# Le programme @ctes
# (Aide au Contrôle de légaliTé dématErialiSé)

## Ministère de l'intérieur

## Direction de Programme @ctes

# Sensibilisation à la sécurité des systèmes d'information

## @ctes et le RGS

# Qu'est-ce qu'un système d'information ?

**Un ensemble organisé de :**

- **ressources (matériels, logiciels, personnel, données et procédures) ;**
- **nécessaires à l'élaboration, à la collecte, au regroupement, au traitement, au stockage, à la classification, à la présentation et à la transmission de l'information ;**
- **au sein d'une structure.**

**@ctes est un système d'information concernant environ 50 000 utilisateurs (tous confondus).**

# Qu'est-ce qu'un émetteur ?

**Dans le cadre de @ctes, on entend par « émetteur » toute entité juridique, dont tout ou partie des actes est soumis au contrôle de légalité, au contrôle budgétaire ou à une obligation de transmission au représentant de l'État.**

**Il peut s'agir de collectivités territoriales, d'établissements publics locaux, de groupements au sens du CGCT (catégorie auxquels appartiennent notamment les établissements publics de coopération intercommunale, interdépartementale ou interrégionale), les sociétés d'économie mixte locales (SEML), les sociétés publiques locales (SPL) ou les associations syndicales de propriétaires.**

# Qu'est-ce qu'un opérateur de télétransmission ?

**Une personne morale de droit public ou privé, fournisseur de services de télétransmission et agréée par le ministère de l'intérieur, exploitant et mettant à disposition des émetteurs qui le souhaitent un dispositif de télétransmission homologué.**

**L'opérateur de télétransmission (OdT) est responsable de la mise en œuvre opérationnelle, de l'exploitation et du fonctionnement de ce dispositif de télétransmission. Il doit être le seul interlocuteur du ministère de l'intérieur pour le dispositif de télétransmission qu'il exploite, que ce dispositif soit mutualisé ou non.**

**Tout opérateur de télétransmission agréé par le ministère de l'intérieur signe une convention de raccordement avec lui.**

# Qu'est-ce qu'un opérateur de mutualisation ?

**Les opérateurs de mutualisation ont vocation à accompagner les élus et les administrations territoriales dans leur mutation vers l'administration électronique dans le cadre d'un projet plus global.**

**Ces organismes peuvent être mis en place par les départements, voire par les régions, pour mutualiser les demandes des collectivités, les infrastructures mises à leur disposition et pour négocier en leur lieu et place avec les tous les prestataires de services dont les opérateurs de télétransmission; ils proposent aussi souvent une prestation d'accompagnement au changement.**

**Ces opérateurs ont des statuts variés : centres départementaux de gestion de la fonction publique territoriale, syndicats de communes, syndicats mixtes, agences créées par les conseils généraux, sociétés publiques locales…**

# Qu'est-ce qu'un certificat d'authentification ?

**Véritable carte d'identité électronique de l'agent, le certificat d'authentification permet d'authentifier de façon sûre la personne physique qui assure cette télétransmission et d'établir une session sécurisée pour la télétransmission des données .**

**Les certificats d'authentification RGS** sont proposés sous forme matérielle, inscrits sur une puce électronique, généralement intégrée à une clé USB ou à une carte, ce qui permet de les utiliser à partir de n'importe quel ordinateur personnel.**

**Nominatif au nom de son utilisateur, le certificat d'authentification utilisateur peut être utilisé pour l'accès à plusieurs services en ligne de l'Etat, et dans le cadre de @ctes, pour le compte de plusieurs émetteurs sous certaines conditions.**

**Donc, un certificat d'authentification utilisateur est INDIVIDUEL ; il est lié à une personne physique.**

# Qu'est-ce qu'un certificat de signature électronique ?

**Un certificat de signature électronique (CSE) est l'équivalent numérique de la signature manuscrite. Il est donc nominatif, délivré à une seule personne physique (et non à un émetteur, personne morale).**

