Fédération Nationale des Tiers de Confiance

La dématérialisation des marchés publics

Guide de Présentation

Collection
Les Guides de la Confiance

SOMMAIRE

1 La dématérialisation des marchés publics dans les textes

Depuis 2001, l'article 56 du Code des marchés publics autorise la passation des marchés publics par voie électronique. Cette autorisation est devenue obligation au 1er janvier 2005 pour toutes les procédures dites "formalisées", c'est-à-dire pour les achats d'un montant plus élevé que les seuils (par exemple 210.000 € pour les marchés de travaux) : pour ces marchés, la Personne Publique ne peut plus refuser de recevoir des candidatures et offres par la voie électronique.

Outre les procédures de passation de marchés, la dématérialisation permet l'usage d'enchères électroniques inversées (décret du 18 septembre 2001), et établit de nouveaux outils pour l'achat tels que le système d'acquisition dynamique ou les accords cadres. Nous n'aborderons pas ici ces pratiques, encore anecdotiques du point de vue de l'usage.

Avec la loi du 13 mars 2000 relative à la signature électronique, la Directive de l'Union européenne du 31 mars 2004 relative à la coordination des procédures de passation des marchés publics de travaux, de fournitures et de services, la Loi du 21 juin 2004 sur la Confiance dans l'Economie Numérique, l'Ordonnance du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, tout un arsenal juridique a été développé pour aboutir à la mise en œuvre effective de la dématérialisation, auquel s'ajoutent des textes de référence sans valeur normative mais publiés par le Ministère de l'Economie, des Finances et de l'Industrie : vade-mecum juridique, Politique de Référencement Intersectorielle de Sécurité, guide sur la sécurité des systèmes d'information…

Par ailleurs, de nombreuses collectivités publiques ont déjà établi en interne un "guide de bonnes pratiques" définissant le mode opératoire dans la "zone de liberté" parfois juridiquement inquiétante que constituent les Marchés à Procédure Adaptée.

1.1 Les obligations de la collectivité publique

Au titre de l'article 56 du Code des marchés publics, la dématérialisation met la Personne Publique face à deux obligations.

Tout d'abord, la publication de l'avis d'appel public à la concurrence au Bulletin Officiel des Annonces des Marchés Publics (BOAMP) doit être effectuée par voie de téléprocédure.

Ensuite, et c'est là le plus contraignant, il doit être en mesure de recevoir des candidatures et des offres par la voie électronique. Et ce, bien entendu, dans le respect des grands principes de l'achat public, et avec à sa charge la lourde responsabilité de garantir la sécurité des transactions et des données.

Pour ce faire, la personne publique se dotera d'une plate-forme de dématérialisation, qui peut être interne ou externalisée (voir § 4). Cette solution informatique lui garantira la conformité du déroulement de la procédure d'achat (voir § 2) et le respect des règles de sécurité (voir § 3).

Chaque procédure d'achat est régie par le Règlement de la Consultation (RC), qui précise les règles applicables. Ce RC comprend désormais, en plus des indications jusqu'ici présentes, les règles relatives à la dématérialisation : adresse de la plate-forme à utiliser, format de signature électronique, Autorités de Certification reconnues, formats acceptables pour les documents électroniques, traitement appliqué aux documents contenant des virus, etc.

1.2 Obligations des candidats

Les entreprises candidates aux marchés publics n'ont aucune obligation de répondre par la voie électronique. Elles ont toujours la possibilité de demander le Dossier de Consultation des Entreprises sous forme papier et de déposer leur réponse sous forme papier.

Le fait de télécharger un cahier des charges électronique ne les contraint pas à répondre par la voie électronique.

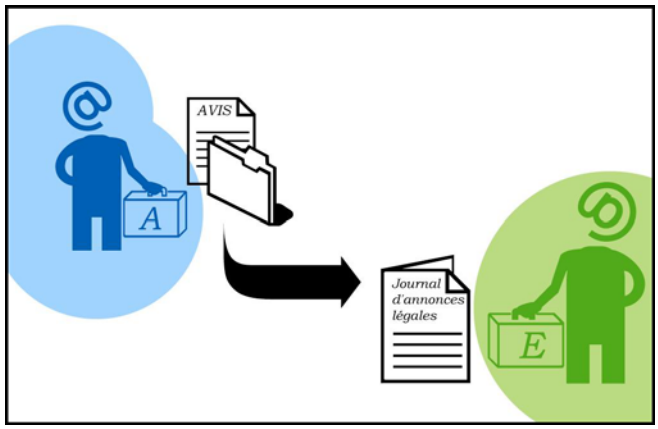
En revanche, si une entreprise choisit de répondre par la voie électronique, elle doit appliquer les contraintes indiquées dans le Règlement de la Consultation en ce qui concerne les modalités de réponse, sous peine de voir son offre rejetée. En particulier, lorsqu'une signature électronique est obligatoire (et c'est systématiquement le cas, dans les procédures formalisées, pour la candidature et l'acte d'engagement), l'entreprise doit acquérir un certificat de signature auprès d'une Autorité de Certification référencée sur un site gouvernemental dont on trouve l'URL dans l'article 6 de l'arrêté du 28 août 2006 : http://www.entreprises.minefi.gouv.fr/certificats/.

