

LE REFERENTIEL GENERAL DE SECURITE – RGS ET LES CERTIFICATS DE SIGNATURE ELECTRONIQUE DANS LES MARCHES PUBLICS

INFORMATIONS PRATIQUES APRÈS L'ECHEANCE DU 19 MAI 2013

I / Le RGS

Le référentiel général de sécurité prévu par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005¹ fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs.

L'article 14 de l'ordonnance fixe le calendrier qui s'impose aux autorités administratives pour la mise en conformité de leurs systèmes d'information avec le RGS : « *Les systèmes d'information existant à la date de publication du référentiel général de sécurité mentionné au I de l'article 9 sont mis en conformité avec celui-ci dans un délai de trois ans à compter de cette date. Les applications créées dans les six mois suivant la date de publication du référentiel sont mises en conformité avec celui-ci au plus tard douze mois après cette date* ».

Compte tenu de la date de parution de l'arrêté approuvant le RGS (18 mai 2010), la date limite fixée par l'ordonnance est le 19 mai 2013.

Pour les systèmes d'information relatifs aux marchés publics, cela signifie que la mise en conformité avec le RGS devait intervenir au plus tard le 19 mai 2013, et que depuis cette date, seuls les produits ou services conformes au RGS (ou à des conditions de sécurité équivalentes) peuvent être utilisés.

Les règles fixées sont définies selon des niveaux de sécurité prévus par le référentiel pour des fonctions de sécurité, telles que l'identification, la signature électronique, la confidentialité ou l'horodatage.

La conformité d'un produit de sécurité et d'un service de confiance à un niveau de sécurité prévu par ce référentiel peut être attestée par une qualification.

L'ordonnance du 8 décembre 2005 prévoit que l'autorité administrative détermine pour chaque système d'information, après étude des risques, le niveau de sécurité requis parmi les niveaux prévus par le RGS (niveau *, ** ou ***). Les échanges intervenant via le système d'information doivent par la suite respecter les règles correspondantes. Pour les marchés publics, si le profil d'acheteur requiert un niveau de sécurité ** du RGS, tous les produits utilisés sur le profil d'acheteur, dont le certificat de signature électronique, devront correspondre au moins aux préconisations du niveau ** du RGS. Cela signifie que la plateforme devra reconnaître et accepter les produits de niveau ** et ***, mais pas ceux de niveau *.

II / Les certificats

Les documents qui doivent être signés par l'opérateur économique le sont au moyen d'un certificat de signature électronique. Pour les marchés publics, les principaux documents sont l'acte de candidature et l'acte d'engagement. Ces documents sont les seuls devant être signés par application du code des marchés publics.

¹ Ordonnance relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Le certificat électronique est une pièce d'identité électronique. Il contient l'identité du titulaire (une personne physique) et l'identité de la personne morale pour laquelle le certificat est délivré. Celui-ci est stocké sur une clé USB à crypto processeur, une carte à puce, ou sur le PC de l'utilisateur, selon le besoin de l'utilisateur (authentification ou / et signature).

Le RGS autorise la signature des documents électroniques en utilisant une clé privée associée à un certificat mono usage, dédié à la signature, ou à un certificat double usage combinant à la fois les fonctions d'authentification **et** de signature (mais il n'y a pas de certificats « double usage » de niveau 3 étoiles)

Les signataires utilisent le certificat de leur choix parmi l'une des trois catégories définies par l'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics. Toutes les catégories de certificats **conformes au RGS ou à des conditions de sécurité équivalentes** sont utilisables (dès lors, bien sûr, que le certificat est utilisable pour les marchés publics : se renseigner auprès des prestataires sur les conditions de commercialisation²)

Prestataires qualifiés et produits qualifiés

Des certificats de signature qualifiés RGS sont commercialisés par des *prestataires de services de confiance qualifiés*.