**Le certificat de signature électronique permet, à l'aide d'un procédé cryptographique, d'identifier le signataire de façon nominative, de garantir l'intégrité du document et d'engager le signataire.**

**En pratique, il est contenu sur une carte à puce ou sur une clé USB.**

# La sécurité d'un système d'information (SSI)

**C'est l'ensemble des moyens**

- **techniques (dispositif logiciel et son installation sur plateforme),**
- **humains et organisationnels,**
- **juridiques et financiers,**

**mis en place pour garantir, conserver et rétablir les quatre valeurs du système d'information.**

**Les quatre valeurs d'un système d'information sont :**

- **Confidentialité ;**
- **Intégrité ;**
- **Disponibilité ;**
- **Traçabilité.**

**La sécurité informatique prend en compte tous les éléments qui composent un système d'information :**

- **les outils (les applications - *software*) ;**
- **les procédures ;**
- **les équipements (ou matériels)**
- **les réseaux**

# Qu'est-ce que le Référentiel Général de Sécurité (RGS) ?

**Le Référentiel Général de Sécurité (RGS)**

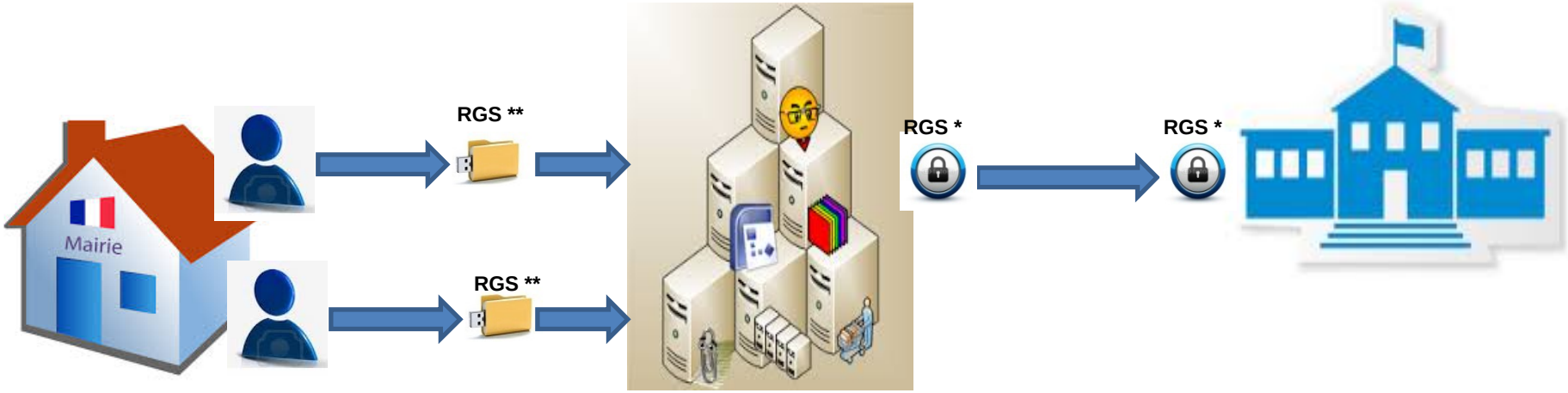
- **impose un ensemble de règles pour assurer la sécurité des informations échangées par voie électronique entre les usagers et les administrations, et entre les administrations entre-elles ;**
- **propose également des bonnes pratiques.**

**Le RGS dispose que la sécurité d'un système d'information s'apprécie de façon globale depuis l'émetteur jusqu'au « récepteur ».**

**Le RGS a été élaboré conformément à l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 *relative aux échanges électroniques entre les usagers et les autorités administratives ainsi qu'entre les autorités administratives*.**