2 Le déroulement de la procédure d'achat

Il existe dans le droit français de nombreuses procédures d'achat public : appels d'offres ouverts ou restreints, concours ouverts ou restreints, marchés négociés, dialogue compétitif, sans oublier les procédures adaptées pour lesquelles la liberté de déroulement est très grande.

Les étapes élémentaires décrites ci-dessous, avec un enchaînement qui peut varier, demeurent semblables pour toutes les procédures.

2.1 Publication d'avis



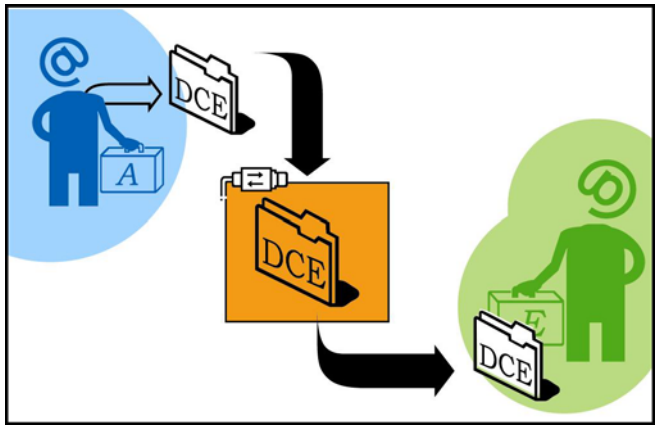
La publicité visant à la mise en concurrence doit être adaptée en fonction du montant, de la nature de l'achat et de la réalité concurrentielle sur le marché.

Une publicité réalisée via un site web peut venir en complément d'une publicité dans les organes de presse habilités, ou être suffisante pour les petits marchés.

Des services d'alertes ciblées permettront de faciliter l'accès des entreprises aux marchés publics.

L'élément important demeure la date d'envoi en publication, qui doit être connue de manière certaine car c'est elle qui marque le début du délai de remise des plis.

2.2 Mise en ligne du Dossier de Consultation des Entreprises



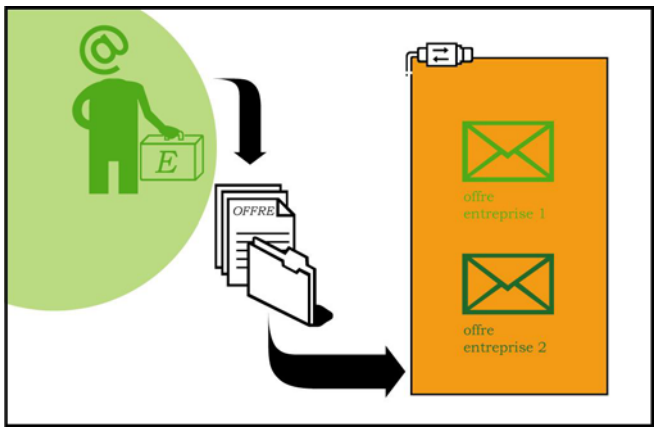
Au titre de l'arrêté du 28 août 2006, la Personne Publique met en ligne de son Dossier de Consultation des Entreprises (DCE – il s'agit du cahier des charges), à l'exclusion des éléments qu'elle estime sensibles ou confidentiels, ou trop volumineux pour être téléchargés. Le téléchargement des cahiers des charges est actuellement le service qui rencontre le plus de succès : on dénombre entre 6 et 10 téléchargements de DCE en moyenne.

La Personne Publique a la possibilité de signer électroniquement tout ou partie des fichiers de manière à en garantir l'intégrité et l'authenticité, sans que cela ait un caractère d'obligation.

Le téléchargement du DCE par les entreprises donnera lieu à la tenue automatique, par la plate-forme de dématérialisation, du Registre des Retraits. En cas de modification du dossier, un mécanisme d'alerte par mail permettra aux entreprises ayant déjà effectué un retrait d'être tenues au courant de la disponibilité d'une nouvelle version.

Il est apprécié par les entreprises, surtout pour les dossiers volumineux, de pouvoir procéder à un téléchargement partiel, ou de pouvoir demander des éléments sur support papier, par exemple pour les plans.

2.3 Transmission des plis par les entreprises



Le dépôt d'un pli par l'entreprise, comprenant la candidature et/ou l'offre, doit être soumis à des conditions de sécurité très strictes, mais doit également bénéficier d'une ergonomie particulièrement soignée afin d'éviter toute erreur de manipulation qui peut avoir des conséquences graves.

La nécessité d'engagement a priori de l'entreprise sur son offre rend nécessaire l'inclusion, dans les interfaces, d'un outil intégré de signature électronique et de vérification de signature.

L'exigence de confidentialité des plis pousse à opter pour un chiffrement (cryptage) de bout en bout : le pli, une fois chiffré sur le poste du candidat, ne pourra ainsi être déchiffré que par la Personne Publique lors de la Commission d'ouverture, sans que la plate-forme de dématérialisation ou l'hébergeur exploitant le service puisse en prendre connaissance.

Afin d'éviter des impossibilités de dépôt, il est fondamental que la plate-forme de dématérialisation offre des garanties de disponibilité importantes, fondées sur la redondance des serveurs et des procédures d'exploitation très strictes. Il serait en effet possible à un candidat qui se serait trouvé dans l'impossibilité de déposer son pli de faire annuler une procédure.

