parameters SHALL be implemented according to Section 3 of [RFC4855].

Since SCIP includes its own facilities for capabilities exchange, it is only necessary to negotiate the use of SCIP within SDP Offer/ Answer; the specific codecs to be encapsulated within SCIP are then negotiated via the exchange of SCIP messages.

The information carried in the media type specification has a specific mapping to fields in the Session Description Protocol (SDP) [RFC8866], which is commonly used to describe RTP sessions. When SDP is used to specify sessions employing the SCIP codec, the mapping is as follows:

- The media type ("audio") goes in SDP "m=" as the media name for audio/scip, and the media type ("video") goes in SDP "m=" as the media name for video/scip.

- The media subtype ("scip") goes in SDP "a=rtpmap" as the encoding name. The required parameter "rate" also goes in "a=rtpmap" as the clock rate.

- The optional parameters "ptime" and "maxptime" go in the SDP "a=ptime" and "a=maxptime" attributes, respectively.

An example mapping for audio/scip is:

```
m=audio 50000 RTP/AVP 96
a=rtpmap:96 scip/8000
```

An example mapping for video/scip is:

```
m=video 50002 RTP/AVP 97
a=rtpmap:97 scip/90000
```

An example mapping for both audio/scip and video/scip is:

```
m=audio 50000 RTP/AVP 96
a=rtpmap:96 scip/8000
m=video 50002 RTP/AVP 97
a=rtpmap:97 scip/90000
```

The application negotiation between endpoints will determine whether the audio and video streams are transported as separate streams over the audio and video payload types or as a single media stream on the video payload type.

5.4. SDP Offer/Answer Considerations

In accordance with the SDP Offer/Answer model [RFC3264], the SCIP device SHALL list the SCIP payload type number in order of preference in the "m" media line.

6. Security Considerations

RTP packets using the payload format defined in this specification are subject to the security considerations discussed in the RTP specification [RFC3550], and in any applicable RTP profile such as RTP/AVP [RFC3551], RTP/AVPF [RFC4585], RTP/SAVP [RFC3711], or RTP/SAVPF [RFC5124]. However, as "Securing the RTP Protocol Framework: Why RTP Does Not Mandate a Single Media Security Solution" [RFC7202] discusses, it is not an RTP payload format's responsibility to discuss or mandate what solutions are used to meet the basic security goals like confidentiality, integrity, and source authenticity for RTP in general. This responsibility lays on anyone using RTP in an application. They can find guidance on available security mechanisms and important considerations in "Options for Securing RTP Sessions" [RFC7201]. Applications SHOULD use one or more appropriate strong security mechanisms. The rest of this Security Considerations section discusses the security impacting properties of the payload format itself.

This RTP payload format and its media decoder do not exhibit any significant non-uniformity in the receiver-side computational complexity for packet processing, and thus do not inherently pose a denial-of-service threat due to the receipt of pathological data. Nor does the RTP payload format contain any active content.

7. IANA Considerations

The audio/scip and video/scip media subtypes have previously been registered with IANA [AUDIOSCIP] [VIDEOSCIP]. IANA should update [AUDIOSCIP] and [VIDEOSCIP] to reference this document upon publication.

8. Change Controller Address

SCIP Working Group, CIS3 Partnership
NATO Communications and Information Agency
Oude Waalsdorperweg 61, 2597AK
The Hague, The Netherlands
Email: ncia.cis3@ncia.nato.int

9. References

9.1. Normative References

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

[RFC2736] Handley, M. and C. Perkins, "Guidelines for Writers of RTP Payload Format Specifications", BCP 36, RFC 2736, DOI 10.17487/RFC2736, December 1999, <https://www.rfc-editor.org/info/rfc2736>.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, DOI 10.17487/RFC3264, June 2002, <https://www.rfc-editor.org/info/rfc3264>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550, July 2003, <https://www.rfc-editor.org/info/rfc3550>.