La liste des organismes habilités par l'ANSSI³ à qualifier des *prestataires de service de confiance* est disponible à l'adresse suivante :

<http://www.ssi.gouv.fr/fr/certification-qualification/qualification-d-un-prestataire-de-service-de-confiance/organismes-de-qualification-habiles.html>

La société LSTI (La Sécurité des Technologies de l'Information), organisme accrédité par le COFRAC, est, au 15 avril 2013, la seule entité habilitée à qualifier des *prestataires de service de confiance qualifiés*.

Une liste des *prestataires qualifiés* au sens du RGS⁴ figure sur le site de LSTI (auquel on accède également via celui de l'ANSSI : <http://www.ssi.gouv.fr/fr/produits-et-prestataires/prestataires-de-services-de-confiance-qualifies/>):

<http://www.lsti-certification.fr/>

Il n'existe pas de liste officielle (ni même officieuse) des produits RGS commercialisés et utilisables pour les marchés publics.

Toutefois, en page d'accueil du site de LSTI, l'onglet « Prestataires qualifiés RGS » permet d'accéder à un tableau (format pdf) dénommé « Liste des prestataires de certification électronique qualifiés »

Ce tableau fournit les noms des prestataires et donne la liste, pour chacun d'eux, des produits ou services qu'il a développé et parmi lesquels, pour certains prestataires, figurent des certificats qui permettent la signature des candidatures et des offres⁵.

Les sites Internet des prestataires ne renseignent pas toujours clairement sur les certificats de signature proposés.

Il est donc pratiquement toujours nécessaire (et prudent) de les contacter afin de connaître leurs produits, leurs conditions d'utilisation, et leurs coûts.

Certains de ces prestataires (ou Autorités de certification) commercialisent⁶ des certificats permettant à des entreprises de répondre aux marchés publics (information à la date du 15 avril 2013, sous réserve de vérification) : l'Assemblée permanente des Chambres de Métiers, Certeuropa, Certinomis, Chambersign

² Les certificats électroniques conçus par les prestataires ne sont pas tous des certificats de signature.

³ Agence nationale de la sécurité des systèmes d'information

⁴ Les prestataires peuvent également demandés à être qualifiés au sens des normes européennes ETSI (European Telecommunications Standards Institute) : TS 102 042 (qui équivaut, selon le niveau de confiance, au RGS 1 étoile ou 2 étoiles) et TS 101 456.

⁵ La qualification de ces produits ou services relève de l'ANSSI.

⁶ A la date du 15 avril 2013.

France (association créée par les Chambres de commerce et d'industrie), Click & Trust, Dhimyotis, Keynectis (l'onglet « certificats », en haut et à gauche de la page d'accueil, conduit au site Internet de SSL Europa, son distributeur), NATIXIS (mais uniquement auprès des entreprises ayant un compte ouvert chez NATIXIS), SG Trust Services (Société Générale)⁷.

Certains produits font par ailleurs l'objet d'un référencement, lequel atteste que le certificat est interopérable⁸. On accède aux produits référencés par le lien suivant⁹ :

<http://references.modernisation.gouv.fr/liste-des-offres-r%C3%A9f%C3%A9renc%C3%A9es>

Les listes de confiance

L'arrêté du 15 juin 2012 prévoit que le certificat de signature utilisé puisse appartenir à l'une des catégories de certificats délivrées par une autorité de certification figurant sur la liste de confiance d'un Etat-membre, telle qu'établie, transmise et mise à la disposition du public par voie électronique par la Commission européenne.

La « liste de listes de confiance » ainsi tenue par la Commission européenne (European Commission: List of Trusted List information as notified by Member States) permet d'accéder aux listes de confiance des Etats-membres.

Cette liste est provisoirement accessible sous format XML et sous format PDF aux adresses respectives suivantes :

https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf

La liste de confiance française (Trust-service Status List – TSL) est également disponible au format « machine » XML sur le site :

<http://references.modernisation.gouv.fr/fr>

Les informations figurant sur une liste de confiance permettent la vérification facilitée de la signature électronique ; mais ces listes ne citent généralement pas les produits ou services, seulement les entités bénéficiant de la confiance. Elles ne peuvent donc suffire à opérer le contrôle de la conformité ou de l'équivalence au RGS. En pratique, ces listes comportent des informations principalement destinées à des machines, les rendant inutilisables pour des personnes.