La notion de délai de réponse étant incontournable, un horodatage certain des dépôts de plis sera effectué par la plate-forme. Sur cette base, le dépôt des plis donnera lieu à la tenue automatique, par la plate-forme de dématérialisation, du Registre des Dépôts.

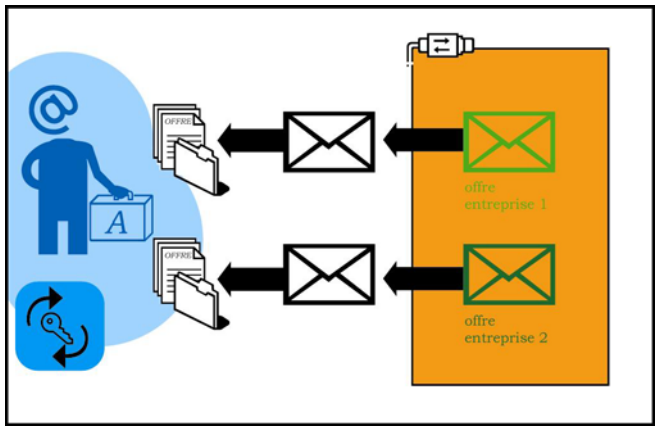
Un accusé de réception de pli horodaté devra être fourni à l'entreprise pour attester de son dépôt.

Par ailleurs, les entreprises ont la possibilité de doubler le dépôt électronique par un envoi sur papier support physique électronique appelé "copie de sauvegarde". Cet exemplaire ne sera ouvert qu'en cas de problème de transmission ou de découverte d'un virus informatique dans le pli déposé électroniquement.

2.4 Analyse des candidatures et offres

Une fois le délai imparti pour la réponse dépassé, la Personne Publique pourra procéder à la commission d'examen des candidatures et/ou des offres.

Pour ce faire, il est préférable que le téléchargement des plis puisse se faire préalablement à la tenue de la Commission, de manière à éviter un temps de transfert potentiellement long, qui nuirait au bon déroulement de la séance.



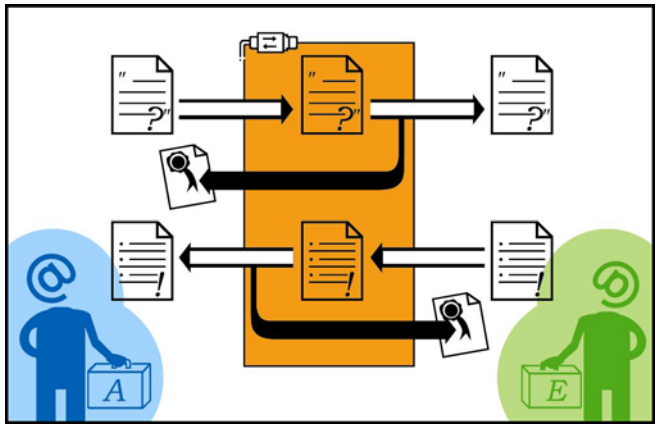
Les aspects organisationnels de cette commission doivent être prévus avec soin : ordinateur dédié et projecteur vidéo sont nécessaires pour permettre à tous les membres de visualiser les plis et leur contenu.

Le président de séance désignera les enveloppes qui doivent être ouvertes et celles qui ne doivent pas l'être, en fonction des délais de réception et/ou des capacités des candidats. La plate-forme sera le garant de ces choix et devra fournir, en fin de procédure, un compte-rendu infalsifiable rendant compte des actions d'ouverture réalisées. Il pourra ainsi être démontré que l'offre d'un candidat non retenu n'a pas pu être ouverte par la Personne Publique.

Une fois les plis électroniques ouverts, les fichiers qui les composent pourront être acheminés vers les services chargés de les analyser par tout moyen : partage sur le réseau, courrier électronique, CD-ROM gravé….

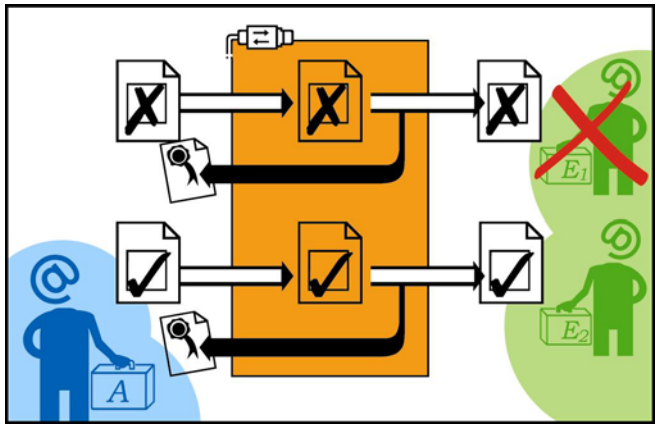
Enfin, le service acheteur procèdera à la synthèse des plis déposés par voie papier et de ceux qui auront été reçus par la voie électronique pour aboutir à un procès-verbal exhaustif. La plate-forme de dématérialisation et, le cas échéant, le logiciel de suivi de marché faciliteront ce travail en fournissant les données à un format compatible.

2.5 Échanges entre la Personne Publique et les candidats



La plate-forme de dématérialisation pourra offrir un service de courrier recommandé électronique permettant les échanges de questions / réponses ou encore les demandes de précisions ou de pièces complémentaires.