[RFC3551] Schulzrinne, H. and S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control", STD 65, RFC 3551, DOI 10.17487/RFC3551, July 2003, <https://www.rfc-editor.org/info/rfc3551>.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, DOI 10.17487/RFC3711, March 2004, <https://www.rfc-editor.org/info/rfc3711>.

[RFC4585] Ott, J., Wenger, S., Sato, N., Burmeister, C., and J. Rey, "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)", RFC 4585, DOI 10.17487/RFC4585, July 2006, <https://www.rfc-editor.org/info/rfc4585>.

[RFC5124] Ott, J. and E. Carrara, "Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF)", RFC 5124, DOI 10.17487/RFC5124, February 2008, <https://www.rfc-editor.org/info/rfc5124>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8866] Begen, A., Kyzivat, P., Perkins, C., and M. Handley, "SDP: Session Description Protocol", RFC 8866, DOI 10.17487/RFC8866, January 2021, <https://www.rfc-editor.org/info/rfc8866>.

9.2. Informative References

[AUDIOSCIP] Faller, M. and D. Hanson, "audio/scip: Internet Assigned Numbers Authority (IANA)", 28 January 2021, <https://www.iana.org/assignments/media-types/audio/scip>.

[RFC4040] Kreuter, R., "RTP Payload Format for a 64 kbit/s Transparent Call", RFC 4040, DOI 10.17487/RFC4040, April 2005, <https://www.rfc-editor.org/info/rfc4040>.

[RFC4855] Casner, S., "Media Type Registration of RTP Payload Formats", RFC 4855, DOI 10.17487/RFC4855, February 2007, <https://www.rfc-editor.org/info/rfc4855>.

[RFC6184] Wang, Y.-K., Even, R., Kristensen, T., and R. Jesup, "RTP Payload Format for H.264 Video", RFC 6184, DOI 10.17487/RFC6184, May 2011, <https://www.rfc-editor.org/info/rfc6184>.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <https://www.rfc-editor.org/info/rfc6838>.

[RFC7201] Westerlund, M. and C. Perkins, "Options for Securing RTP Sessions", RFC 7201, DOI 10.17487/RFC7201, April 2014, <https://www.rfc-editor.org/info/rfc7201>.

[RFC7202] Perkins, C. and M. Westerlund, "Securing the RTP Framework: Why RTP Does Not Mandate a Single Media Security Solution", RFC 7202, DOI 10.17487/RFC7202, April 2014, <https://www.rfc-editor.org/info/rfc7202>.

[RFC8088] Westerlund, M., "How to Write an RTP Payload Format", RFC 8088, DOI 10.17487/RFC8088, May 2017, <https://www.rfc-editor.org/info/rfc8088>.

[RFC8130] Demjanenko, V. and D. Satterlee, "RTP Payload Format for the Mixed Excitation Linear Prediction Enhanced (MELPe) Codec", RFC 8130, DOI 10.17487/RFC8130, March 2017, <https://www.rfc-editor.org/info/rfc8130>.

[SCIP210] SCIP Working Group, "SCIP Signaling Plan", SCIP-210, r3.10, October 2017.

[VIDEOSCIP] Faller, M. and D. Hanson, "video/scip: Internet Assigned Numbers Authority (IANA)", 28 January 2021, <https://www.iana.org/assignments/media-types/video/scip>.

Authors' Addresses

Daniel Hanson
General Dynamics Mission Systems, Inc.
150 Rustcraft Road
Dedham, MA 02026
United States of America

Email: dan.hanson@gd-ms.com

Michael Faller
General Dynamics Mission Systems, Inc.
150 Rustcraft Road
Dedham, MA 02026
United States of America

Email: michael.faller@gd-ms.com

Keith Maver
General Dynamics Mission Systems, Inc.
150 Rustcraft Road
Dedham, MA 02026
United States of America

Email: keith.maver@gd-ms.com