ASSEMBLÉE NATIONALE

14ème législature

actes administratifs

Question écrite n° 53551

Texte de la question

M. Alain Calmette attire l'attention de M. le ministre des finances et des comptes publics sur les procédures de transmission dématérialisée entre les collectivités locales et les préfectures. L'obligation qui est faite aux communes de se doter d'un certificat de type RGS (référentiel général de sécurité), dans le cadre de la dématérialisation des actes, entraînera un surcoût pour les collectivités. Une instruction ministérielle récente précise que sa mise en œuvre sera effective à compter du 18 mai 2014. Il est également mentionné « l'obligation d'utilisation de certificats d'authentification RGS et de certificats serveurs RGS interviendra après la parution du futur cahier des charges de la télétransmission dans Actes et de l'arrêté modifiant celui de 2005 en portant approbation ». Ce report permettra aux collectivités de ne pas avoir à acquérir plusieurs certificats à quelques mois d'intervalle. Néanmoins, cette nouvelle exigence technique, même si elle constitue une avancée dans le mode de gestion communale, aura un coût qui pèsera sur les communes et plus particulièrement sur les plus petites situées en milieu rural. Or, si la collectivité estime que les inconvénients sont supérieurs aux avantages, elle dispose de la faculté en application de l'article R. 2131-3 du CGCT de renoncer à la télétransmission comme la convention qu'elle a signée avec l'État le prévoit. Il lui demande de bien vouloir lui indiquer quelles sont les dispositions qui ont été être prises pour favoriser la cohérence, la généralisation et l'harmonisation des pratiques, tout en limitant ce surcoût, notamment pour les communes les plus modestes.

Texte de la réponse

L'Association des maires de France (AMF) a demandé par un courrier du 16 mai 2013 au secrétariat général pour la modernisation de l'action publique (SGMAP) que le niveau de sécurité du certificat émetteur à utiliser par les collectivités sur @CTES (et HELIOS) soit fixé au RGS** « afin de créer un espace de confiance pérenne » ; ce niveau résulte, par ailleurs, d'une étude de risques à laquelle il a été procédé par les services du ministère de l'intérieur, conformément aux dispositions du décret dit « décret RGS » pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 dite « ordonnance téléservices ». Le recours au certificat serveur de niveau RGS* (une étoile) ne concerne que les opérateurs ou, de façon marginale, les collectivités de grande taille. Il n'existe pas à proprement parler de surcoût par rapport à ce qui était antérieurement exigé pour émettre sur @CTES, ce certificat RGS ne faisant que remplacer un certificat du type PRIS d'authentification forte précédemment exigé, selon les termes du cahier des charges du système d'information @ctes de 2005. Le certificat PRIS n'étant plus conforme aux nouvelles normes de sécurité, il n'est plus proposé à la vente depuis l'entrée en vigueur du RGS. Si le prix d'un certificat RGS d'authentification et/ou de signature affiché par certains prestataires (autour de 250 € pour trois ans) peut paraître supérieur au prix du certificat précédent, les acheteurs peuvent prendre les conseils de l'AMF, des opérateurs de transmission ou se réunir en groupement de commandes, par exemple sous l'égide de conseils généraux ou d'opérateurs de mutualisation. Le prix a pu, dans certains cas, être ramené à moins de 100 € pour trois ans. Les émetteurs ont jusqu'à la fin de l'année 2014 pour se mettre en conformité avec le RGS, dans le cadre du système d'information @ctes. L'objectif commun aux services de l'Etat et à l'AMF est de permettre l'utilisation d'un même certificat sécurisé aux collectivités qui transmettent sur plusieurs systèmes d'information. Le certificat RGS** (deux

étoiles) préconisé à l'ensemble des émetteurs pour émettre sur le système d'information @ctes pourrait être utilisé pour se connecter à différents systèmes d'information, qui requièrent un niveau de sécurité équivalent ou inférieur (tels qu'INERIS, SYLAE, etc.). Dans la même optique, le ministre a demandé à ses services d'accélérer les négociations déjà engagées avec l'Agence nationale des titres sécurisés (ANTS) qui, sous la double responsabilité du ministère de la justice et du ministère de l'intérieur, est l'autorité de certification et d'enregistrement publique nationale de certificats, notamment dédiés à la connexion avec la plateforme « communication électronique de données d'état civil » (COMEDEC) afin d'étendre l'usage de certificats communs. En outre, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) confirme qu'elle admet le caractère « multi-rôles » ou « multi-qualités » des certificats d'authentification et/ou de signature par nature nominatifs : par exemple, un maire peut signer avec le même certificat en tant que président du centre communal d'action sociale de sa commune et président d'un établissement public de coopération intercommunale. De même, il est possible à un secrétaire de mairie employé par plusieurs communes d'utiliser un seul certificat nominatif pour adresser les actes de ses différents employeurs sur le système d'information @ctes, pour autant que l'entité émettrice soit toujours clairement identifiée. L'ANSSI admet également l'utilisation de certificats double usage, à la fois authentification et signature jusqu'au niveau RGS** (deux étoiles).

Données clés

Auteur : M. Alain Calmette
Circonscription : Cantal (1re circonscription) - Socialiste, écologiste et républicain
Type de question : Question écrite
Numéro de la question : 53551
Rubrique : Collectivités territoriales
Ministère interrogé : Finances et comptes publics
Ministère attributaire : Finances et comptes publics

Date(s) clée(s)

Question publiée au JO le : 15 avril 2014, page 3311
Réponse publiée au JO le : 2 décembre 2014, page 10078