# Circuit de la télétransmission dans @ctes

## (de l'émetteur à la préfecture, via un opérateur de télétransmission)




**Emetteur**

un certificat **RGS**** par agent chargé de la télétransmission

**Opérateur de télétransmission**

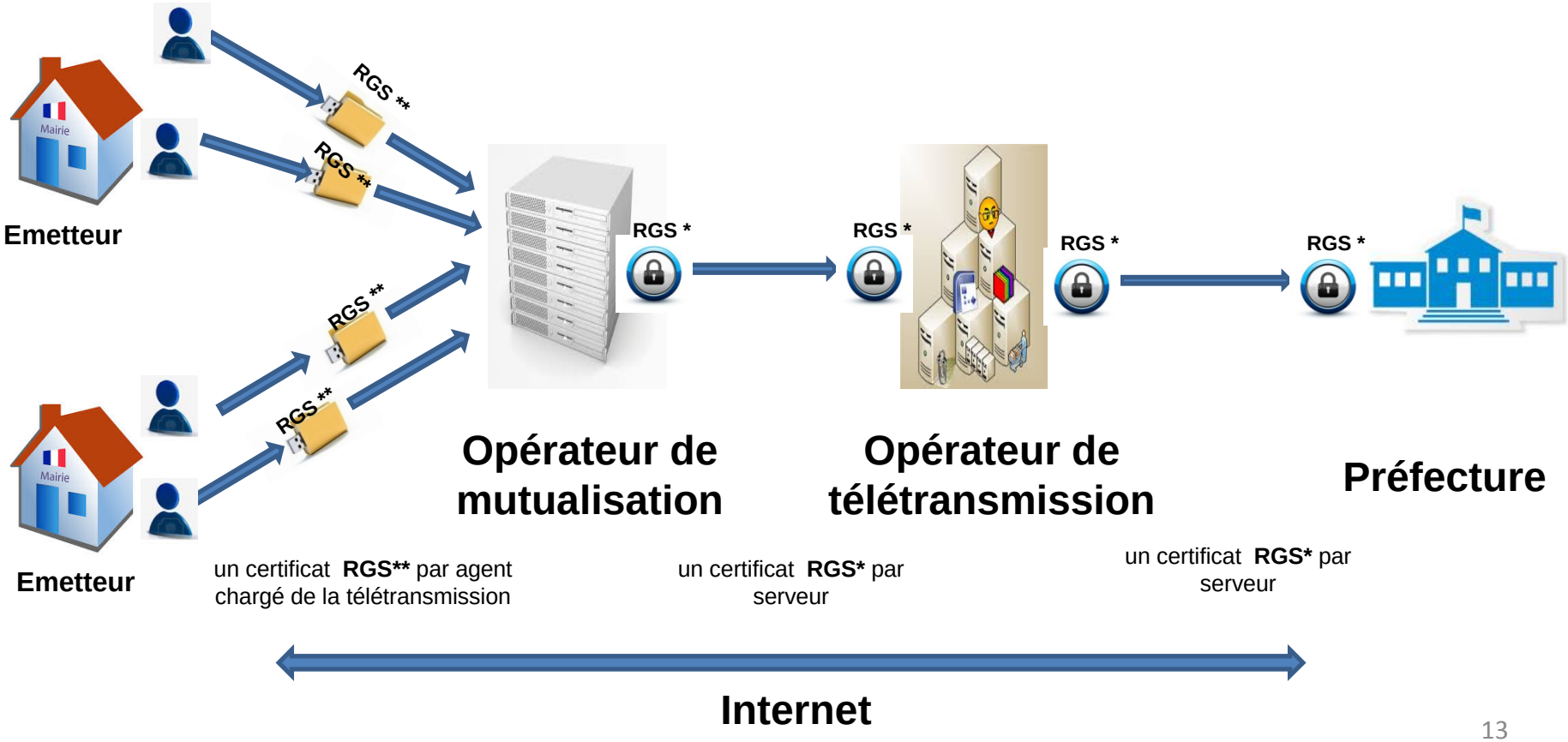
un certificat **RGS*** par serveur

**Préfecture**

**Internet**

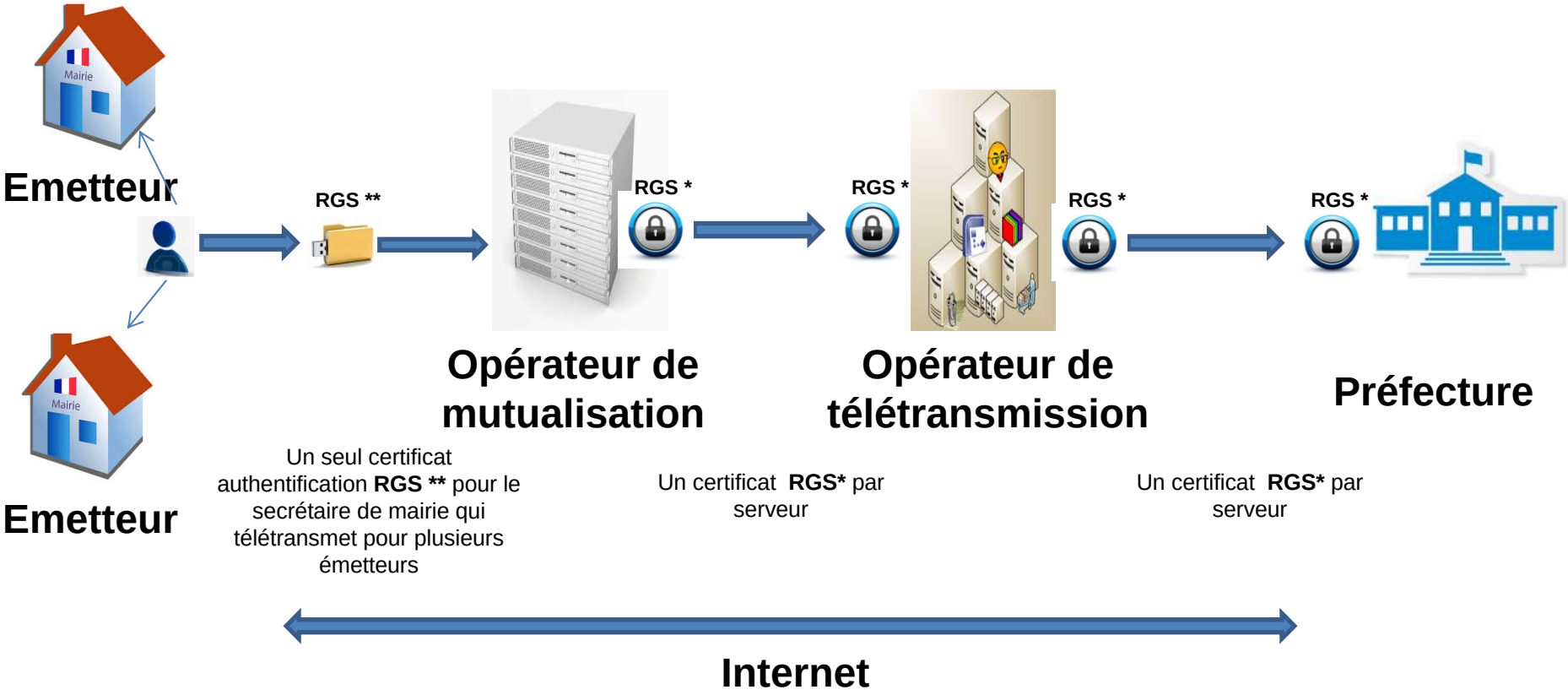
# Circuit de la télétransmission dans @ctes