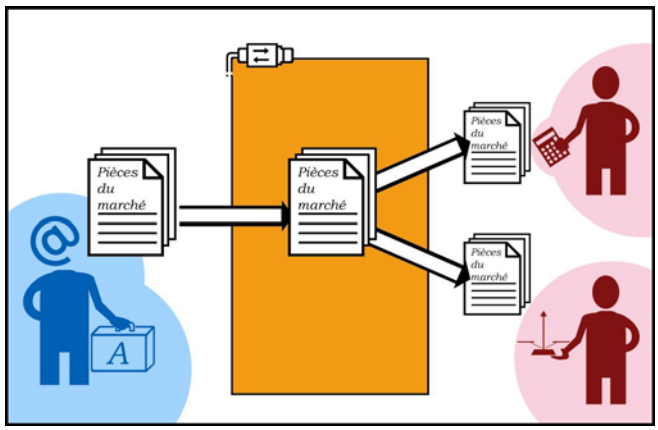
2.6 Notification du marché



Si le marché est attribué à une entreprise ayant répondu par la voie électronique, la notification du marché peut avoir lieu également par la voie électronique.

La Personne Publique doit alors signer électroniquement l'acte d'engagement fourni par l'entreprise avant de le lui renvoyer par courrier électronique recommandé. L'outil de signature électronique inclus doit donc inclure la possibilité de co-signature afin de disposer, pour le même document, de la signature de l'entreprise et de celle de la Personne Publique.

2.7 Continuité : comptable / contrôle de légalité / juge des comptes

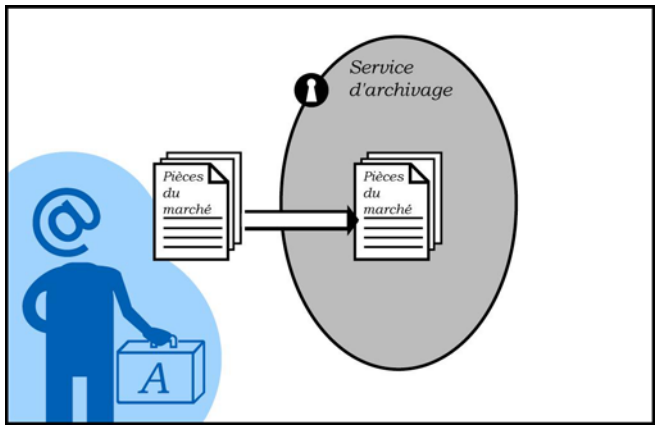


Les échanges électroniques inter-administrations se développeront parallèlement à la dématérialisation elle-même, ce qui permettra d'étendre la chaîne de la dématérialisation jusqu'au contrôle de légalité et à la comptabilité publique.

Si cette possibilité n'existe pour l'heure qu'à titre expérimental, elle sera prochainement généralisée ; de ce fait, la capacité de la plate-forme de dématérialisation à s'interfacer avec ces services est importante ; toutefois, cette interconnexion pourra également être offerte par un logiciel de gestion des marchés.

Dans un premier temps, le transfert de ces pièces passe par une rematérialisation : il faudra donc imprimer et re-signer de manière manuscrite les pièces à transmettre aux organes de contrôle.

2.8 Archivage



Les pièces relatives aux marchés publics doivent être archivées pour des durées de l'ordre de 10 à 30 ans.

La Personne Publique, pour tous les domaines dans lesquels la dématérialisation se développe (factures, fiches de paye, délibérations…), se trouvera face à la problématique de l'archivage ; c'est pourquoi il est souhaitable d'aborder ce sujet de manière transversale et non uniquement du point de vue des marchés publics.

La Personne Publique doit donc se doter d'une solution d'archivage qui respecte la législation en la matière. Il faut être attentif à la fiabilité, à la disponibilité et à la pérennité de l'archivage ainsi réalisé. On pourra opter pour une solution d'archivage internalisée ou externalisée lorsque la loi le permet. Les capacités d'intégration de la plate-forme de dématérialisation avec le système d'archivage de la collectivité doivent être prises en compte.

3 La sécurité et le rôle du Tiers de Confiance

La dématérialisation de la passation des achats publics passe par la mise en œuvre de dispositifs sécurisés. En effet, les textes imposent de nombreuses contraintes sur le traitement des informations, et les attentes des collectivités publiques comme des fournisseurs vont souvent bien au-delà de ces exigences réglementaires, de manière à garantir à la procédure menée par voie électronique une sécurité juridique au moins équivalente, voire meilleure, qu'à la procédure papier traditionnelle.

La récente ordonnance du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives instaure un Référentiel Général d'Interopérabilité et un Référentiel Général de Sécurité. Ces référentiels seront publiés prochainement par le MINEFI et décriront les niveaux de sécurité qu'il est nécessaire de mettre en œuvre pour chaque type de procédure dématérialisée.

Toutefois, les attentes et les exigences de la dématérialisation des marchés publics sont déjà connues. Nous les détaillons ci-dessous.

