Network Working Group
Request for Comments: 4581
Updates: 3972
Category: Standards Track

M. Bagnulo
UC3M
J. Arkko
Ericsson

October 2006

Cryptographically Generated Addresses (CGA) Extension Field Format

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document defines a Type-Length-Value format for Cryptographically Generated Address (CGA) Extensions. This document updates RFC 3972.

Table of Contents

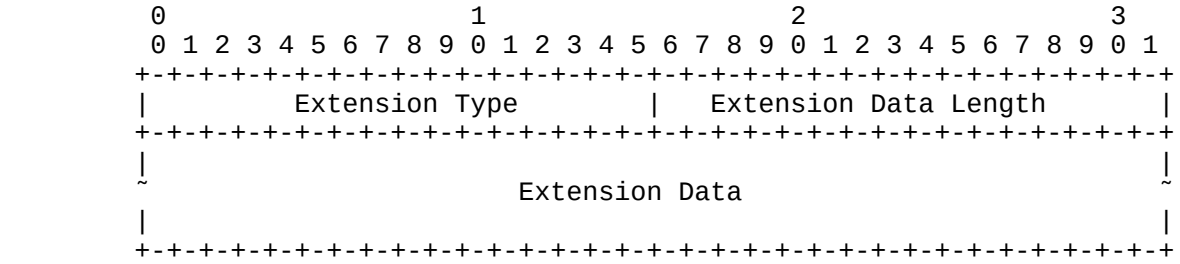
1. Introduction 2
2. CGA Extension Field Format 2
3. IANA Considerations 2
4. Security Considerations 3
5. Acknowledgements 3
6. Normative References 3

1. Introduction

The Cryptographically Generated Address (CGA) specification [1] defines Extension Fields that allow additional information to be included in the CGA Parameter Data Structure. So far there seems to be enough interest in including additional data items into the CGA Parameter Data Structure through these Extension Fields that it seems reasonable to expect that more than one mechanism will require its usage. In order to simplify the addition of multiple data items, this document updates RFC 3972 [1], and it defines a Type-Length-Value format for the Extension Fields.

2. CGA Extension Field Format

Data items to be included in Extension Fields of the CGA Parameter Data Structure MUST be encoded using the following Type-Length-Value (TLV) format:



Extension Type: 16-bit identifier of the type of the Extension Field.

Extension Data Length: 16-bit unsigned integer. Length of the Extension Data field of this option, in octets.

Extension Data: Variable-length field. Extension-Type-specific data.

3. IANA Considerations

The IANA has created and will maintain a registry entitled, "CGA Extension Type". The values in this name space are 16-bit unsigned integers. Initial values for the CGA Extension Type field are given below; future assignments are to be made through Standards Action [2]. Assignments consist of a name and the value.

As recommended in [3], this document makes the following assignments for experimental and testing use: the value 0xFFFD, with name Exp_FFFD; the value 0xFFFE, with name Exp_FFFE, and the value 0xFFFF, with name Exp_FFFF.

4. Security Considerations

No security concerns are raised by the adoption of the CGA Extension format described in this document. However, proper security analysis is required when new CGA Extensions are defined in order to make sure that they introduce no new vulnerabilities to the existing CGA schemes.

5. Acknowledgements

Comments to this document were provided by Sam Hartman, Allison Mankin, Pekka Savola, Thomas Narten, Tuomas Aura, Stefan Rommer, Julien Laganier, and James Kempf.

6. Normative References

[1] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[2] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[3] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", BCP 82, RFC 3692, January 2004.

Authors' Addresses

Marcelo Bagnulo
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
SPAIN

Phone: 34 91 6249500
EMail: marcelo@it.uc3m.es
URI: http://www.it.uc3m.es

Jari Arkko
Ericsson
Jorvas 02420
Finland

EMail: jari.arkko@ericsson.com

Full Copyright Statement

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).