Authentification des émetteurs et signature électronique des actes

Selon le cahier des charges de transmission @ctes, tous les émetteurs raccordés au système d'information doivent être pourvus d'une authentification conforme à l'article 5.2 de l'annexe 2 du cahier des charges « Sécurisation des échanges » de la transmission @ctes qu'il convient désormais de concilier avec le Référentiel Général de Sécurité (RGS) résultant du décret n° 2010-112, dit « décret RGS », du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005, dite « ordonnance téléservices ».

Le certificat PRIS V1 dont l'utilisation était demandée dans la version du cahier des charges de 2005 doit être remplacée par des **certificats d'authentification utilisateurs RGS****.

Le seul cas où la transmission sur le système d'information @ctes ne requiert pas d'authentification au moyen de certificats d'authentification utilisateurs RGS** est celui des collectivités de taille importante où l'envoi des actes est effectué directement depuis un serveur situé sur le réseau même de la collectivité. Dans cette hypothèse, les agents s'identifient à ce serveur par simple *login* / mot de passe pour accéder à la fonction de transmission ; ce système nécessite une authentification serveur de niveau RGS*.

Il est nécessaire de rester vigilant face à certains opérateurs de transmission (ODT) qui, pour attirer les clients par des prix plus bas, ne respectent pas les dispositions du cahier de charges actuel et n'exigent ni certificats d'authentification utilisateurs de la part des agents et/ou des élus qui transmettent leurs actes sur le système d'information @ctes, ni certificats serveurs quand la configuration de leur réseau interne s'y prête.

En outre, le caractère « multi-rôles » ou « multi-qualités » des certificats d'authentification et/ou de signature, par nature nominatifs, est accepté pour autant que l'entité émettrice est toujours clairement identifiée : par exemple, un maire peut signer avec le même certificat en tant que maire, 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 en temps partagé d'utiliser un seul certificat nominatif pour adresser les actes de ses différents employeurs sur le système d'information @ctes.

En cas de démission, de décès, de changement de poste ou de mandat électoral, un tel certificat ne pourra pas être utilisé par le nouveau titulaire du poste ou du mandat ou par qui que ce soit, si éloigné soit-il de sa date de péremption.

Authentification des émetteurs et signature électronique des actes

Seule l'utilisation d'un certificat d'authentification est imposée par le cahier des charges de transmission @ctes, mais il est conseillé aux élus d'utiliser un certificat de signature électronique, dans la mesure où les protections dispensées par un certificat d'authentification et un certificat de signature sont complémentaires. Dans les structures où l'élu se charge lui-même des transmissions, il lui est conseillé d'utiliser un certificat « double usage », servant à la fois à l'authentification et à la signature, autorisé par l'ANSSI pour les certificats RGS** (deux étoiles).

Si la personne qui transmet n'est pas l'autorité signataire, deux certificats seront utilisés, l'un au nom de l'élu signataire, l'autre au nom de l'agent en charge de la transmission.