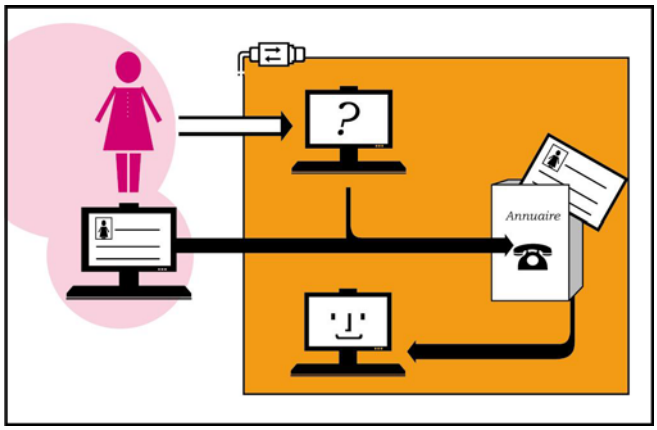
La mise en œuvre de la sécurité engageant la responsabilité de la personne publique qui passe le marché, elle aura intérêt, pour garantir sa sécurité juridique, à faire appel à un Tiers de Confiance dont le métier est précisément de prendre un engagement sur des prestations de sécurité.

3.1 Identification certaine des acteurs

Le mécanisme d'authentification des personnes et des sites web sur Internet repose sur une "carte d'identité" infalsifiable : le certificat.

Dans le mécanisme de signature électronique, c'est l'utilisation du certificat qui permet d'être certain de l'identité du signataire.

Dans le mécanisme de chiffrement, c'est l'usage du certificat qui permet de garantir que seul le destinataire souhaité sera capable de réaliser le déchiffrement.

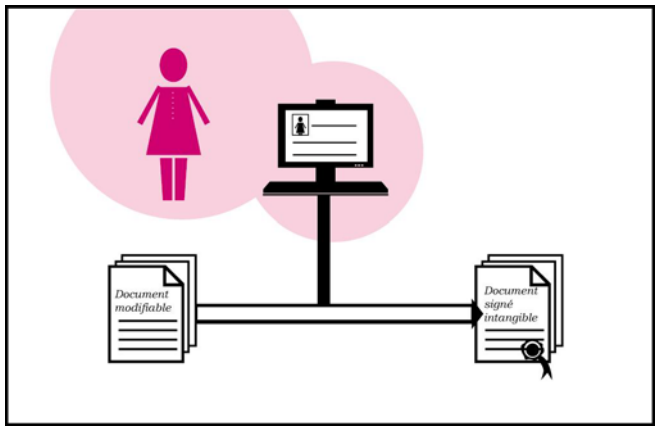


Dans le mécanisme de web sécurisé (protocole SSL, https), c'est encore le certificat qui permet d'authentifier un site.

Toutefois, l'authentification forte par certificat n'est pas indispensable à toutes les étapes : une simple identification déclarative est suffisante pour qu'une entreprise retire un cahier des charges, et une authentification par identifiant / mot de passe peut suffire pour les actions les plus "anodines" côté acheteur.

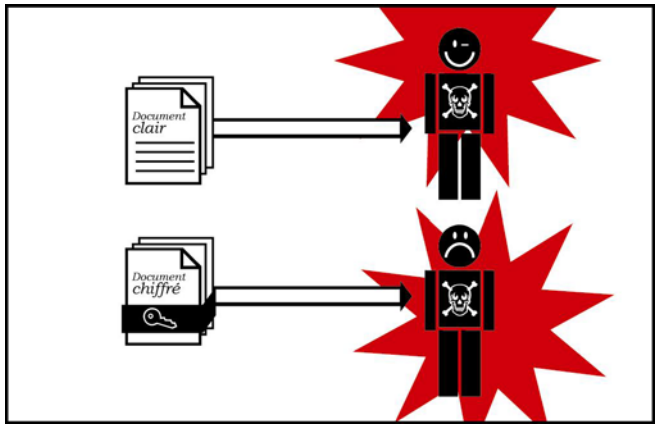
3.2 Intangibilité des données

Une donnée électronique transmise par Internet peut être modifiée, soit pendant sa transmission si elle est interceptée, soit après sa réception, par son destinataire légitime. Or dans le processus de commande publique, il est impératif que cela soit rendu impossible : il faut garantir l'intangibilité des données, aussi appelée "intégrité".



C'est le mécanisme de signature électronique qui permet d'assurer que les documents reçus sont exactement identiques à ce qu'ils étaient lors de l'émission. En effet, lors de la vérification de la signature, toute altération des données entraîne un avertissement.

3.3 Confidentialité

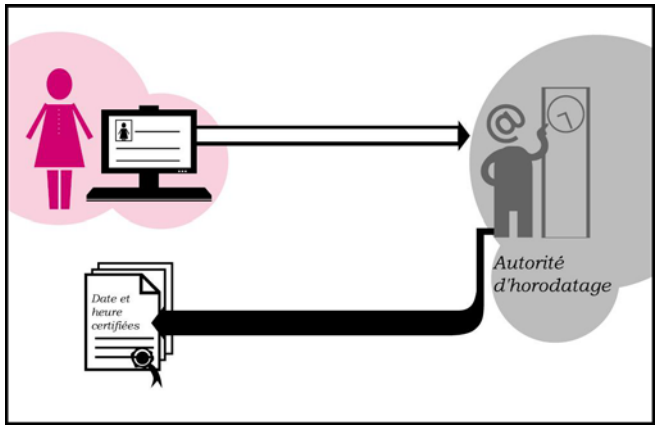


Deux mécanismes permettent de garantir la confidentialité des données échangées.

