The Stream Control Transmission Protocol (SCTP) as a Transport for the Diameter Protocol
draft-pascual-dime-sctp-00

Abstract

This document provides the guidelines for usage of SCTP (the Stream Control Transmission Protocol) as the transport mechanism between Diameter entities.

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 May 11, 2011.

Copyright Notice

Copyright (c) 2010 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 ................................................. 3
2. Terminology .................................................. 3
3. SCTP Usage ..................................................... 3
   3.1. Payload Protocol Identifier ............................... 3
   3.2. Mapping of Diameter messages into SCTP Streams .......... 3
   3.3. Port Number ............................................... 4
   3.4. S-NAPTR Parameters ...................................... 4
4. TLS over SCTP Usage ........................................... 4
5. DTLS over SCTP Usage .......................................... 4
   5.1. Payload Protocol Identifier ............................... 4
   5.2. Mapping of Diameter messages into SCTP Streams .......... 5
   5.3. Port Number ............................................... 5
   5.4. S-NAPTR Parameters ...................................... 5
6. SCTP over IPsec Usage ......................................... 5
7. Security Considerations ...................................... 6
8. IANA Considerations .......................................... 6
9. Acknowledgements ............................................ 6
10. References ................................................... 6
    10.1. Normative References ................................... 6
    10.2. Informative References .................................. 6
Appendix A. Change Log ........................................... 7
1. Introduction

The Diameter base protocol [RFC3588] is intended to provide an Authentication, Authorization and Accounting (AAA) framework for applications such as network access or IP mobility in both local and roaming situations. Among other aspects, [RFC3588] specifies the transport service used by all Diameter applications. [draft-ietf-dime-rfc3588bis] (work in progress) aims to obsolete this specification.

Diameter messages are either requests or answers and are sent over a reliable transport that offers congestion control; hence in [draft-ietf-dime-rfc3588bis] the base Diameter protocol is defined to run over TCP [RFC793], SCTP [RFC4960] or TLS [RFC5246], assuming that TLS is run on top of TCP when it is used. According to the same document, the use of a secured transport for exchanging Diameter messages is mandatory being TLS the primary method and IPsec a secondary alternative. However, TLS over SCTP [RFC3436] has some serious limitations.

This document updates [draft-ietf-dime-rfc3588bis] by specifying the usage of Diameter over SCTP and its associated security mechanisms.

2. Terminology

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

The other concepts and terminology used in this document are compatible with [draft-ietf-dime-rfc3588bis], [draft-ietf-tsvwg-dtls-for-sctp], [RFC3436], [RFC3554] and [RFC4960].

3. SCTP Usage

3.1. Payload Protocol Identifier

No SCTP identifier needs to be defined for Diameter messages. Therefore, the Payload Protocol Identifier in SCTP DATA chunks transporting Diameter messages MUST be set to zero. [Editor’s note: However, for protocol analyzers it is much easier if a specific PPID is used.]

3.2. Mapping of Diameter messages into SCTP Streams

Diameter messages need to be mapped into SCTP streams in a way that avoids Head Of the Line (HOL) blocking. Among the different ways of
performing this mapping that fulfill this requirement, the simplest alternative is proposed; a Diameter entity SHOULD send every Diameter message (request or response) over stream zero with the unordered flag set. On the receiving side, a Diameter entity MUST be ready to receive Diameter messages over any stream.

Although both sides of the SCTP association SHOULD use stream 0 for Diameter requests and responses if they follow this recommendation, if a Diameter request arrives over a particular stream, the server is free to return responses over a different stream. This way, both sides manage the available streams in the sending direction, independently of the streams chosen by the other side to send a particular Diameter message. This avoids undesirable collisions when seizing a particular stream.

3.3. Port Number

The IANA has assigned port number 3868 for SCTP.

3.4. S-NAPTR Parameters

[draft-ietf-dime-rfc3588bis] registers a S-NAPTR Application Service Tag value of "aaa". Additionally, it also registers the S-NAPTR Application Protocol Tag for SCTP: diameter.sctp

4. TLS over SCTP Usage

As exposed in [draft-ietf-tsvwg-dtls-for-sctp], TLS over SCTP [RFC3436] has some serious limitations. In order to overcome these limitations, Diameter over DTLS/SCTP [draft-ietf-tsvwg-dtls-for-sctp] is proposed as an alternative to TLS/SCTP.

5. DTLS over SCTP Usage

DTLS over SCTP is described in [draft-ietf-tsvwg-dtls-for-sctp] and overcomes the limitations of TLS over SCTP.

The IESG has recently approved DTLS over SCTP as a Proposed Standard and it will be published as a Standards Track RFC. SCTP over IPSec is the RECOMMENDED solution for securing Diameter messages until DTLS/SCTP gets widely adopted by the industry.

5.1. Payload Protocol Identifier

No SCTP identifier needs to be defined for Diameter messages over DTLS. Therefore, the Payload Protocol Identifier in SCTP DATA chunks transporting DTLS-based Diameter messages MUST be set to zero.

[Editor's note: However, for protocol analyzers it is much easier if
5.2. Mapping of Diameter messages into SCTP Streams

Diameter messages need to be mapped into SCTP streams in a way that avoids Head Of the Line (HOL) blocking. Among the different ways of performing this mapping that fulfill this requirement, the simplest alternative is proposed; a Diameter entity SHOULD send every Diameter message (request or response) over stream zero with the unordered flag set. On the receiving side, a Diameter entity MUST be ready to receive Diameter messages over any stream.

Although both sides of the SCTP association SHOULD use stream 0 for Diameter requests and responses if they follow this recommendation, if a Diameter request arrives over a particular stream, the server is free to return responses over a different stream. This way, both sides manage the available streams in the sending direction, independently of the streams chosen by the other side to send a particular Diameter message. This avoids undesirable collisions when seizing a particular stream.

5.3. Port Number

The port number [TBD] has been assigned for DTLS/SCTP.

5.4. S-NAPTR Parameters

[draft-ietf-dime-rfc3588bis] registers a S-NAPTR Application Service Tag value of "aaa". The present document registers the S-NAPTR Application Protocol Tag for DTLS/SCTP: diameter.dtls.sctp

6. SCTP over IPsec Usage

When Diameter is used over SCTP over IPsec, two modes are possible. The straightforward way is to create an association and Security Policy Database (SPD) selector for each SCTP IP Address and port involved in an association, treating SCTP as any other layer above IP, and thus potentially creating multiple entries for a single SCTP association. Implementations MUST at least support this straightforward mode, if they support this document and Diameter over SCTP over IPsec.

Alternatively, implementations MAY also support [RFC3554] which provides a minor optimization to reduce the number of IPsec associations/selectors for SCTP connections. Note that [RFC3554] creates a new IKE ID for this purpose. Generally such an optimization is unnecessary for Diameter applications, both because of the relatively low number of Diameter connections per system, and
because one of the main advantages of SCTP is multi-homing across interfaces which makes [RFC3554] potentially impossible to implement.

7. Security Considerations

TBD

8. IANA Considerations

TBD

9. Acknowledgements

The authors wish to thank Hadriel Kaplan (Acme Packet), Juan Luis Esteban (Acme Packet) and Michael Tuexen (Muenster Univ. of Applied Sciences) for their contributions to this work.

10. References

10.1. Normative References


10.2. Informative References


Appendix A. Change Log

New Document

Authors' Addresses

V. Pascual
Acme Packet
Anabel Segura 10
Madrid 28108
Spain

EMail: VPascual@acmepacket.com

G. Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: Gonzalo.Camarillo@ericsson.com