

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: January 5, 2013

G. Zorn  
Network Zen  
Q. Wu  
Huawei  
July 4, 2012

A Lightweight Approach to Node-to-Node Security in Diameter  
draft-zorn-dime-n2n-sec-lite-03

## Abstract

This document describes a lightweight method for cryptographically protecting a portion of the contents of a Diameter message in transit between an arbitrary pair of Diameter nodes. The scheme assumes that the destination node possesses an X.509 certificate containing an RSA public key and that that certificate is retrievable through a DNS query by the node originating the message.

In addition to describing the operation of the protocol, this note specifies an Attribute-Value Pair (AVP) for the encapsulation of encrypted AVPs.

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#). This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

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 5, 2013.

## Copyright Notice

Copyright (c) 2012 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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Protocol Operation . . . . .	<a href="#">3</a>
<a href="#">3.1.</a>	Client Operation . . . . .	<a href="#">3</a>
<a href="#">3.1.1.</a>	Key Establishment . . . . .	<a href="#">3</a>
<a href="#">3.1.2.</a>	Protected Data Transfer . . . . .	<a href="#">3</a>
<a href="#">3.2.</a>	Server Operation . . . . .	<a href="#">3</a>
<a href="#">3.2.1.</a>	Key Establishment . . . . .	<a href="#">3</a>
<a href="#">3.2.2.</a>	Protected Data Transfer . . . . .	<a href="#">4</a>
<a href="#">4.</a>	Attribute-Value Pair Definitions . . . . .	<a href="#">4</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">4</a>
<a href="#">7.</a>	References . . . . .	<a href="#">4</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">4</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">5</a>
	Authors' Addresses . . . . .	<a href="#">5</a>

## [1.](#) Introduction

Historically, Authentication, Authorization and Accounting (AAA) network traffic has been secured on a hop-by-hop basis: messages between AAA entities (such as Diameter clients, agents and servers) have been protected on the wire but those entities have had unfettered access to the message contents. This has not typically been considered to be a concern when all of the entities in question were within the same sphere of administrative control, but may be problematic if the messages pass through an outside system (for example, an agent residing in an intermediate domain in a roaming situation). This document describes a lightweight method for cryptographically protecting a portion of the contents of a Diameter message while in transit between an arbitrary pair of Diameter nodes.

## [2.](#) 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](#)].

## [3.](#) Protocol Operation

The following sections describe the operation of the proposed end-to-end security scheme. Although key establishment and data transfer are discussed separately, both will usually take place in the same message.

### [3.1.](#) Client Operation

#### [3.1.1.](#) Key Establishment

TBC.

### [3.1.2.](#) Protected Data Transfer

TBC.

## [3.2.](#) Server Operation

### [3.2.1.](#) Key Establishment

TBC.

Zorn & Wu

Expires January 5, 2013

[Page 3]

---

Internet-Draft

Node-to-Node Security in Diameter

July 2012

### [3.2.2.](#) Protected Data Transfer

TBC.

## [4.](#) Attribute-Value Pair Definitions

This section defines a container AVP for the transport of encrypted AVPs in Diameter applications.

## [5.](#) Security Considerations

The security considerations applicable to the Diameter Base Protocol [[RFC3588](#)] are also applicable to this document.

## [6.](#) IANA Considerations

TBC.

## [7.](#) References

### [7.1.](#) Normative References

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

- [RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", [RFC 3588](#), September 2003.
- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", [RFC 3748](#), June 2004.
- [RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", [RFC 4072](#), August 2005.
- [RFC4398] Josefsson, S., "Storing Certificates in the Domain Name System (DNS)", [RFC 4398](#), March 2006.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 5226](#), May 2008.

## [7.2.](#) Informative References

- [I-D.ietf-smime-cms-rsa-kem]  
Brainard, J., Turner, S., Randall, J., and B. Kaliski,  
"Use of the RSA-KEM Key Transport Algorithm in CMS",  
[draft-ietf-smime-cms-rsa-kem-13](#) (work in progress),  
May 2010.
- [RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", [RFC 5216](#), March 2008.
- [RFC5247] Aboba, B., Simon, D., and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework", [RFC 5247](#), August 2008.
- [RFC5295] Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", [RFC 5295](#), August 2008.
- [RFC5296] Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)", [RFC 5296](#), August 2008.

## Authors' Addresses

Glen Zorn  
Network Zen  
227/358 Thanon Sanphawut  
Bang Na, Bangkok 10260  
Thailand

Phone: +66 (0) 87-040-4617  
Email: glenzorn@gmail.com

Qin Wu  
Huawei Technologies Co., Ltd.  
101 Software Avenue, Yuhua District  
Nanjing, Jiangsu 21001  
China

Phone: +86-25-84565892  
Email: sunseawq@huawei.com