Algorithme de vérification d'une adresse CGA
(source : livre de Gisèle Cizeault)

L'algorithme prend en entrée une adresse IPv6 et une structure de paramètres CGA, tel que définie plus haut. Cette adresse est l'adresse source d'une paquet NDP reçu, et la structure des paramètres CGA est reçue via l'option ND CGA de ce même paquet. (cf. protocole SEND).

Vérifier que le compteur de collision contienne la valeur 0, 1 ou 2. Dans le cas contraire, la vérification échoue

Vérifier que le préfixe réseau des paramètres CGA est égal au préfixe réseau de l'adresse IPv6. Dans le cas contraire, la vérification échoue

Appliquer l'algorithme SHA-1 sur la structure des paramètres CGA. Garder les 64 bits de gauche. Le résultat est **Hash1**.

Comparer **Hash1** avec l'identifiant d'interface, en ignorant les bits u et g, et les 3 bits **Sec** (les 3 bits les plus à gauche). Si la comparaison échoue, la vérification échoue.

Extraire la valeur Sec (les 3 bits les plus à gauche) de l'identifiant d'interface

Concaténer, de droite à gauche, le modifieur, 9 octets vides, la clé publique et les éventuelles extensions contenues dans la structure des paramètres CGA. Appliquer SHA-1 sur cette concaténation et garder les 112 bits les plus à gauche. La valeur obtenue est **Hash2**.

Comparer les 16***Sec** bits les plus à gauche de Hash2 avec 0. Si un seul d'entre eux n'est pas nul, la vérification échoue, sinon elle réussit.