Le premier consiste à utiliser le protocole SSL pour établir un "tuyau sécurisé" qui garantit les échanges entre les utilisateurs et la plate-forme de dématérialisation contre toute écoute extérieure.

Mais une fois les données transmises par ce moyen, elles sont disponibles en clair pour les exploitants de la plate-forme de dématérialisation. Afin de garantir la confidentialité des plis déposés par les entreprises, il faut ajouter à cela un mécanisme de chiffrement de bout en bout garantissant que les enveloppes scellées par le soumissionnaire ne puissent être ouvertes que par la Personne Publique, et ce sous contrôle de la plate-forme de dématérialisation de manière à garantir la transparence et la traçabilité.

3.4 Dates et heures certaines



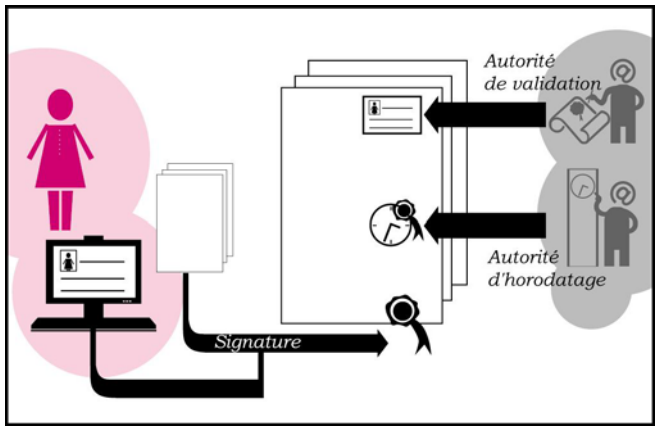
Les dates et heures fournies par les ordinateurs personnels, les serveurs web ou les serveurs de messagerie ne sont pas fiables.

Or, les procédures d'achat public nécessitent de garantir la date et l'heure de certains événements, comme par exemple le dépôt des plis d'un soumissionnaire.

La solution consiste en un service appelé "horodatage" : à partir d'une source d'heure présumée fiable (telle que le GPS, la bande FM,

l'observatoire de Paris, l'ENS…), une Autorité d'Horodatage fournit des "jetons d'horodatage" infalsifiables liant un document à la date et heure à laquelle son existence lui a été prouvée. Ainsi, la plate-forme de dématérialisation pourra attester de la réception d'un pli en horodatant une « preuve de dépôt de pli ».

3.5 Signature électronique



L'envoi d'un document, par mail ou via une interface web par exemple, n'est pas suffisant pour garantir l'engagement de l'émetteur sur le contenu de ce document. En effet, il est très facile de forger de toutes pièces tout type de fichier informatique, et de faire semblant de l'envoyer depuis quelque emplacement que ce soit.

De même, ajouter dans un document une image figurant une signature manuscrite scannée ne vaut pas engagement sur le contenu du document.

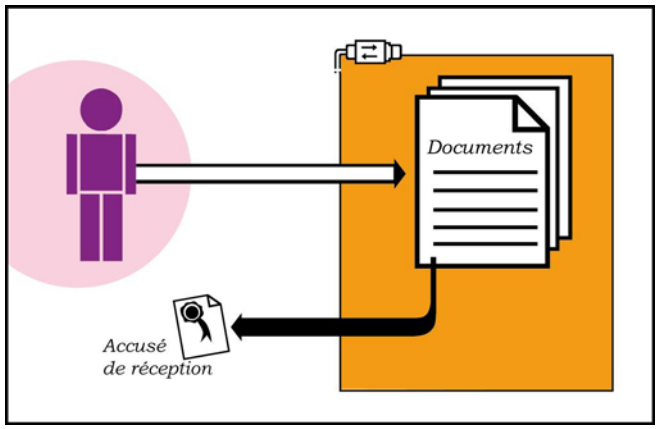
Le mécanisme qui permet de garantir l'engagement de l'émetteur d'un document sur le contenu de ce document est la signature électronique. La plate-forme de dématérialisation doit offrir la possibilité de réaliser et de vérifier une signature électronique à toutes les étapes où cela peut être nécessaire. Cette fonctionnalité peut être offerte soit directement par la

plate-forme, ce qui garantit une ergonomie optimale, soit par un logiciel externe.

Outre l'engagement du signataire, la signature électronique permet de s'assurer de l'intégrité du document : toute modification de celui-ci entraîne une invalidité de la signature. Afin de permettre sa vérification, une signature électronique comprendra également un horodatage de l'instant où elle a été réalisée, ce qui offre une datation certaine du document signé.

Une signature électronique est réalisée à l'aide d'un certificat, que le signataire doit acquérir. L'arrêté du 28 août 2006 précise quelles familles de certificats peuvent être employées pour la dématérialisation des marchés publics. La plate-forme de dématérialisation offrira a minima un lien vers cette liste de certificats.

