Network Working Group F. Dupont, Ed.
Internet-Draft Point6
Expires: December 25, 2005 June 23, 2005

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

Status of this Memo

Copyright Notice

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

Disclaimer of Validity

Copyright Statement

Acknowledgment

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