## (de l'émetteur à la préfecture, via un opérateur de mutualisation et un opérateur de télétransmission)



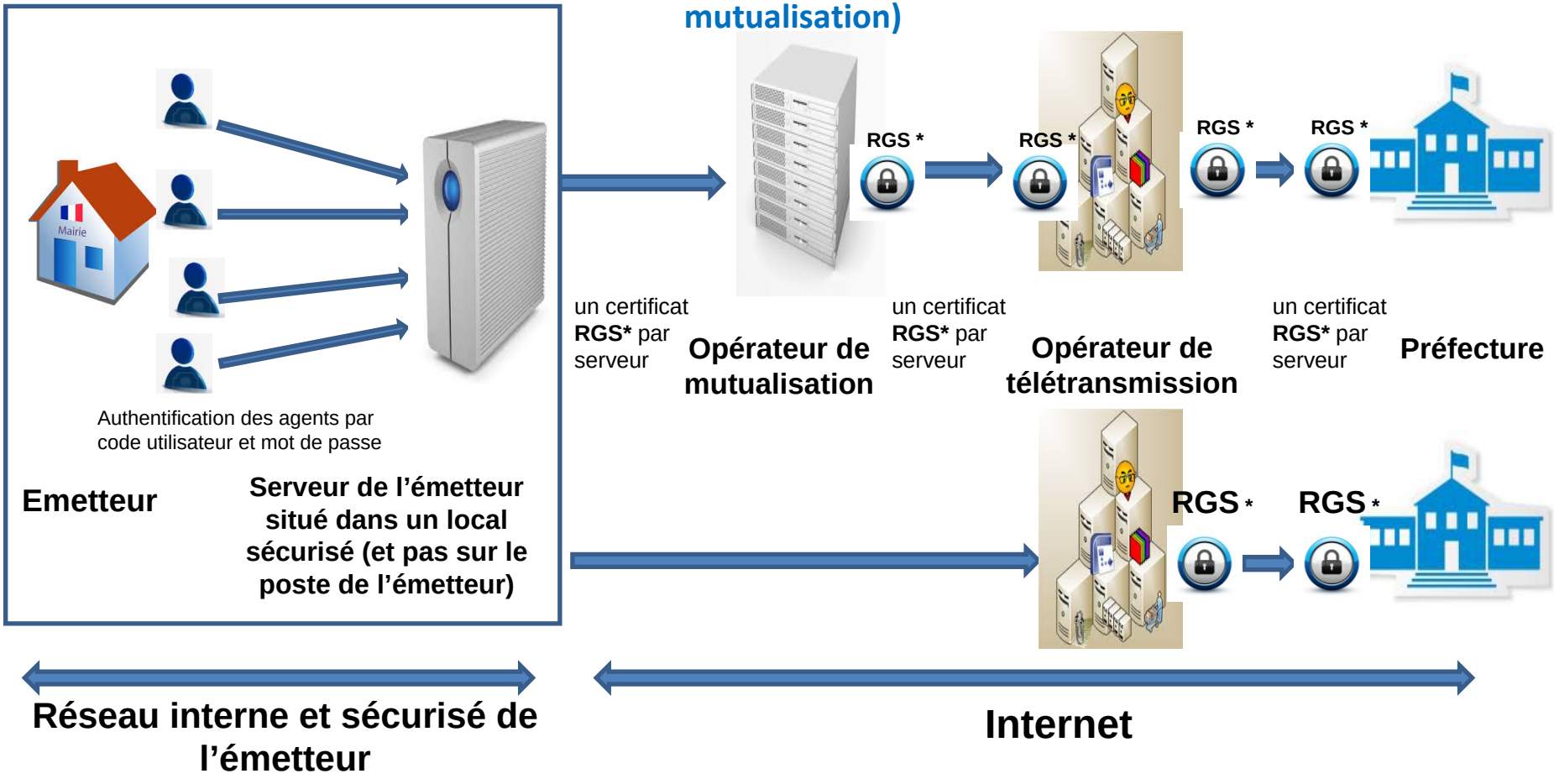
# Circuit de la télétransmission dans @ctes