3.6 Accusés de réception



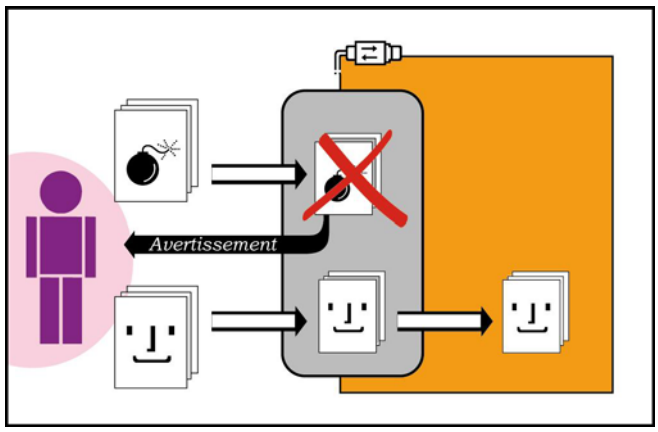
Les nombreux échanges qui ont lieu au cours des procédures de passation de marchés publics nécessitent la fourniture systématique d'accusés de réception faisant foi de l'opération et lui donnant date et heure certaines.

Que ce soit via le service de dématérialisation, comme pour l'envoi d'un avis aux organes de publicité et le dépôt de pli, ou via un service de courrier électronique recommandé, comme pour les questions / réponses, les demandes de précisions ou la notification du marché, les accusés de réception sont omniprésents.

Si certains logiciels de messagerie, tels qu'Outlook ou Notes par exemple, offrent des mécanismes dits "d'accusés de réception", ces fonctionnalités basiques n'offrent absolument pas la même validité juridique qu'un envoi recommandé postal et n'offrent aucune garantie de fiabilité.

Il est donc nécessaire de mettre en œuvre un mécanisme garantissant la date et l'heure d'émission d'un pli, garantissant sa réception et garantissant l'identité de la personne qui l'a réceptionné.

3.7 Contrôle anti-virus



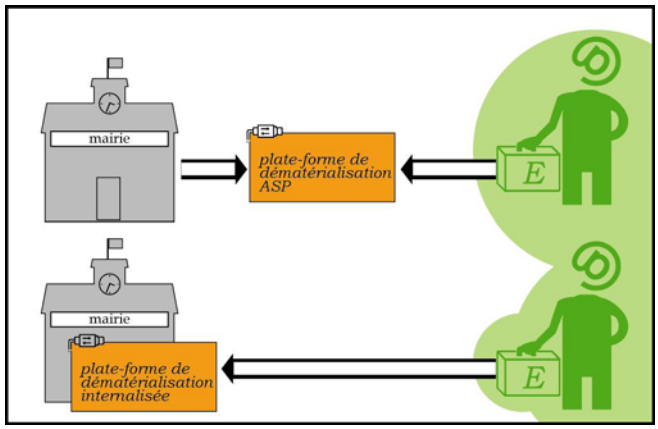
Un contrôle anti-virus doit être réalisé systématiquement sur les fichiers qui transitent par internet de manière à éviter toute contamination.

Pour les documents passant en clair par la plate-forme de dématérialisation (les cahiers des charges par exemple), il est souhaitable que la plate-forme propose un service automatique d'inspection.

En revanche, pour les documents transmis chiffrés, l'inspection doit avoir lieu lors du déchiffrement. En cas de présence d'un virus, le traitement du fichier doit être décrit dans le Règlement de la Consultation, conformément aux attentes du Code des marchés publics. La plate-forme de dématérialisation pourra avantageusement offrir un service de mise en quarantaine pérenne des plis contaminés.

4 Le choix d'une solution de dématérialisation

4.1 Mode internalisé et mode ASP



La Personne Publique, pour sa plate-forme de dématérialisation, a le choix d'opter pour une solution internalisée ou pour une solution en ligne, dite "ASP" (Application Service Provider).

Les éléments permettant d'argumenter un choix dans ce domaine se regroupent en quatre familles.

La responsabilité liée à la dématérialisation est importante. La plate-forme doit garantir une bonne disponibilité, et être irréprochable en termes de confidentialité. Le fait de faire appel à un Tiers de Confiance externe permet d'avoir un horodatage indiscutable et de reporter sur lui, de manière mutualisée et donc moins coûteuse, les exigences de sécurité technique et juridique.

L'évolutivité : les textes juridiques relatifs à la dématérialisation sont en constante évolution depuis 2001, ce qui demande aux plates-formes de s'adapter constamment. Là encore, le recours à une plate-forme mutualisée réduit ces coûts d'adaptation et garantit l'évolutivité.

L'image : les services web sont une composante importante de l'affichage politique d'une collectivité territoriale. Une plate-forme internalisée permettra plus facilement une personnalisation des services rendus et de la charte graphique ; toutefois une grande latitude de personnalisation est parfois source d'erreurs, et les plates-formes mutualisées permettent souvent l'inclusion de ce service au sein d'un portail général de la Personne Publique.

Le coût : outre le coût de développement et de mise en œuvre initial, il faut prendre en compte le coût des évolutions et de l'exploitation de la plate-forme.

4.2 Critères de sélection

Cinq critères de sélection principaux peuvent être mis en œuvre pour le choix d'une plate-forme de dématérialisation.

La qualité fonctionnelle : la plate-forme doit être conforme aux textes et capable d'évoluer selon le contexte réglementaire. Elle doit assurer la sécurité juridique de l'acheteur. Elle doit assurer au mieux l'adhésion des entreprises en donnant confiance et en offrant une ergonomie de qualité. Elle doit offrir un bon niveau d'ouverture : publication des avis, certificats de signature, interfaçage avec les logiciels d'élaboration et de suivi, archivage, contrôle de légalité et comptabilité publique…

La qualité opérationnelle : la plate-forme doit garantir une bonne disponibilité, un temps de réponse rapide, une bande passante suffisante pour éviter les engorgements lors des dépôts d'offres volumineuses.

