

Internet Engineering Task Force  
Internet-Draft  
Intended status: Standards Track  
Expires: July 18, 2015

S. Jiang  
Huawei Technologies Co., Ltd  
D. Zhang  
Alibaba Co., Ltd  
S. Krishnan  
Ericsson  
January 14, 2015

**CGA SEC Option for Secure Neighbor Discovery Protocol**  
**draft-jiang-6man-cga-sec-option-01**

Abstract

A Cryptographically Generated Address is an IPv6 addresses binding with a public/private key pair. It is a vital component of Secure Neighbor Discovery (SeND) protocol. The current SeND specifications are lack of procedures to specify the Sec bits. A new SEC option is defined accordingly to address this issue.

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 July 18, 2015.

Copyright Notice

Copyright (c) 2015 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="#">2</a>
<a href="#">2.</a>	Requirements Language . . . . .	<a href="#">2</a>
<a href="#">3.</a>	CGA SEC Option . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Host Behavior . . . . .	<a href="#">3</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">3</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">3</a>
<a href="#">7.</a>	Acknowledgements . . . . .	<a href="#">4</a>
<a href="#">8.</a>	References . . . . .	<a href="#">4</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">4</a>
<a href="#">8.2.</a>	Informative References . . . . .	<a href="#">4</a>
	Authors' Addresses . . . . .	<a href="#">4</a>

## [1.](#) Introduction

Cryptographically Generated Addresses (CGA, [[RFC3972](#)]) are used to make sure that the sender of a Neighbor Discovery message is the "owner" of the claimed address. Although it is not mandatory, it is a vital component of Secure Neighbor Discovery (SeND, [[RFC3971](#)]) protocol. After CGA has been defined, as an independent security property, many other CGA usages have been proposed and defined, such as Enhanced Route Optimization for Mobile IPv6 [[RFC4866](#)], Site Multihoming by IPv6 Intermediation (SHIM6) [[RFC5533](#)], etc.

SEC bits are an important parameter in the generation of CGAs. Particularly, SEC values are used to artificially introduce additional difficulty in the CGA generation process in order to provide additional protection against brute force attacks. Therefore, in different environments, host may be required to use different SEC bits in the generation of their CGAs. However, the base SeND protocol fails to distribute the SEC values to the hosts. As a result, the network administration cannot propagate any requirements regarding to SEC value of host-generated CGA addresses. In order to fill this gap, a new CGA SEC Option, is defined in this document.

## [2.](#) Requirements Language

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 [[RFC2119](#)].



### 3. CGA SEC Option

CGA SEC Option is used to indicate on link hosts the lowest CGA SEC value they SHOULD use. It SHOULD be contained in and only in the Router Advertisement Message [[RFC4861](#)].

```

      0               1               2               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   OPTION_CGA_SEC_OPTION   |   option-len   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   SEC bits   |
+---+---+---+---+---+

```

option-code   OPTION\_CGA\_SEC\_OPTION (TBA1)

option-len   1.

SEC bits   The value of SEC bits is specified in [[RFC3972](#)].

### 4. Host Behavior

On receiving the CGA SEC Option with a recommended SEC value, a host SHOULD use a CGA with the recommended or higher SEC value. If choosing a CGA with a SEC value lower than the recommended, the host MAY take the risk that it is not able to use full network capabilities. The network may consider the hosts that use CGAs with lower SEC values as unsecure users and decline some or all network services.

### 5. Security Considerations

This document extends SeND with a CGA SEC Option to transport SEC bits used in the generation of GCAs, which enables administrators to specify and adjust the security level of the CGAs used in the network. Apart from that, this approach does not introduce any significant changes to the underlying security issues considered in [Section 9 of \[RFC3971\]](#).

### 6. IANA Considerations

This document defines a new Neighbor Discovery Protocol options, which must be assigned an Option Type value within the IPv6 Neighbor Discovery Option Formats table of Internet Control Message Protocol version 6 (ICMPv6) Parameters (<http://www.iana.org/assignments/icmpv6-parameters>):



Type	Description	Reference
TBA1	CGA SEC option	This document

## 7. Acknowledgements

The authors would like to thanks the valuable comments made by members of 6man WG.

This document was produced using the xml2rfc tool [[RFC2629](#)].

## 8. References

### 8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.
- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.

### 8.2. Informative References

- [RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", [RFC 2629](#), June 1999.
- [RFC4866] Arkko, J., Vogt, C., and W. Haddad, "Enhanced Route Optimization for Mobile IPv6", [RFC 4866](#), May 2007.
- [RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", [RFC 5533](#), June 2009.

## Authors' Addresses

Sheng Jiang  
Huawei Technologies Co., Ltd  
Q14, Huawei Campus, No.156 Beiqing Road  
Hai-Dian District, Beijing, 100095  
P.R. China

Email: [jiangsheng@huawei.com](mailto:jiangsheng@huawei.com)



Dacheng Zhang  
Alibaba Co., Ltd  
9th Floor, A Area, Wentelai World Finance Centre, 1 West Dawang Road  
Chaoyang District, Beijing, 100095 100025  
P.R. China

Email: dacheng.zdc@alibaba-inc.com

Suresh Krishnan  
Ericsson  
8400 Decarie Blvd.  
Town of Mount Royal, QC  
Canada

Phone: +1 514 345 7900 x42871  
Email: suresh.krishnan@ericsson.com



