Groupe de travail Réseau
Request for Comments : 4581
RFC mise à jour : 3972
Catégorie : Sur la voie de la normalisation

M. Bagnulo, UC3M
J. Arkko, Ericsson
octobre 2006
Traduction Claude Brière de L'Isle

Format de champ d'extension des adresses générées cryptographiquement (CGA)

Résumé
Le présent document définit un format de Type-Longueur-Valeur pour les extensions d'adresse générée cryptographiquement (CGA, *Cryptographically Generated Address*). Ce document met à jour la RFC 3972.

Table des matières

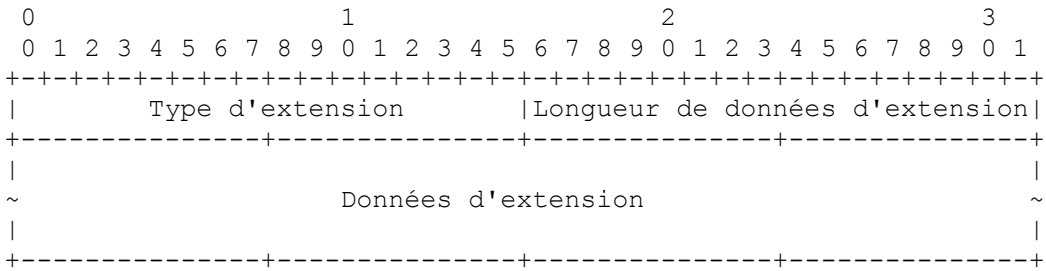
1. Introduction....1
2. Format de champ d'extension CGA....1
3 Considérations relatives à l'IANA....2
4 Considérations sur la sécurité....2
5. Remerciements....2
6. Références normatives....2
Adresse des auteurs....2
Déclaration complète de droits de reproduction....3

1. Introduction

La spécification d'adresse générée cryptographiquement (CGA, *Cryptographically Generated Address*) [RFC3972] définit des champs d'extension qui permettent que des informations supplémentaires soient incluses dans la structure de données de paramètre CGA. Jusqu'à présent il a semblé qu'il y ait suffisamment d'intérêt pour inclure des éléments de données supplémentaires dans la structure de données de paramètre de CGA par ces champs d'extension pour qu'il semble raisonnable de s'attendre à ce que plus d'un mécanisme exige son utilisation. Afin de simplifier l'ajout de plusieurs éléments de données, le présent document met à jour la [RFC3972], et il définit un format de Type-Longueur-Valeur pour les champs d'extension.

2. Format de champ d'extension CGA

Les éléments de données à inclure dans les champs d'extension de la structure de données de paramètre de CGA DOIVENT être codés en utilisant le format de Type-Longueur-Valeur (TLV) suivant :



Type d'extension : identifiant de 16 bits du type du champ d'extension.

Longueur de données d'extension : entier non signé de 16 bits. Longueur du champ Données d'extension de cette option, en octets.

Données d'extension : champ de longueur variable. Données spécifiques du type d'extension.

3 Considérations relatives à l'IANA

L'IANA a créé et va tenir un registre intitulé "Type d'extensions de CGA". Les valeurs dans cet espace de nom sont des entiers non signés de 16 bits. Les valeurs initiales pour le champ Type d'extension de CGA sont données ci-dessous ; les futures allocations sont à effectuer par action de normalisation [RFC2434]. Les allocations consistent en un nom et la valeur.

Comme recommandé dans la [RFC3692], le présent document fait les allocations suivantes pour l'utilisation expérimentale et d'essais :
la valeur 0xFFFD, avec le nom Exp_FFFD ;
la valeur 0xFFFE, avec le nom Exp_FFFE ,
la valeur 0xFFFF, avec le nom Exp_FFFF.

4 Considérations sur la sécurité

Aucun souci de sécurité n'est soulevé par l'adoption du format d'extension de CGA décrit dans le présent document. Cependant, une analyse de sécurité appropriée est nécessaire quand de nouvelles extensions de CGA sont définies afin de s'assurer qu'elles n'introduisent pas de nouvelles vulnérabilités aux schémas existants de CGA.

5. Remerciements

Des commentaires sur le présent document ont été fournis par Sam Hartman, Allison Mankin, Pekka Savola, Thomas Narten, Tuomas Aura, Stefan Rommer, Julien Laganier, et James Kempf.

6. Références normatives

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC3692] T. Narten, "L'allocation de numéros expérimentaux et d'essai est considérée comme utile", janvier 2004. (BCP0082)

[RFC3972] T. Aura, "Adresses générées cryptographiquement (CGA)", mars 2005. (*MàJ par* RFC4581, RFC4982) *(P.S.)*

Adresse des auteurs

Marcelo Bagnulo
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
SPAIN
téléphone : 34 91 6249500
mél : marcelo@it.uc3m.es
URI : http://www.it.uc3m.es

Jari Arkko
Ericsson
Jorvas 02420
Finland
mél : jari.arkko@ericsson.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.