## (dans le cas où un secrétaire de mairie télétransmet pour plusieurs émetteurs à la préfecture, via un opérateur de mutualisation et un opérateur de télétransmission)



# Circuit de la télétransmission dans @ctes

## (dans le cas où l'émetteur dispose d'un serveur sur son réseau interne pour procéder à la télétransmission à la préfecture, via un opérateur de télétransmission et/ou un opérateur de mutualisation)



# @ctes et le Référentiel Général de Sécurité (RGS) ?

**Les exigences du référentiel général de sécurité (RGS) s'imposent au système d'information @ctes. Il s'agit d'une obligation légale.**

**A la suite de l'étude de sécurité qui a été menée sur le système d'information @ctes, il en ressort que :**

- **Tous les émetteurs raccordés au SI @ctes doivent être munis de certificats d'authentification utilisateurs RGS** (RGS 2 étoiles) ;**
- **Si une collectivité utilise un serveur sur son réseau interne pour émettre vers @ctes , ses agents s'authentifient à l'aide d'un code utilisateur et d'un mot de passe sur le serveur qui lui est équipé d'un certificat d'authentification serveur RGS* (RGS 1 étoile) ;**
- **Les serveurs des opérateurs (de télétransmission et de mutualisation) doivent être équipés de certificats d'authentification serveurs RGS* (RGS 1 étoile).**

**Un courrier a été adressé par l'AMF (Association des Maires de France) au SGMAP (Secrétariat Général pour la Modernisation de Action Publique rattaché au Premier Ministre) le 16 mai 2013 à la suite d'une analyse de risques, afin d'exiger des certificats d'authentification RGS** pour la télétransmission sur @ctes et HELIOS.**

# Les arguments qui justifient les choix réalisés pour la mise en conformité de @ctes avec le RGS

**Les certificats d'authentification RGS sont plus robustes mais dotés de la même fonction que les certificats d'authentification utilisés actuellement sur @ctes (de type PRIS) : authentifier l'émetteur personne physique.**

**Les certificats d'authentification RGS** sont liés à un support matériel (support USB ou carte à puce) au contraire des certificats RGS*,donc difficilement duplicables.**

**Les certificats RGS** peuvent être utilisés sur tous les systèmes d'information qui requiert une authentification RGS* ou RGS**, mais pas pour les authentifications RGS*** (par exemple : COMEDEC).**

**Inversement, un certificat RGS*** peut être utilisé pour télétransmettre sur @ctes.**

# Les exigences de @ctes en matière de contrôle d'application du RGS

**L'actuel cahier des charges de la télétransmission @ctes fait déjà obligation aux opérateurs de télétransmission de s'assurer de l'utilisation d'un certificat d'authentification électronique pour l'accès aux plateformes des opérateurs.**

**Les opérateurs de télétransmission qui ne respectent pas cette obligation doivent se mettre en conformité rapidement car les émetteurs (leurs clients) ne sont pas protégés.**

**Dès le 18 mai 2014, les opérateurs de télétransmission qui ne respecteraient pas le cahier des charges de la télétransmission @ctes pourraient se voir suspendre leur agrément ou le perdre ; dans cette hypothèse, leurs émetteurs ne pourraient plus télétransmettre leur actes.**

# Les exigences de @ctes en matière de contrôle d'application du RGS

**La DGCL a exigé de tous les opérateurs de télétransmission la liste des certificats de tous les émetteurs.**

**Ces certificats d'authentification doivent être mis à niveau pour le 18 mai 2014 : à cette date, les certificats d'authentification utilisateurs devront être de niveau RGS** (deux étoiles) et les certificats serveurs d'authentification de niveau RGS*.**

**Un certain nombre d'opérateurs de télétransmission ont exigé de leurs clients l'achat immédiat de certificats d'authentification RGS** (deux étoiles) ; or, les émetteurs disposent d'un délai courant jusqu'au 18 mai 2014 pour se mettre en conformité.**

