

An IPv6 Prefix for Cryptographically Generated IDs
draft-dupont-ipv6-cgpref-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 25, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document proposes the allocation of a dedicated prefix for Cryptographically Generated IDs (CGIDs). This prefix makes the distinction between a CGID and a real IPv6 global address trivial.

1. Introduction

Some ideas floating at the IETF are about Cryptographically Generated IDs which provide intrinsic proofs of ownership. Cryptographically Generated Addresses [[RFC3972](#)] are an example but this document

addresses some needs for CGIDs using the global unicast IPv6 address format [[RFC3587](#)].

If all CGIDs use a dedicated prefix, marked as not routable, then the distinction between a CGID and a real global unicast IPv6 address will be instantaneous. With such a prefix on n bits, a CGID will be the concatenation of the n bits of the prefix followed by $128 - n$ bits cryptographically generated (i.e., from the result of a hash function applied to parameters, including in many examples a public RSA key).

2. Security Considerations

The generation of a CGID should use a random value, like the CGA modifier, in order to make it unpredictable. A small value of " n " makes collisions statically impossible and direct attacks very hard.

3. IANA Considerations

This document argues in favour of the allocation of a dedicated prefix of 16 to 32 bits in length from the global unicast space. IANA is in charge of allocations in this space [[RFC3513](#)].

4. Acknowledgments

Gabriel Montenegro was the first to present the CGID idea. IANA people helped us to find a reasonable range for the " n " value.

5. References

5.1 Normative References

[RFC3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", [RFC 3513](#), April 2003.

5.2 Informative References

[RFC3587] Hinden, R., Deering, S., and E. Nordmark, "IPv6 Global Unicast Address Format", [RFC 3587](#), August 2003.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.

Author's Address

Francis Dupont (editor)
Point6
c/o GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30

Email: Francis.Dupont@enst-bretagne.fr

Intellectual Property Statement

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.

Disclaimer of Validity

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.

Copyright Statement

Copyright (C) The Internet Society (2005). 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.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

