Authentification des émetteurs et signature électronique des actes

Depuis le 19 mai 2013, le décret dit « RGS » du 2 février 2010 pris en application de l'ordonnance dite « téléservices » n° 2005-1516 du 8 décembre 2005 s'applique aux systèmes d'information mettant en œuvre des échanges par voie électronique, entre des autorités administratives. Les exigences du référentiel général de sécurité (RGS) s'imposent au système d'information @CTES.

En application de ce texte, les élus ou les agents en charge de la transmission électronique dans les collectivités doivent être équipés de certificats d'authentification utilisateurs RGS**, pour transmettre par voie électronique les actes afin de garantir la sécurité des accès et des échanges de la collectivité avec les plates-formes des opérateurs.

Ces certificats d'authentification utilisateurs ne doivent pas être confondus avec les certificats de signature souvent présents sur les mêmes supports physiques, mais non obligatoires dans le cadre de la transmission électronique des actes. Seule l'utilisation d'un certificat d'authentification est imposée par le cahier des charges de transmission @CTES, mais, s'ils le souhaitent, les élus peuvent utiliser un certificat de signature électronique pour signer les actes à transmettre au contrôle de légalité, voire un certificat « double usage », servant à la fois à l'authentification et à la signature.

En l'absence de signature électronique, il n'est pas nécessaire que les collectivités transmettent des actes comportant la représentation de la signature manuscrite. Cette opération est chronophage, source d'une augmentation de la volumétrie des actes transmis, consommatrice de bande passante et peu utile au contrôle.

Les certificats d'authentification utilisateurs et/ou de signature sont nominatifs. Seul leur titulaire peut les utiliser. En cas de démission, de décès, de changement de poste ou de mandat électoral (si le certificat est au nom d'un élu), un tel certificat ne pourra plus être utilisé par le nouveau titulaire du poste ou du mandat ou par qui que ce soit, si éloigné soit-on de sa date de péremption.

Dans le cas où une infrastructure technique intervient au niveau de la collectivité, @CTES requiert une authentification serveur de niveau RGS*.

Pour réduire le coût d'achat de ces certificats, 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 d'opérateurs de mutualisation.

La liste des fournisseurs de certificats qualifiés au sens du RGS est publiée sur le site de l'organisme de qualification habilité par l'ANSSI.

Le caractère « multi-rôles » des certificats d'authentification utilisateurs et/ou de signature, par nature nominatifs, est accepté pour autant que l'entité émettrice soit toujours clairement identifiée.

- 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.

De plus, les certificats d'authentification RGS** et les certificats serveur RGS* peuvent servir aux collectivités émettrices pour s'authentifier auprès d'autres services en ligne de l'État nécessitant l'acquisition d'un certificat de même catégorie et d'un niveau identique ou inférieur (tels qu'INERIS, SYLAE, etc.) ; l'investissement consenti pour leur acquisition est donc facile à amortir.