



ASSEMBLÉE NATIONALE

11ème législature

réseaux de données

Question écrite n° 28690

Texte de la question

M. Olivier de Chazeaux appelle l'attention de M. le secrétaire d'Etat à l'industrie sur les dispositions de l'arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisations relatives aux moyens et prestations de cryptologie. Cet arrêté fait référence dans la partie technique à « un dossier préalablement déposé pour un produit usant du même procédé de cryptologie ». La question se pose de savoir par quel moyen le service central de sécurité des systèmes informatiques va informer l'industriel du contenu du « dossier préalablement déposé ». Il s'agit là en effet d'un enjeu industriel considérable dans la mesure où la référence à un dossier précisément défini permet de créer une liste de référentiels où les produits sont déjà recensés. Dès lors qu'un industriel se référera à tel ou tel produit préalablement défini, il s'exonérera d'une expertise juridique et technique coûteuse qui seule permet en réalité de satisfaire pleinement aux conditions de l'arrêté. C'est pourquoi il lui demande de bien vouloir définir la nature exacte de ce dossier et les droits que fera naître la référence à ce dernier.

Texte de la réponse

L'honorable parlementaire attire l'attention de M. le Premier ministre sur la question des modalités de description des produits et prestations de cryptologie soumis à déclaration ou autorisation. L'arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie prévoit que ce dossier comprend une partie technique relative à la description du produit concerné. Cette description comporte notamment « soit la description complète des procédés de cryptologie employés, sous la forme d'une description mathématique et d'une simulation dans un langage de haut niveau, type C ou Pascal », « soit la référence à un dossier préalablement déposé pour un produit usant du même procédé de cryptologie, soit la référence à un standard reconnu, non équivoque, et dont les détails techniques sont accessibles aisément et sans condition ». Les deux alternatives à la description mathématique accompagnées d'une simulation ont été prévues afin de faciliter aux industriels la description demandée. La première (référence à un dossier préalablement déposé) figurait déjà dans l'arrêté du 13 mars 1998, la seconde (référence à un standard reconnu) est une innovation de l'arrêté du 17 mars 1999. La première alternative était admise, en pratique depuis plusieurs années. Le SGDN (SCSSI) acceptait, dès avant sa consécration par les textes, qu'un industriel fasse référence à des dossiers qu'il avait lui-même préalablement déposés, voire à des dossiers déposés par un autre industriel dont il intégrait des modules ayant des fonctions cryptologiques. Cette deuxième hypothèse était néanmoins plus rare, et parfois déconseillée par le SGDN (SCSSI) : le dossier technique déposé par un industriel n'étant pas communiqué, les références que pouvait en faire d'autres industriels risquaient d'être inappropriées, ce qui aboutissait à compliquer et donc à ralentir le traitement des dossiers ; la pratique était néanmoins admise en cas de réutilisation complète d'un produit ou d'un module bien précis, ayant fait l'objet d'un dossier technique, dans un autre produit soumis à autorisation ou déclaration. Cette possibilité mise en oeuvre avec pragmatisme par le SGDN (SCSSI), ne semble pas avoir suscité de problème jusqu'à présent. Mais il n'est pas envisagé, au-delà de cette commodité désormais consacrée par les textes, de mettre à disposition des industriels une liste de produits déclarés ou autorisés de

leurs concurrents, assortie des informations techniques afférentes, qui pourrait servir de référentiel dans le cadre de la description d'un produit. La SGDN (SCSSI) publie sur son site internet une liste de produits déclarés et autorisés, mais seulement après accord formel des industriels concernés, et sans information technique ; systématiser cette publication et l'assortir d'informations techniques se heurteraient en revanche aux obstacles suivants : en aucun cas le SCSSI ne publie le contenu d'un dossier déposé ; il est au contraire tenu de veiller à la confidentialité des informations qui lui sont communiquées (art. 26 du décret n° 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie) ; tout au plus, dans le cadre d'une relation directe avec un industriel, le SCSSI peut faire savoir à celui-ci s'il est nécessaire ou non de décrire un procédé de cryptologie non publié ; la déclaration par référence peut-être source de confusion et d'erreurs dès lors que le dossier référencé, tel qu'il a été déposé par un industriel, n'est pas complètement connu des autres industriels ; en outre, si un produit s'avérait, après examen, non conforme à sa description, tous les dossiers faisant référence à celui déposé pour ce produit seraient entachés du même défaut, mais sans qu'il soit nécessairement possible d'obtenir les informations nécessaires auprès de l'industriel originel, au moment où la non-conformité serait mise en évidence. La deuxième alternative (référence à un standard reconnu), était également admise par le SGDN (SCSSI), en pratique, depuis plusieurs années. Sa consécration par les textes, entérinant cette pratique, n'a donc soulevé aucun problème pour les industriels et SGDN (SCSSI). Le caractère de standard reconnu dont les détails techniques sont accessibles aisément et sans condition ne semble pas avoir posé de problème d'interprétation tant pour les procédés de cryptologie que pour les autres informations du dossier technique. En cas de doute portant sur l'implémentation d'un standard reconnu (la plupart des standards permettent plusieurs implémentations qui ont laissés au choix de l'industriel : pour les algorithmes de chiffrement par exemple, RC 4, blowfish, AES, etc., la longueur de la clé n'est généralement pas fixée a priori), les incertitudes sont rapidement levées grâce aux contacts directs entre le SGDN (SCSSI) et l'industriel concerné. Le SGDN (SCSSI) n'a donc pas jugé utile de publier des précisions sur cette disposition. Il n'a d'ailleurs pas reçu de demande dans ce sens de la part des industriels.

Données clés

Auteur : [M. Olivier de Chazeaux](#)

Circonscription : Hauts-de-Seine (5^e circonscription) - Rassemblement pour la République

Type de question : Question écrite

Numéro de la question : 28690

Rubrique : Télécommunications

Ministère interrogé : industrie

Ministère attributaire : Premier Ministre

Date(s) clé(s)

Question publiée le : 19 avril 1999, page 2301

Réponse publiée le : 29 mai 2000, page 3230