Le coût : il prend en compte le coût initial, le coût récurrent annuel, le coût à la consommation, mais également le coût de formation à l'outil.

La mise en œuvre : la plate-forme doit être facile à déployer, en un temps raisonnable. La disponibilité et les modalités des formations sont importantes.

La réversibilité : en cas de changement de plate-forme lors du renouvellement du marché, la Personne Publique doit s'assurer de la continuité du service de dématérialisation.

5 Conclusion

La dématérialisation est une révolution technologique. Mais pour qu'elle porte ses fruits en matière de réduction des coûts, d'optimisation de l'achat, d'amélioration de la transparence et de la mise en concurrence, elle doit s'accompagner d'une véritable refonte des processus d'achat, dans un but d'efficience de la commande publique.

Grâce à l'émergence des Tiers de Confiance, des solutions techniques de qualité, qui permettent la dématérialisation dans de bonnes conditions, sont largement disponibles. Deux défis restent maintenant à relever.

Tout d'abord, la professionnalisation du métier d'acheteur public, qui prendra une réelle dimension achat en plus de la dimension presque exclusivement juridique qu'il a aujourd'hui.

Ensuite, l'adhésion des entreprises, encore frileuses dans le dépôt des réponses par la voie électroniques. Gageons que les opérateurs économiques ne tarderont pas à voir tout l'avantage qu'ils ont à avoir recours à l'électronique en termes de simplification des démarches et de gain de temps. Ils n'auront d'ailleurs pas le choix si les acheteurs publics décident d'employer la nouvelle procédure, entièrement électronique, offerte par le Code des marchés publics 2006 : le système d'acquisition dynamique. Sans oublier qu'à partir de 2010, la Personne Publique sera libre d'imposer la réponse par voie électronique pour toutes les procédures !

6 Glossaire

- **Accusé de Réception** : message permettant d'informer l'émetteur de la prise en compte, de la mise en suspens ou du rejet de ses opérations et de la détection d'éventuelles anomalies

- **Archivage électronique** : conservation d'informations pendant une durée déterminée. Cette conservation est destinée à respecter les obligations juridiques imposées par les textes, à prouver les droits d'une personne, ou peut être conçue en vue d'une éventuelle consultation ultérieure des documents.

- **Authentification forte** : processus visant à établir de manière formelle et intangible l'identification des parties à un échange ou à une transaction électronique. Elle se distingue de l'authentification faible par la nécessité d'usage de deux éléments de secret (par exemple : carte à puce + code) et non d'un seul (par exemple : mot de passe).

- **Autorité de Certification (AC)** : organisme ayant la confiance d'une ou plusieurs entités pour produire, distribuer, révoquer, suspendre, renouveler ou archiver des certificats numériques.

- **Autorité d'horodatage (AH)** : entité qui atteste la date de création ou de signature d'un document électronique.

- **BOAMP (Bulletin Officiel des Annonces des Marchés Publics)** : le BOAMP publie les Avis d'Appel Public à la Concurrence (AAPC) afin d'informer les candidats potentiels à un marché des principales caractéristiques de ce dernier.

- **Certificat** : donnée numérique établissant le lien entre une clef publique et l'identité de son propriétaire dans un système cryptographique à clef publique.

- **Chiffrement / Déchiffrement**: procédé visant à transformer, à l'aide de conventions secrètes, des informations ou des signaux clairs en informations ou signaux inintelligibles pour des tiers. Le procédé peut également permettre de réaliser l'opération inverse, grâce à des matériels ou logiciels conçus à cet effet (art. 28 de la

loi du 29 décembre 1990 modifiée par la loi du 21 juin 2004). Ce processus utilise généralement des algorithmes cryptographiques.

- **Enchères Electroniques Inversées** : procédé de mise en concurrence de soumissionnaires à un marché via lequel ils peuvent revoir à la baisse le prix de leur prestation. D'autres critères quantifiables que le prix peuvent également être employés, tels que le délai de livraison ou la durée de garantie.

- **Horodatage** : l'horodatage est un ensemble de techniques utilisant des algorithmes cryptographiques permettant de s'assurer qu'un document électronique a été créé, signé, déposé, reçu, demandé ou consulté à une certaine date et heure. La datation des messages échangés se doit d'être fiable, précise, protégée et reconnue par les partenaires à l'échange puisque c'est le système d'horodatage mis en place qui servira de preuve en cas de litige.

- **Protocole SSL** : protocole de sécurisation permettant de chiffrer des informations sensibles à partir d'un navigateur internet standard, sans recours à un logiciel de cryptage spécifique.

- **Référentiel** : document technique définissant les caractéristiques que doit présenter un produit ou un service et les modalités de contrôle de la conformité du produit ou service à ces caractéristiques.

- **Signature électronique** : La signature électronique est une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification du signataire et de l'origine des informations. La signature électronique doit satisfaire aux quatre exigences suivantes : être propre au signataire ; permettre d'identifier le signataire ; être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et garantir le lien avec les données auxquelles elle s'attache, de telle sorte que toute modification ultérieure de ces données soit détectable.