# Les préconisations de @ctes en matière de contrôle d'application du RGS

**Il est conseillé aux émetteurs ne disposant d'aucun certificat d'authentification d'acheter et d'installer le certificat demandé le plus tôt possible.**

**Nous suggérons que le ou les certificat(s) d'authentification RGS** soi(en)t établi(s) au nom d'un (ou des) fonctionnaire(s) territorial(aux) en charge de la télétransmission des actes, compte tenu de l'imminence des élections municipales.**

**Pour la même raison, si les émetteurs souhaitent acheter un certificat double usage (authentification ET signature, donc mis au nom du maire), il est préférable qu'ils attendent que les élections soient passées.**

**Les émetteurs ont jusqu'au 18 mai 2014 pour se mettre en conformité.**

# Les préconisations de @ctes en matière de contrôle d'application du RGS

**Les opérateurs de mutualisation sont des prestataires susceptibles d'intervenir sur la chaîne de télétransmission en amont des opérateurs de télétransmission agréés.**

**Ces opérateurs ne doivent rendre accessibles aux émetteurs les fonctions de télétransmission qu'après authentification de l'émetteur au moyen d'un certificat d'authentification RGS** et qu'après authentification des éventuels serveurs des émetteurs au moyen d'un certificat d'authentification RGS*.**

**Dans le futur cahier des charges de la télétransmission, des exigences de sécurité leur seront imposées. Par exemple, fournir aux opérateurs de télétransmission les informations relatives aux coordonnées d'authentification contenues dans les certificats authentification RGS** et RGS*.**

# Les préconisations de @ctes en matière de prix des certificats RGS

**Le prix affiché d'un certificat RGS** peut varier de moins de 100 € jusqu'à 300 € pour trois ans.**

**Possibilité de se réunir en groupements de commande comme cela est pratiqué par certains conseils généraux et centres de gestion de la fonction publique territoriale (coût unitaire de leurs certificats d'authentification divisé par trois environ).**

**Possibilité pour l'opérateur de télétransmission qui en fait commande pour le compte de ses clients d'obtenir un prix de gros.**

**Possibilité d'acheter le certificat d'authentification directement à un fournisseurs de certificats PSCO qualifiés au sens du RGS qui en font commerce.**

**Cette liste est publiée sur le site de l'organisme de qualification habilité par l'ANSSI, la société LSTI, à l'adresse :**
**http://www.lsti-certification.fr/images/liste_entreprise/RGS.pdf**

# Le calendrier de @ctes en matière de mise en conformité avec le RGS

**Au plus tard au 18 mai 2014, tous les émetteurs devront être équipés d'un certificat d'authentification RGS** pour télétransmettre sur @ctes.**

**Au plus tard au 18 mai 2014, tous les serveurs des « collectivités émettrices », des opérateurs de mutualisation et des opérateurs de télétransmission devront être équipés d'un certificat d'authentification RGS* pour télétransmettre sur @ctes.**

**Au plus tard au 18 mai 2014, l'ensemble du système d'information @ctes sera en conformité avec le RGS.**

# La signature électronique dans @ctes

- **Si les collectivités souhaitent signer électroniquement les actes qu'elles envoient au contrôle de légalité, il convient de ne pas les décourager.**

- **Le type de signature (électronique ou manuscrite) n'a pas d'incidence sur la télétransmission.**

- **Le propre des certificats d'authentification et/ou de signature (il existe des certificats ayant ce double usage) est d'être nominatif ; seul son titulaire peut l'utiliser.**

# Groupe de travail sur la mise en conformité de @ctes avec le RGS

- Des experts des services de l'Etat,
- des représentants des émetteurs de toutes tailles,
- des représentants des opérateurs de mutualisation,
- et des opérateurs de télétransmission

se réunissent pour travailler à la ré-écriture du futur cahier des charges de la télétransmission.