Le profil d'acheteur permet généralement d'assister le pouvoir adjudicateur dans la vérification de la signature électronique, la plateforme pouvant récupérer les éléments des listes de confiance disponibles en mode de lecture « machine » pour un examen automatisé du certificat de signature.

Il est donc possible, via la liste de confiance européenne, d'accéder aux TSL des Etats membres (notamment la liste de confiance française), c'est-à-dire aux entités habilitées à délivrer des certificats dont les autorités de certification des différents Etats considèrent qu'ils répondent aux exigences de sécurité fixées par ceux-ci¹⁰.

Il est aussi possible d'accéder à ces listes de confiance par l'outil EU Trust Service status List (TSL) Analysis Tool disponible à l'adresse suivante :

<http://euts1.3xasecurity.com/tools/>

⁷ CRYPTOLOG International devrait commercialiser un produit d'ici septembre 2013, son dossier étant en cours de traitement par LSTI.

⁸ Les certificats une étoile et les certificats « double usage » (authentification et signature) ne sont pas référençables ; seuls sont référençables les certificats de signature (mono usage) deux et trois étoiles, et les certificats d'authentification (mono usage) deux et trois étoiles.

⁹ Il y a davantage de produits référencés que ceux qui figurent sur cette liste, mais ils sont utilisés en interne par le prestataire et ne sont donc pas commercialisés.

¹⁰ De même que tous les prestataires qualifiés par LSTI ne conçoivent pas ou ne commercialisent pas des certificats permettant de soumissionner à un marché public, les produits ou services portés sur ces TSL ne sont pas tous conçus pour signer une candidature ou une offre.

Lorsque le certificat de signature émane d'une entité figurant sur la liste de confiance française ou d'une liste de confiance d'un autre Etat-membre, c'est-à-dire qu'il peut être relié à un prestataire ou un produit de sécurité référencé par la France ou, pour les autres Etats-membres, par la Commission européenne, la conformité du produit au RGS est présumée, et les seules vérifications à opérer sont celles du niveau de sécurité (*, ** ou *** ou leurs niveaux équivalents) et de la validité de la signature.

La responsabilité de l'acheteur

La vérification des certificats de signature électronique et de la validité de la signature elle-même font partie des fonctionnalités classiques d'un profil d'acheteur, sans que l'acheteur ait dû se doter des compétences techniques pour les examiner.

Toutefois, il faut insister sur le fait que, quel que soit le niveau d'automatisation des contrôles opérés, et quel que soit le résultat obtenu, l'acheteur a le pouvoir d'accepter ou de refuser une candidature ou une offre. Il en supporte bien sûr les conséquences, notamment en cas de contentieux ; si, en fonction des clauses de son contrat, la responsabilité du gestionnaire du profil d'acheteur peut être recherchée, elle n'exonère pas l'acheteur de sa responsabilité, la décision lui appartenant seul.

Logiquement, les certificats PRIS v1 ont vocation à disparaître, sauf à démontrer qu'ils garantiraient un niveau de sécurité équivalent aux prescriptions obligatoires du RGS.

Malgré l'échéance du 19 mai 2013, il est possible que certains profils d'acheteur refusent des certificats qualifiés RGS, ou au contraire continuent à accepter des certificats PRIS v1.

Si une certaine souplesse est acceptable dans les premières semaines de la date fatidique du 19 mai 2013, cette situation ne peut être que transitoire.

En tout état de cause, comme énoncé plus haut, l'acheteur devra systématiquement accepter tous les certificats qualifiés RGS, sous réserve que ceux-ci correspondent au niveau de sécurité (*, ** ou ***) rendu obligatoire par l'acheteur, principe qui vaut également pour tous les certificats équivalents au RGS.

Dans ce contexte, il ne faut pas non plus oublier que, comme pour les marchés non dématérialisés, la vérification de la capacité du signataire à engager l'entreprise reste à effectuer par l'acheteur (documents relatifs aux pouvoirs des personnes habilitées à engager les candidats).